IX

АПИНО

ICAIT

9TH INTERNATIONAL CONFERENCE ON ADVANCED INFOTELECOMMUNICATIONS ICAIT 2020

IX МЕЖДУНАРОДНАЯ НАУЧНО-ТЕХНИЧЕСКАЯ
И НАУЧНО-МЕТОДИЧЕСКАЯ КОНФЕРЕНЦИЯ
«АКТУАЛЬНЫЕ ПРОБЛЕМЫ ИНФОТЕЛЕКОММУНИКАЦИЙ
В НАУКЕ И ОБРАЗОВАНИИ»

СБОРНИК НАУЧНЫХ СТАТЕЙ

26–27 ФЕВРАЛЯ 2020 ГОДА

APINO.SPBGUT.RU

СПбГУТ))) 90 ЛЕТ

Санкт-Петербургский государственный университет телекоммуникаций им. проф. М. А. Бонч-Бруевича

АПИНО

ICAIT

9TH INTERNATIONAL CONFERENCE ON ADVANCED INFOTELECOMMUNICATIONS ICAIT 2020

IX МЕЖДУНАРОДНАЯ НАУЧНО-ТЕХНИЧЕСКАЯ И НАУЧНО-МЕТОДИЧЕСКАЯ КОНФЕРЕНЦИЯ «АКТУАЛЬНЫЕ ПРОБЛЕМЫ ИНФОТЕЛЕКОММУНИКАЦИЙ В НАУКЕ И ОБРАЗОВАНИИ»

Научные направления:

– Радиотехнологии в связи
– Инфокоммуникационные сети и системы
– Информационные системы и технологии
– Теоретические основы радиоэлектроники
– Цифровая экономика и управление в связи
– Гуманитарные проблемы информационного пространства
– Сети связи специального назначения

Генеральный партнёр:

технологии бесконечности ®
КОМПАНИЯ «Т8»

ООО «Т8»

Партнёры:

Ростелеком

ПАО «Ростелеком»

МегаФон

ПАО «МегаФон»

SERTEK

ООО «Сертек»

АРГУС НТЦ

ООО «НТЦ АРГУС»

специальные системы ФОТОНИКА

ООО «Специальные Системы. Фотоника»

Информационные партнёры:

ТУЗС

журнал
«Труды учебных заведений связи»

НАУЧНО-ТЕХНИЧЕСКИЙ ЖУРНАЛ ИНФОРМАЦИЯ КОСМОС

журнал
«Информация и космос»

Информационная поддержка:

www.iit.sut.ru

электронный журнал «Информационные технологии и телекоммуникации»

26–27 ФЕВРАЛЯ 2020

APINO.SPBGUT.RU

УДК 001:061.3(082)
ББК 72 А43

Актуальные проблемы инфотелекоммуникаций в науке и образовании. IX Международная научно-техническая и научно-методическая конференция;
сб. науч. ст. в 4 т. / Под. ред. С. В. Бачевского;
сост. А. Г. Владыко, Е. А. Аникевич.
СПб. : СПбГУТ, 2020. Т. 1. 885 с.

В научных статьях участников конференции исследуются состояние и перспективы развития мирового и отечественного уровня IT и телекоммуникаций. Предлагаются методы и модели совершенствования научно-методического обеспечения отрасли связи и массовых коммуникаций.

Предназначено научным работникам, аспирантам и студентам старших курсов телекоммуникационных и политехнических вузов, инженерно-техническому персоналу и специалистам отрасли связи.

Научное издание
Литературное редактирование,
корректура Е. А. Аникевич
Оформление Г. И. Юрьев
Верстка Е. М. Аникевич
Подписано в печать 01.08.2020.
Вышло в свет 31.08.2020. Формат 60×90 1/8.
Уст. печ. л. 55,31. Заказ № 061-ИТТ-2020.
пр. Большевиков, д. 22, корп. 1.
Россия, Санкт-Петербург, 193232

ISBN 978-5-89160-197-0

СОДЕРЖАНИЕ

УДК 004.056.55
ГРНТИ 81.93.29

СКРЫТНОЕ РАСПРЕДЕЛЕНИЕ КРИПТОГРАФИЧЕСКИХ КЛЮЧЕЙ ПО ПОСТОЯННОМУ КАНАЛУ, В УСЛОВИЯХ ВОЗМОЖНОГО БЕСШУМНОГО ПЕРЕХВАТА И ПЕРСПЕКТИВЫ ИСПОЛЬЗОВАНИЯ КВАНТОВЫХ КОМПЬЮТЕРОВ

А. С. Герасимович, М. М. Кабардов, В. И. Коржик, В. С. Старостин, В. А. Яковлев

Санкт-Петербургский государственный университет телекоммуникаций им. проф. М. А. Бонч-Бруевича

Предлагается протокол распределения криптоключей по постоянному (типа Интернет) каналу связи в условиях идеального пассивного перехвата. В отличии от известных ранее протоколов, использующих технологию криптосистем с открытым ключом (Диффи-Хеллман и др.) предлагаемый протокол не основан на каких-либо криптографических предположениях и поэтому он не может быть скомпрометирован даже при возможном появлении в будущем квантовых компьютеров.

распределение ключей, каналы связи с постоянными параметрами, искусственный шум, собственные числа матриц, квантовые компьютеры.

Известно, что обеспечение информационной безопасности при передаче и хранении цифровых сообщений не может быть достигнуто в современных условиях без использования их стойкого шифрования. Последнее реализуется при помощи как блоковых, так и потоковых шифров, применяющих такие известные стандарты шифрования, как DES, 3DES, ГОСТ 28147-89, IDEA, ГОСТ Р 34.12-2015, AES, A5/1, A5/3 и др. [1]. Стойкость используемых стандартов (т.е. невозможность их взлома без знания ключей шифрования) не вызывает особых опасений. Однако, проблема распределения таких ключей между легитимными пользователями по-прежнему еще далека от своего окончательного решения. В 70-е года прошлого века произошла настоящая *революция в криптографии*, благодаря изобретению *криптосистем с открытым ключом* (КОК) [2, 3]. В отличие от обычных криптосистем, где ключ шифрования и дешифрования должна совпадать, КОК имеют открытый для всех пользователей ключ шифрования и закрытый (секретный) ключ дешифрования. Очевидно, что эти ключи должны

быть как-то связаны между собой, однако, как было показано в работах изобретателей КОК и последующих авторов, развивавших это направление, закрытый ключ может быть рассчитан по открытому ключу, однако, при правильном выборе параметров КОК, это требует нереализуемо большого числа операций и, следовательно, нереализуемо большого времени использования современных ЭВМ даже при оптимистичном прогнозе на увеличение их быстродействия в будущем.

При использовании КОК задача распределения ключей между двумя пользователями *A* и *B* может быть решена весьма просто: *A* генерирует пару ($К_{ША}$, $К_{ДА}$) ключей, где $К_{ША}$ – открытый ключ шифрования *A*, а $К_{ДА}$ – закрытый ключ дешифрования *A*; далее *A* посылает непосредственно *B* (или через доверительный центр) $К_{ША}$, храня ключ $К_{ДА}$ в секрете. Получив ключ $К_{ША}$, легитимный пользователь *B* шифрует свое сообщение на открытом ключе и посылает его *A*, который дешифрует его на своем секретном ключе $К_{ДА}$ (аналогично производится передача секретных сообщений от *B* к *A*).

Невозможность восстановления $К_{Д}$ по известному для всех нелегитимных пользователей ключу $К_{Ш}$ объясняется тем, что это требует решения так называемых *трудных задач математики*. К таким задачам относятся: факторизация (т. е. разложение на множители) больших целых чисел, вычисление дискретных логарифмов, исправление ошибок случайными линейными кодами и др. [1, 2]. Однако, сравнительно недавно, Шором была доказана теорема о том, что при использовании *квантовых компьютеров* многие из этих задач могут быть решены в *полиноминальное время* (т. е. со сложностью «n^S», где *n* – длина ключа в битах, а *S* – некоторое (умеренно большое) натуральное число [4].

К сожалению (или к счастью для разработчиков шифра) создание квантовых компьютеров кажется пока весьма проблематичным. Достигнуты лишь очень слабые результаты по обработке так называемых *q*-битов и прогноз прогресса в этой области достаточно пессимистичен [5].

Однако, поскольку противоположное утверждение о том, что невозможно создать такой квантовый компьютер также не доказано, то представляет интерес разработка криптосистем и систем распределения ключей стойких к атакам, использующим квантовые компьютеры. Такие системы получили название *постквантовых.* В последнее время появилось много статей и даже проводятся специализированные конференции, посвященные данному направлению [6].

Протокол распределения ключей, который предлагается и обосновывается в настоящей работе, также является постквантовым. Однако, в отличии от других постквантовых технологий он не базируется ни на каком крипто-

графическом предположении (*cryptographic assumption*), т. е. на недоказанных утверждениях о трудности решения различных криптографических проблем (например, на трудности факторизации больших чисел и т. п.).

Еще одним примером протокола, который, казалось бы, позволяет зашифровать сообщения без предварительного распределения ключей, является протокол, основанный на выполнении следующего условия:

$$f_K(f_{K'}(M)) = f_{K'}(f_K(M)), \quad (1)$$

где $f_K(M), f_{K'}(M)$ – это алгоритм симметричного шифрования сообщения M на ключах K и K', соответственно.

Тогда A может передать сообщения M в зашифрованном виде, выполняя следующие 4 шага протокола по обмену информации между легитимными пользователями A и B:

$$\begin{aligned} 1.\ C_A &= f_{KA}(M) \\ 2.\ C_B &= f_{KB}(C_A) \\ 3.\ C'_A &= f_{KA}\, f_{KA}^{-1}(C_B) \\ 4.\ f_{KB}^{-1}(C'_A) &= M, \end{aligned} \quad (2)$$

где C_A – криптограмма сообщения M на ключе K_A, переданная от A к B; C_B – криптограмма сообщения C_A на ключе K_B, переданная от B к A; C'_A это дешифрованное сообщение C_B на ключе K_A и переданное от A к B; $f_{KB}^{-1}(\mathrm{C}'_\mathrm{A})$ – это дешифрованное сообщение C'_A на ключе K_B, которое восстанавливает пользователь B.

Однако протокол (2) «работает» при выполненном условии (1), которое не выполняется для обычных блоковых шифров. Если же использовать блоковый шифр в виде КОК, то это сведется к криптографическому предположению о сложности решения некоторых задач.

Для потокового шифра шифрование сводится к сложению с гаммой, зависящей от ключа, то есть:

$$f_K(M) = M \oplus \gamma(K),\ f_{K'}(M) = M \oplus \gamma(K'),$$

где $\oplus$ – операция сложения mod2 для двоичных сообщений и гамм.

Но тогда после выполнения шагов 1 и 2, перехватчик находит $\gamma(K_B)$, складывая по mod2 C_A и C_B, а затем на шаге 4, находит M.

Еще один подход к распределению ключей предложен в работе [7]. В этом случае пользователи передают случайные биты в общую сеть, однако, должна быть сохранена анонимность создания бит ключа самими пользователями. Совпадающие биты ключа выбранной пары пользователей удаляются, а в качестве ключа используются не удаленные биты A (или B), по договорённости. Однако, уязвимостью данного метода оказывается возможность нарушения анонимности битов A и B, например, по исследованию

особенностей распространения сигналов, переданных по каналу связи между *A* и *B*.

Наконец, в последние года появилось целое направление обеспечения информационной безопасности (*physical layer security*, PHY) [8], когда секретность обеспечивается за счет физических свойств каналов с флюктуацией параметров (например, в каналах с замираниями для технологии MIMO).

Так в работе [9] авторы предложили криптосистему, основанную на MIMO технологии, однако, в [10] было доказано, что она не обеспечивает секретности передачи сообщений, если количество антенн перехватчика больше, чем количество антенн легитимных пользователей.

Анализируя направление PHY можно сделать общий вывод, что к настоящему времени *не существует безопасного протокола выработки общих ключей, если не предполагать каких-либо преимуществ легитимных пользователей перед нелегитимными*.

Предлагаемый в данной работе протокол не требует никаких предположений невыполнимых для практики. В частности, возможно даже выполнение условия, что шумы и флюктуация параметров вообще отсутствуют для канала перехвата, а обмен информацией производится пакетами данных, например, как в сети Интернет.

Единственное условие, которое должно выполняться, это *аутентификация пользователей*, т. е. легитимные пользователи должны быть уверены, что они обмениваются сигналами с легитимными же пользователями, а не с перехватчиком.

Однако это условие должно выполнятся и для *любых других протоколов*, в частности для технологии с открытым ключом.

Конечно, можно обеспечить аутентификацию и по каналам связи, но тогда легитимные пользователи должны иметь какие-то преимущества по сравнению с нелегитимными, например, по отношению С/Ш как в [11] (U. Mauer доказал теорему для *Вайнеровской концепции отводного канала* [12] о том, что или должно быть преимущество по отношению С/Ш, или канал должен быть аутентифицирован).

Перейдем теперь к описанию и оценке эффективности предлагаемого протокола. За его основу была взята схема EVSKey, предложенная в работе [13]. Сценарий, соответствующий этой схеме показан на рис. 1 (см. ниже).

Видно, что он реализуется при помощи двух итераций, которые поочередно выполняются легитимными пользователями A и B. Матрицы G_A, G_B, X_A X_B генерируются пользователями случайно, а матрицы H_{AB}, H_{BA} описывают каналы передачи информации. Матрицы N_{A1}, N_{A2} описывают шумы пользователей. После обмена информации, пользователь A формирует мат-

рицу Y_{A2}, а пользователь B матрицу Y_{B2}, что позволяет им вычислить, соответственно, матрицы $PQ = Y_{A2}(X_A)^{-1}$, $QP = Y_{B2}(X_B)^{-1}$, $P = H_{BA}G_B$, $Q = H_{AB}G_A$, где для прямоугольных матриц обратные матрицы могут быть найдены по процедуре Penrose's [14]. Из алгебры [14] известно, что матрицы PQ и QP имеют одинаковые характеристические многочлены и, следовательно, одинаковые собственные числа. Поэтому пользователи A и B, вычисляют одинаковые (с точностью до шумов) собственные числа и после квантования выделяют (возможно с некоторой небольшой ошибкой) общие ключи.

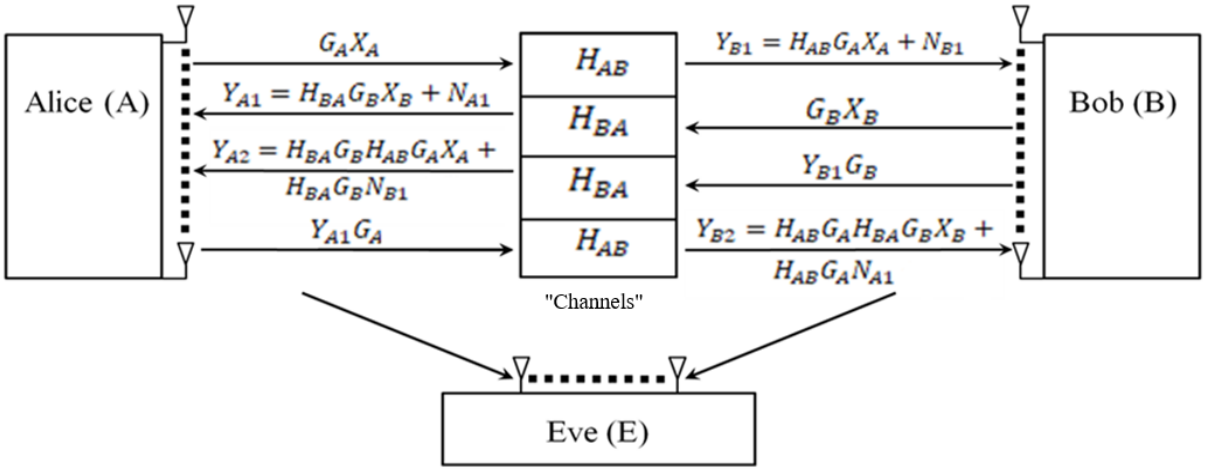


Рис. 1. Сценарий, соответствующий EVSKey схеме [13]

Авторы [13] утверждали, что такие общие ключи полностью защищены от перехвата, если перехватчик расположен даже на малых расстояниях от легитимных пользователей. Однако, в работе [10] было доказано, что при отсутствии шумов у перехватчика это утверждение не верно. (В действительности, авторы [9] «пропустили» такую атаку, как вычисление матрицы $Y = Y_{A2}(Y_{B2})^{-1} \cdot Y_{B2}(Y_{A1})^{-1}$, которая подобна матрице QP и, следовательно, имеет такие же собственные числа, как и матрица QP). Если же в канале перехвата имеется шум, то, как показало моделирование в работе [13], перехватчик так же получит биты ключа с ошибками, но не большими, чем такие же ошибки бит ключа, получаемыми легитимными пользователями.

Поэтому в настоящей работе, будет выполнена существенная модификация данной схемы, которая, как показано далее, обеспечит секретность распределяемых ключей (в терминах утечки информации по Шеннону) и надежность (в терминах высокой вероятности совпадения бит ключа у легальных пользователей). Основные изменения в сценарии распределения ключей по сравнению с работой [13] состояли в следующем:

− канал связи предполагается постоянным (типа сети Интернет), однако матрицы «каналов» H_{AB} и H_{BA} генерируются случайно самими легитимными пользователями;

− шумы N_{B1} и N_{A1} генерируются случайно A и B (т. е. они представляют собой *искусственный шум*).

Биты ключей извлекаются обоими легитимными пользователями из квантованных собственных чисел матриц PQ и QP примерно также, как это делалось в работе [10]. Предполагается также, что перехватчик E извлекает биты ключа легитимных пользователей после квантования матрицы Y.

Для того, чтобы минимизировать утечку к перехватчику информации о ключах и одновременно обеспечить надежное совпадение ключей A и B предлагается использовать протокол *преимущественного улучшения основного канала* (ПУОК), предложенный в [15]. Суть его заключается в том, что пользователь A повторяет S раз каждый бит ключа, выделенный из собственных чисел матрицы PQ, а пользователь B принимает этот бит тогда и только тогда, когда он получает подряд S нулей или S единиц, а остальные биты ключа он стирает и оповещает об этом A. Легко доказать, что после такого преобразования вероятность несовпадения бит у A и B будет:

$$\widetilde{P}_l = \frac{P_l^S}{P_l^S + (1-P_l)^S}, \tag{3}$$

где P_l – вероятность несовпадения «сырых» бит A и B после квантования собственных чисел.

Вероятность ошибки бита ключа у перехватчика, который принимает каждый повторенный S раз бит (где S – четное) по *мажоритарному правилу*, будет равна:

$$\widetilde{P}_e = \sum_{i=\frac{S+1}{2}}^{S} \binom{S}{i} P_e^i (1-P_e)^{S-i}, \tag{4}$$

где P_e – вероятность ошибки бита ключа у перехватчика.

Важно отметить, что смысл создание искусственного шума N_{A1}, N_{B1} легитимными пользователями состоит в том, что этот шум переходит в шум перехватчика, который уже *не может быть уменьшен* даже при нулевом собственном шуме перехватчика.

Для того, чтобы обеспечить S-кратное повторение бит при их выделении из неповторяющихся собственных чисел, предлагается следующая схема, показанная на рис. 2.

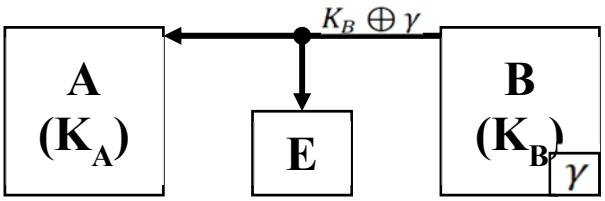


Рис. 2. Схема обеспечения S-кратных повторений «сырых» бит ключа

В этом случае в качестве ключевой последовательности используется двоичная последовательность γ, генерируемая чисто случайно пользователем B, который передает по открытому и бесшумному каналу связи цепочку $K_B \oplus \gamma$, где K_B – цепочка «сы-

рых» ключевых бит, сформированных B из квантованных собственных чисел (В этом случае очевидно, что каждый бит γ легко может быть повторен S раз).

Легко видеть, что после использования схемы по рис. 2, пользователь A получает ключевую цепочку:

$$\widetilde{K_A} = K_B \oplus \gamma \oplus K_A = K_A \oplus \varepsilon_{AB} \oplus K_A \oplus \gamma = \gamma \oplus \varepsilon_{AB},$$

где ε_{AB} – двоичный шум между ключевыми цепочками A и B.

В тоже время, перехватчик E получит искаженную шумом цепочку:

$$\widetilde{K_e} = K_e \oplus \gamma \oplus K_B = K_B \oplus \varepsilon_{BE} \oplus \gamma \oplus K_B = \gamma \oplus \varepsilon_{BE},$$

где ε_{BE} – двоичный шум между B и E.

В таблице 1 показаны результаты моделирования (и теоретических расчетов по (3), (4)) для вероятностей битовых ошибок легитимных пользователей и перехватчика P_l, P_e (до S-кратного повторения) и $\widetilde{P}_l, \widetilde{P}_e$ (после S-кратного повторения) при различных дисперсиях искусственного шума σ^2 и различных размерах $n \times n$ матриц (n = 4 и 64).

ТАБЛИЦА 1. Результаты моделирования вероятностей битовых ошибок до и после выполнения протокола ПУОК

$n = 4$ $\sigma^2 = 0,1$				
P / S	$P_l = 0,26$		$P_e = 0,21$	
	$\widetilde{P}_l^{exp}$	$\widetilde{P}_l^{theor}$	$\widetilde{P}_e^{exp}$	$\widetilde{P}_e^{theor}$
3	0,016	0,041	0,041	0,12
5	0,017	0,0057	0,019	0,068
$n = 4$ $\sigma^2 = 0,2$				
P / S	$P_l = 0,29$		$P_e = 0,25$	
	$\widetilde{P}_l^{exp}$	$\widetilde{P}_l^{theor}$	$\widetilde{P}_e^{exp}$	$\widetilde{P}_e^{theor}$
3	0,029	0,068	0,087	0,16
5	0,029	0,013	0,032	0,11
$n = 64$ $\sigma^2 = 0,1$				
P / S	$P_l = 0,083$		$P_e = 0,092$	
	$\widetilde{P}_l^{exp}$	$\widetilde{P}_l^{theor}$	$\widetilde{P}_e^{exp}$	$\widetilde{P}_e^{theor}$
3	0,0019	0,0007	0,028	0,024
5	0,0021	0,000006	0,010	0,0065
$n = 64$ $\sigma^2 = 0,2$				
P / S	$P_l = 0,085$		$P_e = 0,12$	
	$\widetilde{P}_l^{exp}$	$\widetilde{P}_l^{theor}$	$\widetilde{P}_e^{exp}$	$\widetilde{P}_e^{theor}$
3	0,0022	0,0008	0,057	0,039
5	0,0024	0,000007	0,033	0,014

Примечание. Расчёты по (3), (4) помечены верхним индексом «*theor*», а расчёты моделированием – верхним индексом «*exp*».

По данной таблице можно сделать следующие выводы:

− вероятность ошибки можно уменьшить при увеличении S, причем преимущественно для легитимного пользователя;

− вероятности ошибок убывают при увеличении размеров матрицы «*n*»;

− экспериментально найденные и теоретически рассчитанные вероятности ошибок значительно отличаются, что может говорить о существовании зависимости между легитимным каналом и каналом перехвата.

Вероятности ошибок для легитимных пользователей оказываются, однако, недостаточно малыми. Для их существенного уменьшения целесообразно передать *r* проверочных бит, а затем выполнить исправление ошибок каким-либо эффективным кодом, обладающим конструктивным (т. е. практически реализуемым) алгоритмом декодирования.

С другой стороны, для того, чтобы уменьшить утечку информации о ключевой цепочке к перехватчику, необходимо применить *теорему усиления секретности* [16], которая позволяет оценить сверху количество Шенноновской информации I_o, утекающей к *E*, приняв так же во внимание и тот факт, что *E* в точности знает цепочку длиной *r*, переданную *A*, проверочных бит:

$$I_o \leq \frac{2^{-(k-t_c-l_0-r)}}{\alpha \ln 2},$$

где k – длина «сырой» (первичной) цепочки ключевых бит, выделенных *A* и *B*; $t_c = k(1 + \log_2\left(\widetilde{P_e}^2 + \left(1-\widetilde{P_e}\right)^2\right)$ – информация Реньи; α – коэффициент близкий к 0,42 при больших *k*, *r*, *k* – *r*; l_0 – длина ключа после процедуры «усиления секретности».

Как показано в работе [16], которая и объясняет детально процедуру «усиления секретности», состоящую в том, что ключевая цепочка длинной l_0 хешируется случайно выбранными функциями из универсального класса и затем «прореживается» по определенному правилу.

Для того, чтобы оценить требуемую величину утечки информации по Шеннону $V(I_o)$, предлагается использовать неравенство Фэно [17]:

$$H(U/V) \leq h(\widetilde{P_{ed}}) + \widetilde{P_{ed}} \log_2(M-1),$$

где $H(U/V)$ – условие энтропии для *E*; *M* – количество возможных ключей ($M = 2^{l_0}$); $\widetilde{P_{ed}}$ – вероятность ошибочного декодирования ключа перехватчиком при заданной утечке I_o по Шеннону.

Если утечка I_o мала, то есть $H(U/V)$ велика, то вероятность $\widetilde{P_{ed}}$ будет близка к вероятности случайного угадывания $(M-1)/M$, т. е. перехват оказывается бесполезным.

Для исправления ошибок в ключевых битах легитимных пользователей предлагается использовать класс кодов с *малой плотностью прове-*

рок (LDPC), для которых существуют как методы расчёта вероятности ошибок декодирования, так и конструктивные алгоритмы исправления ошибок, а также оценки необходимых для этого числа вычислительных операций [18].

В таблице 2 приведены результаты оптимального выбора параметров LDPC-кодов для некоторых величин, взятых из таблицы 1 (σ^2, P_l, P_e, S, l_0, $I_o = 10^{-3}$ бит).

ТАБЛИЦА 2. Расчёт оптимизированных величин k_o, r_o LDPC кодов, а также вероятностей ошибочного декодирования ключевых цепочек P_{ld} для этих кодов

$\boldsymbol{\sigma^2 = 0,1, P_l = 0,083, P_e = 0,092}$				
$\boldsymbol{S}$ $\boldsymbol{l_0}$	$\boldsymbol{k_0}$ $\boldsymbol{r_0}$	$\boldsymbol{\frac{k_0}{k_0 + r_0}}$	$\boldsymbol{I_0^{eff}}$ (bit)	$\boldsymbol{P_{ld}}$ $\boldsymbol{I}$(KB)
3 64	1255 25	0,98	0,0007	$3 \cdot 10^{--3}$ 278
5 64	11368 252	0,98	0,0009	$2 \cdot 10^{--3}$ 2992
$\boldsymbol{\sigma^2 = 0,2, P_l = 0,085, P_e = 0,12}$				
$\boldsymbol{S}$ $\boldsymbol{l_0}$	$\boldsymbol{k_0}$ $\boldsymbol{r_0}$	$\boldsymbol{\frac{k_0}{k_0 + r_0}}$	$\boldsymbol{I_0^{eff}}$	$\boldsymbol{P_{ld}}$ $\boldsymbol{I}$
3 64	1080 27	0,98	0,001	$8 \cdot 10^{--3}$ 241
3 256	1990 45	0,98	0,002	$7 \cdot 10^{--3}$ 443
3 512	3689 84	0,98	0,002	10^{--3} 822

Из данной таблицы видно, что при некотором выборе параметров LDPC кодов k_o, r_o обеспечиваются достаточно малые вероятности ошибочного декодирования битовых цепочек для легитимных пользователей, причем это выполняется при помощи конструктивно реализуемого алгоритма декодирования LDPC-кодов.

В нижних строках последние столбцы таблицы 2 приводятся результаты расчета для требуемой передачи траффика (в Мбайтах), который необходимо выполнить по каналам связи легитимными пользователями для выработки ключа [19].

Важной характеристикой предложенного приема является сложность декодирования LDPC-кодов. В работе [19] приведена формула для оценки количества операций, требуемых для декодирования LDPC-кодов с заданными параметрами.

Для примера, где $\sigma^2 = 0,2$ в таблице 2, а $k_o + r_o \approx 2035$, выбран (407,9) LDPC-код. Тогда получим примерное число требуемых операций равное 858770.

В заключение данной работы , можно отметить, что по мнению ее авторов, в ней впервые , в известной им научно-технической литературе, был предложен протокол распределения криптоключей, который обеспечивает теоретический уровень их секретности при обмене информацией по постоянному бесшумному каналу (типа Интернета) при отсутствии любых преимуществ у перехватчика и при отсутствии любых криптографических предположений, за исключением требования аутентификации легитимных пользователей во время обмена информацией. Однако для решения последней проблемы могут использоваться хорошо известные методы, описанные в работах [20, 21, 22, 23].

В качестве перспективных направлений дальнейших исследований можно отметить следующие:

− оптимизацию выбора параметров протокола для минимизации общего трафика обмена информацией между легитимными пользователями;

− уточнение требований по безопасности (в терминах Шенноновской информации);

− проработку наиболее приемлемых методов аутентификации и оценки их сложности;

− разработка алгоритмов декодирования LDPC- кодов и уменьшения их сложности.

Список используемых источников

1. Коржик В. И., Яковлев В. А. Основы криптографии : учебное пособие. СПб. : НЦ Интермедиа, 2016. 296 с. ISBN 978-5-89160-097-3.

2. A. J. Menezes, P. C. van Oorschot, and S. A. Vanstone, Handbook of Applied Cryptography, ser. The CRC Press series on discrete mathematics and its applications. 2000 N. W. Corporate Blvd., Boca Raton, FL 33431-9868, USA: CRC Press, 1997. ISBN 0-8493-8523-7.

3. W. Diffie and M. E. Hellman, “New directions in cryptography,” vol. 22, no. 6, pp. 644–654, 1976.

4. P. W. Shor, “Polynomial-Time Algorithms for Prime Factorization and Discrete Logarithms on a Quantum Computer”, in Proc. of the 35th Annual Symp. on Foundations of Comp. Science, 1994.

5. M. I. Dyakonov, “Is Fault-Tolerant Quantum Computation Really Possible?” in Future Trends in Microelectronics, 2007.

6. Post-Quantum Cryptography, 9th International Conference PQCrypto 2018.

7. M. Yung, “A Secure and Useful 'Keyless Cryptosystem'”, Columbia University Computer Science Technical Reports, CUCS-136-84, 2012.

8. A. Mukherjee, et al. “Principles of Layer Security in Multiuser Wireless Network: A Survey”, arXiv:1011.3754.3 [cs. IP], 2014.

9. T. Dean and A. Goldsmith, “Physical-layer ceyptography through noiseless massive MIMO“, Proc. IEEE Inf. Theory Workshop-2013, pp. 9–16.

10. V. Starostin, V. Korzhik, M. Kabardov, A. Gerasimovich, V. Yakovlev and G. Morales-Luna “Key Generation protocol executing through non-reciprocal fading channels” // International Journal of Computer Science and Applications, vol. 16, no. 1, pp. 1–16, 2019.

11. V. Korzhik, M. Bakin, “Information theoretic secure hybrid authentication in the key distribution problem”, Proc. of the seventh Canadian workstation information theory, pp. 50–69, 2001.

12. A. Wyner, “Wire-tap channel concept,” Bell System Technical Journal, vol. 54, pp. 1355–1387, 1975.

13. D. Qin and Z. Ding “Exploiting Multi-fnyennaNon-Reciprocal Channels for Share Secret Key Generation“, IEEE Trans. on Information Forensics and Security, vol. 11, no. 10, pp. 2691–2705, 2016.

14. Ben-Israel, Adi; Greville, Thomas N. E., p. 7. Generalized inverses: theory and applications (2nded.). NY: Springer. ISBN0-387-00293-6, 2003.

15. U. Maurer, “Secret key agreement by public discussion from common information.” IEEE Transactions on Information Theory, vol. 39, no. 3, pp. 733–742, 1993.

16. V. Korjik, G. Morales-Luna, and V. Balakirsky, “Privacy amplification theorem for noisy main channel”, Lecture Notes in Computer Science, vol. 2200, pp. 18–26, 2001.

17. Fano R. M. Transmission of Information. A statistical theory of communication, Willy Bullisher, 1961.

18. K. Shalkoska, Implementation of LDPC Algorithm: In C Programming Language. LAP LAMBERT Academic Publishing, 2017. ISBN9783330026049. [Online]. Available: https://books.google.com.mx/books?id=1yNcMQAACAAJ

19. V. Korzhik et al, “Protocol of key distribution over public noiseless channels executing without cryptographic assumptions”, IJCSA, 2020 (in printing).

20. D. Dasgupta, A. Roy, and A. Nag, Advances in User Authentication, 1st ed. Springer Publishing Company, Incorporated, 2017. ISBN 3319588060, 9783319588063.

21. R. M. Needham and M. D. Schroeder, “Using Encryption for authentication in Large Network of computers”. ACM, v. 21, pp. 993–999, 1978.

22. Jin R. et al, “MagPairing: Pairing Smartphones in close proximity using magnetometer”, IEEE Trans. of Information Forensics and Security, 6, pp. 1304–1319, 2016.

23. Roy N. et al, “Faster Communication through Physical vibration”, proc. USENIX Symp. Netw. Syst. Design, pp. 671–675, 2016.

ИНФОКОММУНИКАЦИОННЫЕ СЕТИ И СИСТЕМЫ

УДК 004.056
ГРНТИ 81.93.29

SERVER VIRTUALISATION (VMWARE VSPHERE)

M. M. Kovzur, D. D. Hamza

The Bonch-Bruevich Saint-Petersburg State University of Telecommunications

The growth of the companies around the world over the past 10 years is incredible. This has enlarged the sizes and needs of companies. In 2018 the turnover of the global server market increased by 43,7 % year on year to reach $ 22,5 billion in the second quarter. Global server sales increased 20,5 % year over year to 2,9 million units. The global server market continues to experience historic demand, with 2Q18 marking the fourth consecutive quarter of double-digit growth in sales and the highest ever. Volume server revenue increased 42,7 % to $ 18,4 billion, while mid-range server revenue increased 63,0 % to 2,5 billions of dollars. High-end systems rose 30,4 % and are valued at $ 1,7 billion. In 2019 total worldwide server revenue grew 7,5 percent year over year to $ 25,4 billion in the fourth quarter, while server shipments increased 14 percent to just over 3,4 million units. Volume server revenue grew 12 percent year over year to $ 19,7 billion along with 9 percent growth in high-end systems to $ 2,4 billion. With this expansion of companies, physical equipment becomes more expensive, more consuming, more difficult to manage and more occupying space. Server virtualization will help to resolve these problems.

Server Virtualization, VMware, esxi, vCenter, technology, virtual machine, increase, vSphere, GUI, resource, Ram, DRS, physical architecture, cpu, datacenter, HA, VMotion, FT.

More and more companies are migrating from physical servers to virtual servers. More than 92 % of companies use server virtualization [1, 2].

Server virtualization has proven itself to be a revolutionary technology solution for IT management, presenting capabilities that would never be possible within a physical infrastructure. At an economic stance, the benefits of server virtualization are focused on cost savings because it allows multiple applications and systems to be installed on a single physical server [2].

The Server virtualization has brought a lot of advantages to the world:

– *Save time* as it is considerably faster to administer virtual rather than physical servers.

– *Having a reliable disaster recovery plan* is an essential condition for ensuring business continuity. Virtualization makes it possible to be independent of the hardware and to speed up recovery in the event of a disaster or failover.

– *Save* money by reducing administration time (reducing the proliferation of servers), infrastructure needs (avoids the solution of extending the surface of the premises to meet the growing need for Datacenters) and energy consumption (power and cooling).

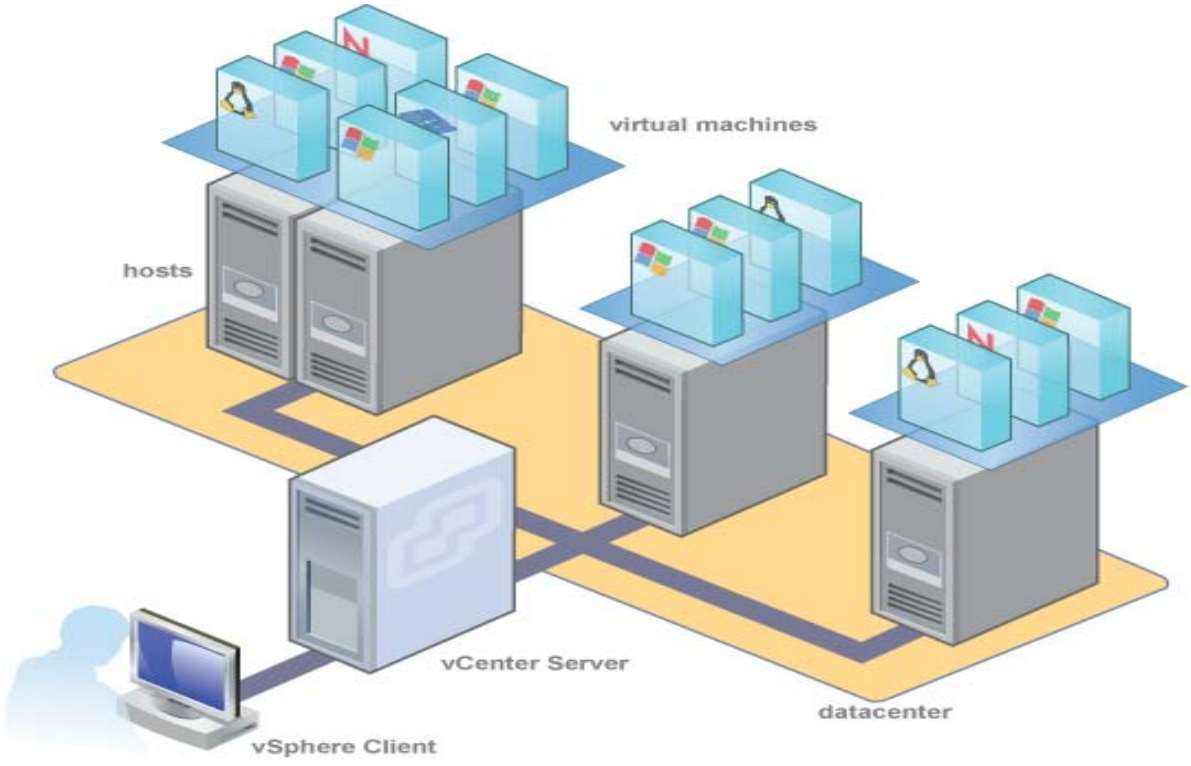
– *Have better power management* within server farms and a decrease in the total cost of ownership of Datacenters.

– *Optimize the resources of a fleet of machines* (distribution of virtual machines on physical machines according to the respective loads).

– *Easy installation, deployment and migration* of virtual machines from one physical machine to another.

– *Isolation of different simultaneous users* of the same machine (central site type use).

In this article we will examine a virtual architecture of VMware vSphere [3, 4].



Pic. 1: Virtual architecture

The vSphere Client is a web-based application that connects to the vCenter Server so IT administrators can manage installations and handle inventory objects in a vSphere deployment.

The vSphere Client presents a graphical user interface (GUI) with an object navigator, the main workspace, and the tasks and alarms panel. Through this GUI, vSphere administrators can manage and supervise the objects listed in a virtualized data center [5, 6, 7].

vCenter is a flagship management tool for the vSphere range. This management tool (optional) allows you to manage all virtual machines and physical hosts [8]. It is also possible through this interface to manage:

supervision alarms (CPU / RAM);

templates (envelopes of pre-configured operating systems);

the use of options (HA, VMotion, DRS, FT ...).

VMware ESXi (host) is a type 1 hypervisor independent of operating systems. It is itself based on the VMkernel operating system which interfaces with the agents whose execution it supports. It is on it that all the machines and server run.

Virtual machine is a computer file, usually called an image, that behaves like a real computer. In other words, it is a computer created inside a computer. ... It is possible to run multiple virtual machines simultaneously on the same physical computer or host (ESXI).

References

1. Kochut, A. and Beaty, K. Washington, D. C. On Strategies for Dynamic Resource Management in Virtualized Server Environments // IEEE Computer Society, 2007. Proceedings of the 2007 15th International Symposium on Modeling, Analysis, and Simulation of Computer and Telecommunication Systems. PP. 193–200.

2. Live Migration of Virtual Machines. Clark, Christopher, et al., et al. 2005 // In Proceedings of the 2nd ACM/USENIX Symposium on Networked Systems Design and Implementation (NSDI).

3. Nguyen, Hien, Tran, F. D. and Menaud, J.-M. SLA-Aware Virtual Resource Management for Cloud Infrastructures. // 2009. Proc. Ninth IEEE Int. Conf. Computer and Information Technology CIT '09. Vol. 1. PP. 357–362.

4. Iqbal, Waheed, Dailey, Matthew N. and Carrera, David. SLA-Driven Dynamic Resource Management for Multi-tier Web Applications in a Cloud // 2010. Proc. 10th IEEE ACM Int Cluster, Cloud and Grid Computing (CCGrid) Conf. PP. 832–837.

5. Krasov A., Vitkova L., Pestov I. Behavioral analysis of resource allocation systems in cloud infrastructure // 2019 International Russian Automation Conference (RusAutoCon) 2019. PP. 886–899.

6. V. Korzhik, E. Gerling, H. Imai, J. Shikata, G. Morales-Luna. On the use of Bhattacharyya distance as a measure of the detectability of steganographic systems // Lecture Notes in Computer Science. 2008. T. 4920 LNCS. PP. 23–32.

7. Shterenberg S. I., Poltavtseva M. A. A distributed intrusion detection system with protection from an internal intruder // Automatic Control and Computer Sciences. 2018. V. 52. No 8. PP. 945–953.

8. Kotenko I., Kuleshov A., Ushakov I. Aggregation of elastic stack instruments for collecting, storing and processing of security information and events // 2017 IEEE SmartWorld, Ubiquitous Intelligence & Computing, Advanced & Trusted Computed, Scalable Computing & Communications, Cloud & Big Data Computing, Internet of People and Smart City Innovation (SmartWorld/SCALCOM/UIC/ATC/CBDCom/IOP/SCI) 2017. PP. 840–847.

УДК 621.391
ГРНТИ 49.40.01

ПЕРЕДАЧА ПОТОКОВЫХ ДАННЫХ В СЕТЯХ БПЛА ДЛЯ СЦЕНАРИЕВ С ОДНИМ ИСТОЧНИКОМ: ОБОБЩЕННЫЙ ОБЗОР РЕЗУЛЬТАТОВ ИССЛЕДОВАНИЙ

А. В. Абилов, Д. С. Васильев, И. А. Кайсина

Ижевский государственный технический университет имени М. Т. Калашникова

В статье представлен обобщенный обзор результатов исследований процесса передачи данных в самоорганизующихся сетях беспилотных летательных аппаратов для сценариев: узел-источник – узел-получатель; узел-источник – узел-ретранслятор – узел-получатель; узел-источник – рой узлов-ретрансляторов – узел-получатель. В сценариях рассмотрено применение методов, улучшающих метрику качества обслуживания по коэффициенту доставки пакетов данных. Даны рекомендации практического применения научных результатов.

сеть БПЛА, потоковая передача данных, ретрансляция, QoS, PDR.

Сети беспилотных летательных аппаратов (БПЛА) являются объектом исследований многих научных коллективов, чему способствует рост промышленности в данном секторе и увеличивающаяся конкуренция. Наиболее востребованными являются следующие области применения БПЛА : чрезвычайные ситуации (МЧС, поиск людей, оповещение населения при ЧС, спасательные операции, лесные пожары, наводнения), мониторинг (электростанции (АЭС), сельское хозяйство, электросети (ЛЭП), земельные ресурсы, нефтегазопроводы, лесные ресурсы, водные ресурсы, инфраструктуры, дороги, ЖД линии, месторождения), безопасность (охрана государственных границ, охрана объектов и людей, обнаружение объектов и людей) и аэрофотосъемка (геокалькулятор, геодезические работы, картографические работы, авиаучет) [1, 2, 3, 4, 5, 6]. Для решения задач в вышеперечисленных областях необходимо используются сети передачи данных, где в качестве узла-источника данных чаще выступает БПЛА, в качестве

узла-получателя – наземная станция. В сети может присутствовать узел-ретранслятор, применение которого является актуальной задачей при выполнении реальных миссий. Также существует ряд задач, связанных с мониторингом обширных наземных территорий в кратчайшие сроки, при решении которых может использоваться рой БПЛА включая несколько узлов-источников и узлов-ретрансляторов.

Ряд сценариев ранее исследован научным коллективом авторов [7, 8, 9, 10, 11, 12, 13, 14, 15, 16]: узел-источник – узел-получатель; узел-источник – узел-ретранслятор – узел-получатель; узел-источник – рой узлов-ретрансляторов – узел-получатель (рис. 1). В работах [8, 10, 14, 15, 16] были представлены методы и алгоритмы, улучшающие качество передачи потоковых данных (видео в режиме реального времени) для сети БПЛА.

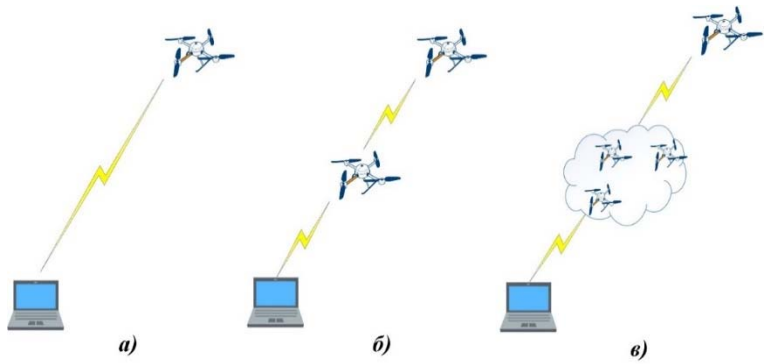


Рис. 1. Сценарии передачи данных в сети БПЛА: а) узел-источник – узел-получатель; б) узел-источник – узел ретранслятор – узел-получатель; в) узел-источник – рой узлов-ретрансляторов – узел-получатель

Характеристики передачи данных для сценария узел-источник – узел-получатель (рис. 1*а*) были исследованы методом имитационного моделирования с применением сетевого симулятора NS-3 [12], а также методом экспериментального исследования с использованием малого БПЛА [16]. Для улучшения качества передачи данных был разработан алгоритм повторной передачи на уровне приложений модели OSI (AL-ARQ) [15, 16, 17, 18, 19]. В программной реализации был определен размер буфера на узле-получателе. При потере фрагмента данных узел-получатель отправляет сообщение с его номером к узлу-источнику, после чего узел-источник повторно отправляет этот фрагмент к узлу-получателю. Алгоритм AL-ARQ продемонстрировал свою эффективность при экспериментальном исследовании. Для оценки алгоритма была выбрана метрика QoS – коэффициент доставки пакетов (*Packet delivery Rate* – PDR), которая вычислялась по формуле:

$$PDR = \frac{R_X}{T_X},$$

где R_X – количество полученных пакетов данных, T_X – количество оправленных пакетов данных.

В экспериментальном исследовании для этого сценария узел-источник (БПЛА) удалялся от наземной станции и совершал облет, во время которого на узел-получатель передавалось потоковое видео. При увеличении расстояние между узлом-источником и узлом-получателем на 200–350 метров метрика PDR без AL-ARQ равнялся 0,97 при использовании AL-ARQ метрика PDR равнялась 1. На интервале от 400 до 500 метров также наблюдалось улучшение значения метрики: при использовании алгоритма 0,9, без применения AL-ARQ 0,8 [16]. Сценарий узел-источник – узел-получатель в настоящее время наиболее распространен при решении задач мониторинга и аэрофотосъемки. Применение имитационного моделирования с заданными параметрами (мощность передатчика, чувствительность приемника и т. д.) может помочь спрогнозировать исход миссии и до начала выполнения скорректировать настройки оборудования для достижения наилучшего результата. Алгоритм AL-ARQ также может улучшить качество передаваемых данных и сократить затраты, связанные с повторными вылетами БПЛА, которые связаны с неудовлетворительным качеством принимаемых данных.

Для второго сценария (рис. 1*б*), узел-источник – узел-ретранслятор – узел-получатель, также было проведено имитационное моделирование в сетевом симуляторе NS-3 [12] и экспериментальное исследование протокола OLSR с использованием микрокомпьютеров Raspberry Pi 3. Целью моделирования являлось определение наиболее эффективного протокола маршрутизации для заданного сценария. В сценарии узел-источник удалялся от узла-получателя от 900 до 2900 метров при этом на расстоянии 1190 метров от узла-получателя находился узел-ретранслятор, который обеспечивал маршрутизацию передаваемых данных по проактивному протоколу OLSR или по реактивному протоколу AODV. Имитационное моделирование показало следующие результаты: на расстоянии 1260 метров оба протокола начинали работу, при этом минимальное значение PDR для AODV составило 0,34, а для OLSR 0,11 [12]. Для экспериментального исследования был выбран протокол OLSR, поскольку он имеет наиболее актуальные обновления и подходил для использования на микрокомпьютерах. В эксперименте на Raspberry Pi 3 была установлена ОС Ubuntu Mate 16 и произведена настройка самоорганизующейся сети на частоте 2,4 ГГц стандарта 802.11 g. Для работы протокола OLSR были подключены необходимые файлы и выполнена настройка. Среди методов для улучшения доставки данных ранее был рассмотрен метод сетевого кодирования. При применении сетевого кодирования на узле-ретрансляторе реализовано суммирование фрагментов данных по модулю 2. После суммирования на узле-ретрансляторе одно ши-

роковещательное сообщение отправляется на узел-источник и узел-получатель. Так как узлы хранят в своем буфере ранее отправленные фрагменты данных, они могут декодировать полученный фрагмент данных. Сетевое кодирование реализовано в протоколе маршрутизации B.A.T.M.A.N., который был рассмотрен в работе [11].

Сценарий с узлом-ретранслятором представляет интерес при решении задач в режиме ЧС, мониторинга и обеспечения безопасности в местностях со сложным рельефом. Сложный рельеф накладывает серьезные ограничения на дальность связи, при этом типичные высоты применения БПЛА для выполнения подобных задач не превышают 500 метров. Таким образом необходимо использовать или отдельные БПЛА ретрансляторы или осуществлять передачу между всеми БПЛА, участвующими в операции.

Для третьего сценария (рис. 1*в*), узел-источник – рой узлов-ретрансляторов – узел-получатель, также было проведено имитационное моделирование в симуляторе NS-3 [7, 13]. Через метрику PDR сравнивалась работа следующих протоколов маршрутизации: HWMP, OLSR, AODV. Для оценки эффективности протоколов было написано несколько программ на языке C++. В программах было задано разное число узлов ретрансляторов в рое: от 10 до 20 с шагом в 5 узлов, также изменялась площадь территории движения узлов со стороной квадрата от 500 до 1500 метров с шагом в 250 метров, узлы ретрансляторы двигались согласно модели мобильности для летающих узлов (*Gauss Markov Mobility Model*). В ходе исследования было выявлено, что наилучший показатель по метрике PDR продемонстрировал гибридный протокол маршрутизации HWMP, на втором месте по значению PDR был проактивный протокол OLSR, наименее эффективным для указанного сценария оказался протокол AODV из-за своего реактивного характера. Метрика PDR для AODV и HWMP не зависела от размера роя узлов-ретрансляторов из-за наличия реактивной составляющей [20]. Сценарий с роем узлов-ретрансляторов также, как и сценарий с одним узлом-ретранслятором может быть практически реализован в режиме ЧС, при решении задач мониторинга и обеспечения безопасности.

В статье был представлен обзор результатов исследований при изучении процесса передачи данных в сети БПЛА для разных сценариев и методов передачи потоковых данных, позволяющих улучшить значения метрики PDR. Среди перспективных сценариев для дальнейшего изучения можно выделить: рой узлов-источников – узел-получатель; рой узлов-источников – узел-ретранслятор – узел-получатель; рой узлов-источников – рой узлов-ретрансляторов – узел-получатель. Перечисленные сценарии могут найти практическое применение в режиме ЧС, а также при задачах мониторинга обширных трудно-достигаемых районов. Сеть с несколькими узлами-источниками в виде БПЛА ставит новые задачи, связанные с: перегрузкой узлов, приоритезацией трафика и выбора наилучшего маршрута.

Работа выполнена при финансовой поддержке РФФИ (проект №19-29-06076).

Список используемых источников

1. Кучерявый А. Е., Владыко А. Г., Киричек Р. В. Теоретические и практические направления исследований в области летающих сенсорных сетей // Электросвязь. 2015. № 7. С. 9.

2. Бондарев А. Н., Киричек Р. В. Обзор беспилотных летательных аппаратов общего пользования и регулирования воздушного движения БПЛА в разных странах // Информационные технологии и телекоммуникации. 2016. Т. 4. № 4. С. 13.

3. Киричек Р. В., Парамонов А. И. Беспилотный летательный аппарат как система массового обслуживания // Электросвязь. 2015. № 7. С. 16–19.

4. Думин Д. И., Динь Ч. З., Фам В. Д., Киричек Р. В. Применение установленных на БПЛА систем обнаружения GSM-устройств для поиска пострадавших в результате ЧС // Информационные технологии и телекоммуникации. 2018. Т. 6. № 2. С. 62–69.

5. Маколкина М. А., Тельтевская В. А., Кулик В. А., Киричек Р. В. Исследование взаимодействия приложений дополненной реальности и методов управления БПЛА // Информационные технологии и телекоммуникации. 2016. Т. 4. № 2. С. 33–42.

6. Леонов А. В., Чаплышкин В. А. Сети FANET // Омский научный вестник. 2015. № 3 (143).

7. Кайсина И. А., Васильев Д. С., Абилов А. В. Анализ эффективности протоколов маршрутизации OLSR и AODV в летающей сети FANET // Вестник ИжГТУ им. М. Т. Калашникова. 2017. Т. 20. № 1. С. 87–90.

8. Vasiliev D. S., Kaysina I. A., Abilov A. Performance evaluation of COPE-like Network Coding in Flying Ad Hoc Networks: Simulation-based Study // Internet of Things, Smart Spaces, and Next Generation Networks and Systems. – Springer, Cham, 2017. PP. 577–586.

9. Vasiliev D. S. et al. Simulation-based Assesment of Quality of Service in UAV-assisted mmWave System in Crowded Area // 2018 23rd Conference of Open Innovations Association (FRUCT). IEEE, 2018. PP. 391–397.

10. Кайсина И. А., Васильев Д. С., Абилов А. В. Сетевое кодирование в сетях FANET // Электросвязь. 2018. № 1. С. 64–68.

11. Kaysina I. A. et al. Performance evaluation testbed for emerging relaying and coding algorithms in Flying Ad Hoc Networks // 2018 Moscow Workshop on Electronic and Networking Technologies (MWENT). IEEE, 2018. PP. 1–5.

12. Кайсина И. А. и др. Сравнительный анализ эффективности ретрансляции потоковых данных в летающей сети // Вестник ИжГТУ им. М. Т. Калашникова. 2019. Т. 22. № 1. С. 108–115.

13. Vasiliev D. S., Meitis D. S., Abilov A. Simulation-based comparison of AODV, OLSR and HWMP protocols for flying Ad Hoc networks // International Conference on Next Generation Wired / Wireless Networking. Springer, Cham, 2014. PP. 245–252.

14. Vasiliev D. S., Vladykina K., Abilov A. Simulation study of application layer relaying algorithms with data-link ARQ in flying ad hoc networks // 2016 19th Conference of Open Innovations Association (FRUCT). IEEE, 2016. PP. 256–263.

15. Vasiliev D. S., Abilov A. Relaying algorithms with ARQ in Flying Ad hoc Networks // 2015 International Siberian Conference on Control and Communications (SIBCON). IEEE, 2015. PP. 1–5.

16. Васильев Д. С. Разработка алгоритмов передачи потоковых данных на прикладном уровне в сетях беспилотных летательных аппаратов: автореф. дисс. канд. ... наук: 05.12.13 / Васильев Данил Сергеевич. Самара, 2015. 19 с.

17. Чунаев А. В., Абилов А. В., Павлова М. М. Алгоритм AL-ARQ для потоковой доставки видеоданных в беспроводной локальной сети // Инфокоммуникационные технологии. 2015. Т. 13. № 1. С. 68–73.

18. Васильев Д. С., Чунаев А. В., Абилов А. В. Экспериментальное исследование качества передачи видео в древовидной P2P сети с алгоритмом ARQ прикладного уровня // T-Comm-Телекоммуникации и Транспорт. 2014. Т. 8. № 1.

19. Чунаев А. В. Алгоритм приоритетной ретрансляции потерянных фрагментов на прикладном уровне для потоковой доставки видеоданных // T-Comm-Телекоммуникации и Транспорт. 2015. Т. 9. № 4.

20. Васильев Д. С., Абилов А. В. Протоколы маршрутизации в MANET // Электросвязь. 2014. № 11. С. 52–54.

УДК 621.396.2
ГРНТИ 49.44.29

ОБЗОР ТИПОВ ВОЛН ДЛЯ БЕСПРОВОДНОЙ ПОДВОДНОЙ СВЯЗИ

С. С. Абрамов[1], Е. С. Абрамова[1], В. Ф. Мышкин[2], И. И. Павлов[1], М. С. Павлова[1]

[1]Сибирский государственный университет телекоммуникации и информатики
[2]Национальный исследовательский Томский политехнический университет

В статье рассматриваются различные типы систем обмена информацией с объектами, находящимися в толще воды. Эти системы связи отличаются используемыми длинами волн: акустические, радиоволны и оптическое излучение. Рассмотрены результаты экспериментов с подводными бистатическими оптико-электронными системами связи, в которых в качестве носителя информации используется рассеянное лазерное излучение.

подводная оптическая связь, оптические волны, беспроводная связь, типы волн.

В настоящее время интенсивно изучаются прибрежные шельфы в связи с подводным мониторингом климатических, биологических, химических и экологических изменений в океанах, морях, озёрах и реках, а также с освоением подводных месторождений полезных ископаемых. Данные задачи решаются с помощью различных подводных роботизированных комплексов, которые требуют наличия надёжной и эффективной системы обмена информацией [1, 2].

Системы беспроводной подводной оптической связи (ПОС) представляют собой одну из немногочисленных технологий, которая может исполь-

зоваться для создания высоко скоростного канала связи в водной среде. Поэтому важно изучение возможностей ПОС, перспективных для многих применений.

К ключевым преимуществам такого способа связи можно отнести высокую скорость передачи информации и мобильность. Потенциальные потребители ПОС выдвигают следующие требования к ней:

– скорость передачи информации не менее 100 Мбит/с;

– высокая четкость передачи видеоизображений в режиме реального времени;

– бесконтактная передача информации, что особенно актуально в водной среде;

– большие углы обзора – важный параметр для использования на роботизированных подвижных платформах [3].

Целью данной статьи является сравнение типов волн (акустических волн, радиоволн и оптического излучения). Выявить их сильные и слабые стороны. В статье основное внимание уделяется пониманию целесообразности и надежности подводных оптических линий связи.

Типы волн для подводной беспроводной связи

Подводная беспроводная передача информации в различных подводных сетях (которые могут включать в себя автономные подводные транспортные средства, беспилотные подводные батискафы или сенсорные сети) активно исследуются на протяжении многих десятилетий. В настоящее время подводная беспроводная связь чаще всего использует два типа волн – акустические и радиоволны. Менее распространены системы, использующие оптические волны. Сравним их сильные и слабые стороны.

Акустические волны

Среди трех типов волн, акустические волны используются в качестве основного носителя для подводной беспроводной связи из-за их относительно малого поглощения и большого расстояния распространения. Первая подводная связь была разработана в Соединенных Штатах с использованием амплитудной модуляции с подавлением несущей в одной боковой полосе на частотах от 8 до 15 кГц. Передаваемый сигнал имел низкое качество и требовал необходимости обнаруживать и обрабатывать искаженный поток информации. С развитием цифровой связи в 1960 году, увеличилась скорость передачи данных и ширина рабочего диапазона частот. В дальнейшем многие исследователи разработали сложные методы для формирования канала оценки и разработали различные алгоритмы, обеспечивающие более эффективную подводную акустическую связь [4].

Мультиплексирование с ортогональным частотным разделением (OFDM) широко использовалось в подводной акустической связи

для достижения высоких скоростей передачи данных даже без сложных эквалайзеров. Но, несмотря на невероятные технологические достижения, подводная акустическая связь по-прежнему не лишена различных недостатков. Это связано с тем, что подводная среда вносит большие искажения. Поэтому система, предназначенная для одних условий, не может быть использована при других.

Кроме того, эти волны характеризуются тремя основными факторами: частотно-зависимым затуханием, многолучевым распространением и большой задержкой. При этом задержка может составлять от 10 до 100 мс. Эти значения задержки приводят к межсимвольным помехам, которые могут превышать 20–300 символов при скорости передачи данных 2–10 кБод и тем самым, ограничивать скорость передачи данных [2].

Радиоволны

Использование радиочастотных волн под водой было направлено для повышения скорости передачи данных, что обеспечивает высокую пропускную способность. В зависимости от архитектуры системного проектирования частота радиоволн может варьироваться от нескольких десятков Гц до ГГц. Электромагнитные волны на низких частотах (30–300 Гц) широко используются в военных целях или при установлении связи между наземными и подводными объектами. Системы подводной радиосвязи на большие расстояния предназначены для связи с подводными лодками. Первый проект, в котором применялись низкие частоты, был разработан в 1968 году для общения между подводными лодками. В этом проекте система оповещения, с высокой пропускной способностью, была использована для вызова подводной лодки к поверхности. Использовалась наземная радиолиния.

Радиоволны в диапазоне МГц способны распространяться в морской воде на расстоянии до 100 м с использованием дипольного излучения с высокой мощностью передачи порядка 100 Вт. Для этого требуется сложная конструкция антенны и высокая мощность передачи.

Система, которая включает в себя связь между подводным и наземным приемопередатчиком, работает эффективно в диапазоне частот от МГц до ГГц. Такая система связи, схема которой показана на рис. 1*а* (см. ниже), называется плавучей системой радиосвязи. Другой вариант системы включает в себя прямой канал радиосвязи между двумя приемопередатчиками, установленными под водой, или одним, установленным под водой, и вторым, установленным в воздухе. Этот тип системы называется системой с прямой видимостью и представлен на рис. 1*б* [4].

Оптические волны

Поскольку радиоволны требуют использования антенн большого размера, большую мощность передатчика в пресной воде и имеют большое затухание в морской воде, следующим очевидным выбором для подводной связи стало использование оптического излучения. Оптическое излучение имеет высокую частоту, поэтому скорость передачи по оптическому каналу может превышать несколько Гбит/с на расстояние нескольких сотен метров. Однако, оптическая связь в подводной среде сталкивается с несколькими проблемами из-за поглощения воды или рассеяния, вызванного взвешенными частицами или из-за дополнительного возмущения, вызванного солнцем [3].

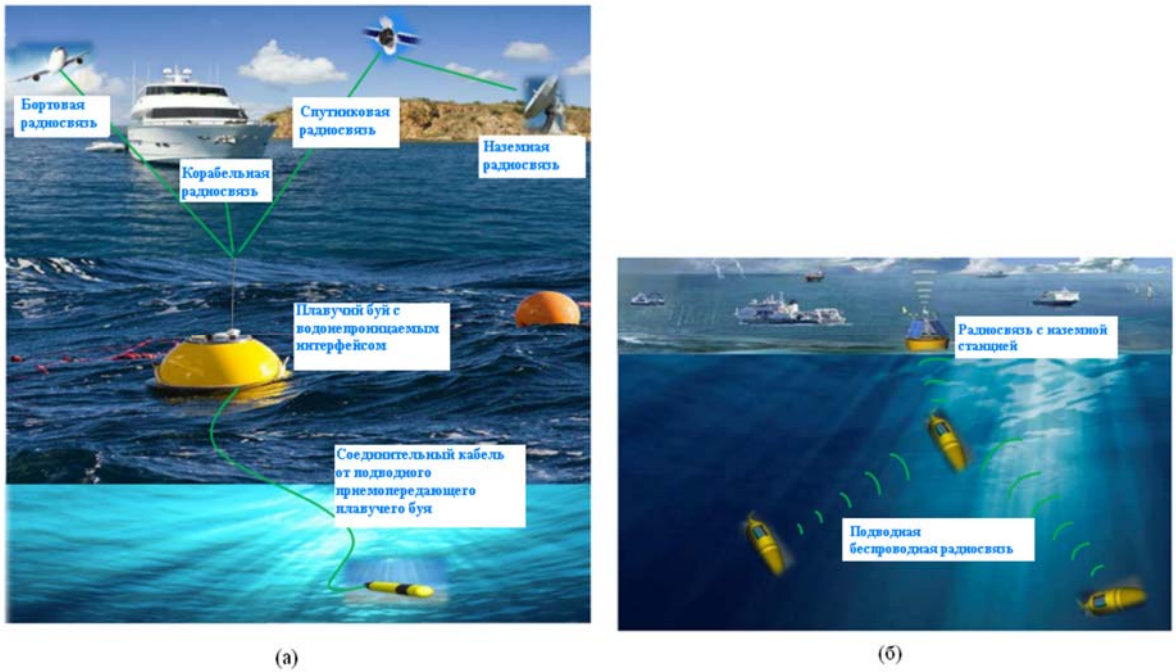


Рис. 1. Подводные системы радиосвязи: а) плавучая система радиосвязи; б) система радиосвязи с прямой видимостью [4]

Рассмотрим некоторые закономерности распространения оптического излучения на границе атмосферы и воды. Скорость распространения оптического излучения в водной среде на 25 % ниже, чем в атмосфере. При прохождении границы двух сред компоненты оптического излучения на разных длинах волн преломляется по-разному. Поэтому, когда свет падает на поверхность воды, волны одной длины преломляются, а другой – отражаются. Количество преломлённого на поверхности воды света зависит от угла падения лучей, состояния водной поверхности и степени рассеянности света.

На рис. 2 показаны процессы взаимодействия солнечных лучей с водой. Находясь в зените, солнечные лучи падают на воду под углом 90 градусов. При этом лишь около 3 % лучей отражаются, остальные проникают в толщу

воды. Лучи, падающие под углом, почти полностью отражаются от спокойной поверхности воды. Волнения поверхности воды приводят к изменению углов падения солнечных лучей.

При проникновении света в воду наблюдается последовательное отфильтровывание волн разной длины. Первыми исчезают волны красного цвета, далее волны оранжевого и желтого цветов, затем зеленого цвета, и самые последние – волны синего цвета. Дальность распространения различных компонентов света в воде представлена на рис. 3 [2].

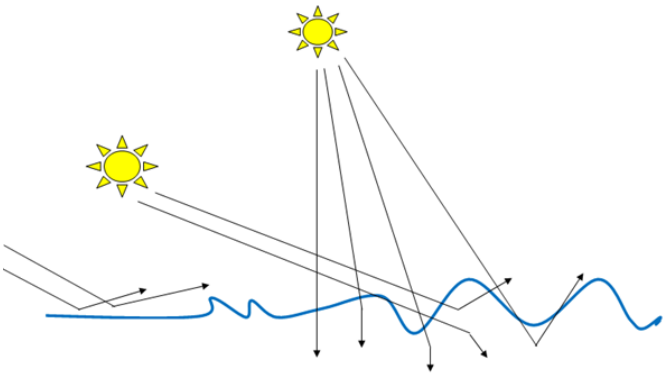


Рис. 2. Взаимодействие солнечных лучей с поверхностью воды

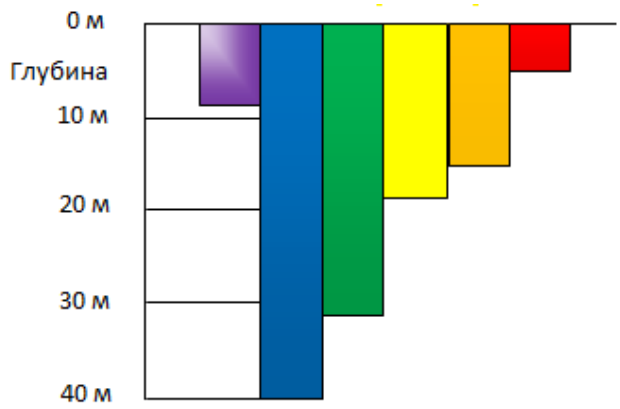


Рис. 3. Дальность распространения оптического излучения в воде

В данной статье были рассмотрены акустические волны, радиоволны и оптическое излучение. Были проведены их сравнения и выявлено, что подводная оптическая связь становится более перспективной в связи с тем, что возможно создать канал высокоскоростной связи, имеющий высокую надежность и помехозащищенность. Предпочтительнее выбирать лазеры, генерирующие излучение в сине-зеленой области спектра (0,42–0,53 мкм) из-за меньшего ослабления этих длин волн в толще воды.

Список используемых источников

1. Shlomi Arnon. Underwater optical wireless communication network. Journal of optical engineering, january 2010. 110 p.

2. Кириллов С. Н., Балюк С. А., Кузнецов С. Н., Есенин А.С. Разработка модели распространения оптического сигнала в водной среде для подводных систем передачи информации // Вестник РГРТУ. 2012. № 2 (вып. 40). С. 3–8.

3. Кузнецов С., Огнев Б., Поляков С. Система оптической связи в водной среде // Первая миля. 2014. № 2 (41). С. 46–51.

4. Kaushal, Hemani & Kaddoum, Georges. (2016). Underwater Optical Wireless Communication. IEEE Access. 4. 1518–1547. 10.1109/ACCESS.2016.2552538.A.

УДК 621.391.82
ГРНТИ 47.05.09

ОБЩИЕ ПОНЯТИЯ АДАПТИВНОЙ СИСТЕМЫ РАДИОСВЯЗИ

С. С. Абрамов, Е. С. Абрамова, И. И. Павлов, М. С. Павлова

Сибирский государственный университет телекоммуникации и информатики

Защита систем связи различного назначения от радиопомех представляет собой одну из важнейших задач, возникающих как при разработке, так и при практическом использовании радиотехнических устройств. Решение проблемы априорной неопределенности помеховой обстановки в каналах радиосвязи в настоящее время осуществляется по нескольким направлениям. Одно из направлений можно условно назвать адаптивным, оно состоит в подстройке структуры и параметров системы при изменении условий ее функционирования.

адаптация, радиосвязь, помехоустойчивость, сигнал, адаптивная система.

Адаптация представляет собой процесс целенаправленного изменения параметров, структуры или свойств системы на основе сбора информации в процессе выполнения основных задач, с целью достижения оптимального функционирования при изменяющихся условиях [1]. В общем случае адаптивная система представляет собой замкнутый контур, содержащий объект управления, устройство контроля, решающее устройство и устройство управления (рис. 1).

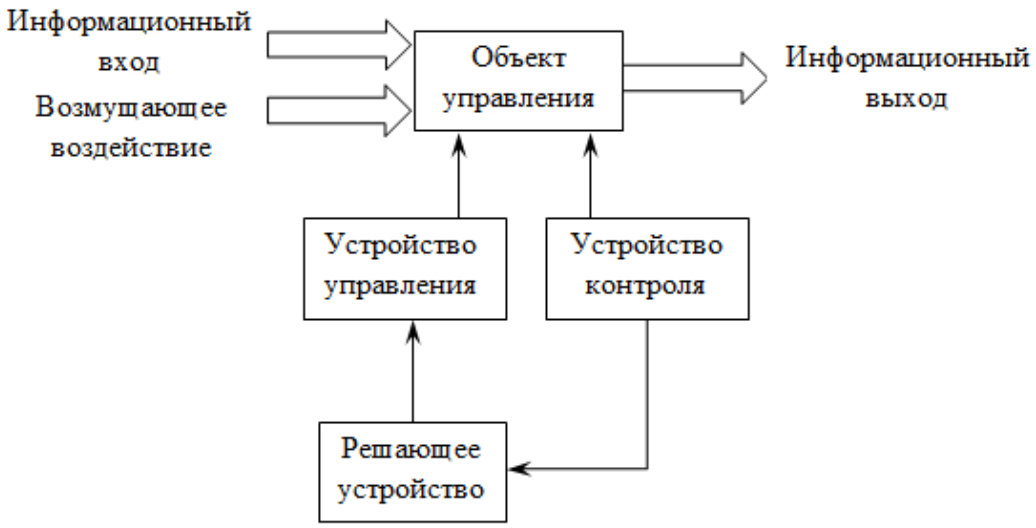


Рис. 1. Адаптивная система с управлением

В системах передачи информации адаптация обычно производится с целью обеспечения наибольшей помехоустойчивости канала связи или его пропускной способности. Общепринятое определение адаптивной радиолинии состоит в том, что при априорно неизвестном изменении параметров радиоканала за счет изменения структуры или параметров его отдельных элементов функционирование радиолинии поддерживается с требуемыми качественными показателями. При этом адаптация возможна на любом из этапов преобразования дискретных сообщений: кодирование-декодирование, модуляция-демодуляция. Характерной особенностью адаптивных алгоритмов приема является наличие в них процедуры обучения, с помощью которой недостающая априорная информация о характеристиках радиоканала заменяется моделью помеховой обстановки в канале. В результате обучения по сигналу на входе приемника, в общем случае, формируются оценки неизвестных функций распределения и их параметров для всех помех. Сертифицированная модель помеховой обстановки в радиоканале используется в дальнейшем для оптимальной обработки принимаемого сигнала на интервале принятия решения. Адаптивные алгоритмы приема достигают требуемых качественных показателей только по истечении определенного времени обучения, они зависят от стационарности характеристик помеховой обстановки и поэтому в большинстве своем являются асимптотически оптимальными.

Применение принципов адаптации в процессе ее функционирования требует осуществления контроля прохождения информации через отдельные узлы системы. Контроль прохождения информации может осуществляться в передатчике УЗО и в приемных устройствах АПД.

На рис. 2 (см. ниже) схематично показаны устройства, в которых может производится контроль прохождения информации, и соответствующие процедуры, выполняемые в результате этого контроля.

В наиболее распространенном варианте построения адаптивных систем передачи информации результаты контроля во второй решающей схеме приемника сообщаются на передающую сторону с целью введения дополнительной избыточности за счет повторной дачи сообщения, принятого с ошибкой. Результаты контроля в приемнике могут быть использованы и для перестройки кодирующего и декодирующего устройств системы связи.

По результатам контроля качества сигнала в первой решающей схеме приемника может осуществляться перестройка характеристик передатчика (мощности и частоты настройки) и радиоприемника (частоты настройки и включения в него соответствующих блоков защиты от различных типов помех). Можно существенно повысить эффективность приема за счет перестройки характеристик канала связи, если использовать результаты контроля качества сигналов в решающих схемах приемника для изменения

структурных характеристик, передаваемых сигналов. Обычно для этого используют обратный канал связи.

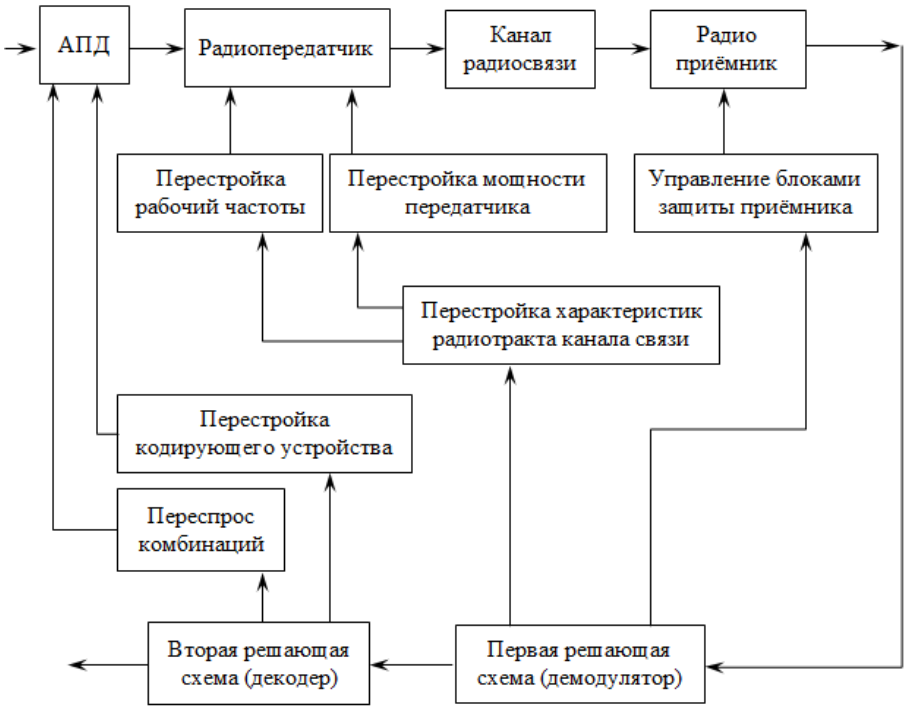


Рис. 2 Структурная схема адаптивной системы радиосвязи

Далее будут рассматриваться способы адаптивной обработки сигналов при использовании результатов контроля качества сигналов преимущественно в первой решающей схеме приемного устройства с целью подавления воздействующих на него помех. Такой подход является традиционным при исследовании поэлементного приема. Для понимания принципов адаптивного подавления различных типов помех в каналах связи необходимо знать структуру воздействующих помех и принимаемых сигналов. Поэтому в данном разделе рассмотрим некоторые основные сведения о сигналах и помеховой обстановке в каналах радиосвязи.

В настоящее время все более широкое распространение получают цифровые методы передачи информации, которые имеют существенные преимущества по сравнению с аналоговыми. Эти преимущества заключаются в более высокой помехозащищенности, возможности регенерации сигнала в пунктах переприема, а также в большей эффективности использования пропускной способности канала связи. При использовании цифровых систем передачи информации сообщение (кодовая комбинация) состоит из N элементов, в которых модулируемый параметр v_l может принимать q_0 значений (q_0 –основание кода). Эта кодовая комбинация может включать M информационных элементов и K избыточных, служащих для обнаружения и исправления возникающих ошибок.

Сигналом называется изменяющаяся физическая величина, отображающая какое-либо сообщение. Сигнал S является функцией времени *t* и записывается в виде $S = S(t)$. Множество сигналов $S(t)$, определенное единым правилом формирования создает систему сигналов. При построении системы связи правило формирования сигналов априорно задано, т. е. система сигналов определена. Объем системы сигналов *R* определяется числом сигналов в системе:

$$r = \overline{1, R}.$$

Для передачи по каналам радиосвязи используются финитные сигналы, т.е . сигналы одинаковой и конечной длительности *T*. Наиболее распространенная модель сигналов, применяемая при синтезе и анализе алгоритмов приема цифровых систем связи, представляется в следующем виде [2]:

$$S(t) = \sum_{r=1}^{R} S_r(t, \lambda, \vartheta), \qquad (1)$$

где $S_r(t, \lambda, \vartheta) = S_r \exp\{-jw(t-\tau) - j\vartheta_r - j\varphi\}$ – детерминированная, интегрируемая в квадрате функция, определяющая структуру *r*-го варианта передаваемого сигнала; $\lambda = [S, \tau, \varphi]$ – вектор непрерывных параметров сигнала, определяемый амплитудой *S*, временем действия τ и фазой сигнала φ; ω – частота несущего колебания.

При ограниченной ширине полосы пропускания канала связи элементы сигнала $S_r(t, \lambda, \vartheta)$ растягиваются во времени, что приводит к наложению их друг на друга, т. е. к появлению межсимвольных помех. С точки зрения математического описания радиосигналы как узкополосных, так и широкополосных систем связи по своему характеру представляются узкополосными процессами, т. е. они удовлетворяют условию:

$$F_r \ll f_{0r},$$

где f_{0r} – некоторая средняя частота энергетического спектра сигнала; F_r – условная полоса частот, в которой сосредоточена основная энергия сигнала.

В этом смысле полезный сигнал, в точке приема, всегда может быть представлен в виде квазидетерминированной модели:

$$S_r(t) = A_r(t)\cos[\omega_0 t + \varphi_r(t)],$$

где $A_r(t)$ – огибающая, ω_0 – несущая частота, а $\varphi_r(t)$ – медленно меняющаяся часть фазы *r*-го варианта сигнала.

Как правило, ω_0 не зависит от номера сигнала и постоянна для рассматриваемой системы сигналов. Представлению (1) соответствует модель радиосигнала, у которого все параметры известны в детерминированном или статистическом смысле. Сигнал вида (1) может быть представлен и в квадратурной форме:

$$S_r(t) = \mu_{c_r}(t)\cos\omega_0 t + \mu_{s_r}(t)\sin\omega_0 t,$$

где $\mu_{c_r}(t)$ и $\mu_{s_r}(t)$ квадратурные и сопряженные по Гильберту коэффициенты передачи канала связи для *r*-го варианта сигнала.

$$A_r(t) = \sqrt{\mu_{c_r}{}^2(t) + \mu_{s_r}{}^2(t)};$$

$$\varphi_r(t) = \operatorname{arctg}\frac{\mu_{cr}}{\mu_{s_r}}.$$

Представленная модель полезных сигналов охватывает практически все системы связи, как узкополосные, так и широкополосные, в том числе и многоканальный разнесенный прием. Таким образом, в общем случае, сигнал, несущий полезную информацию, может быть записан в следующем вице:

$$S(t) = \{\sum_{r=1}^{m} S_{r_q}(t, \lambda, \vartheta)\}_{q=1,2,\dots Q},$$

где q – число ветвей разнесения, λ – множество неизвестных параметров сигнала в q-й ветви разнесения.

Список используемых источников

1. Лосев Ю. И. Адаптивная компенсация помех в каналах связи. М. : Радио и связь, 1988. 208 с.

2. Сикарев А. А., Фалько А. И. Оптимальный прием дискретных сообщений. М. : Связь, 1978. 328 с.

УДК 004.05
ГРНТИ 20.15.05

СРАВНИТЕЛЬНЫЙ АНАЛИЗ КОНЦЕПЦИИ ОБЛАЧНОЙ ИНФРАСТРУКТУРЫ OPENSTACK И ТРАДИЦИОННОЙ АРХИТЕКТУРЫ ВИРТУАЛИЗАЦИИ

М. Л. Авдеева, И. А. Ушаков, А. А. Филиппов

Санкт-Петербургский государственный университет телекоммуникаций им. проф. М. А. Бонч-Бруевича

В современном мире все большую популярность набирают облачные вычисления. Пользователям уже нет необходимости задаваться вопросами: Как обработать дан-

ные? Где их обработать? Когда? В данной статье будет произведено сравнение решений на основе традиционной архитектуры виртуализации, а также инфраструктуры на основе открытого исходного кода – OpenStack.

облачные технологии, cloud computing, OpenStack, VMware vSphere, IaaS, технологии виртуализации.

Облачные вычисления – технология при использовании которой обеспечивается комфортный сетевой доступ по запросу к некоторому общему набору информационных вычислительных ресурсов. Таких, как сети передачи данных, серверы, устройства хранения данных, приложения и сервисы – как вместе, так и по отдельности, которые могут быть незамедлительно предоставлены и освобождены с минимальными затратами на эксплуатацию или обращениями к провайдеру [1].

Модели построения облачных инфраструктур подразделяют на 4 категории:

1. Частное облако – инфраструктура, доступная ограниченному кругу лиц или одной организации.
2. Публичное облако – инфраструктура для использования широкой публикой.
3. Общественное облако – вид инфраструктуры для использования конкретным обществом потребителей из организаций с общими целями.
4. Гибридное облако – комбинация из двух и более облачных инфраструктур.

В свою очередь модели обслуживания, по которым конечным пользователям предоставляются услуги, разделяются на 3 вида (рис. 1):

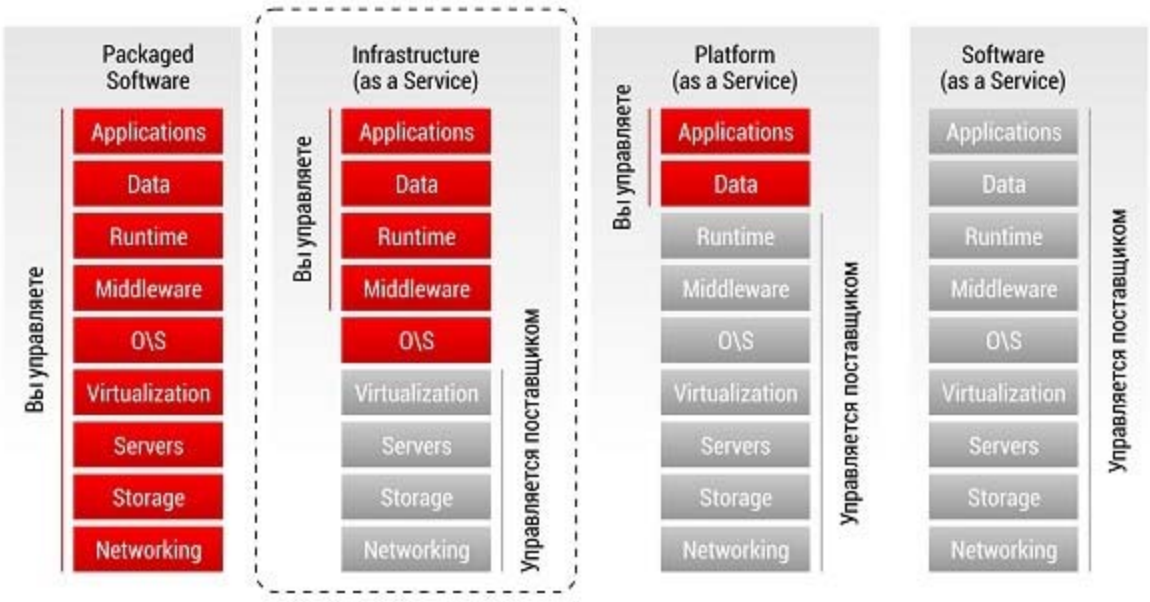


Рис. 1. Типы облачных инфраструктур

1. Инфраструктура как сервис (IaaS) – вычислительная инфраструктура, которая предоставляет информационно-технологические ресурсы для запуска собственных программных решений.

2. Платформа как сервис (PaaS) – набор сервисов и инструментов для разработки и запуска облачных приложений.

3. Программное обеспечение как сервис (SaaS) – модель обслуживания, при которой клиентам предоставляется готовое программное обеспечение, полностью обслуживаемое провайдером.

OpenStack – комплекс ПО, реализующий функции облачной инфраструктуры. Он позволяет манипулировать наборами различных ресурсов по типу IaaS. OpenStack взаимодействует с основной инфраструктурой через открытые или предоставляемые вендорами драйверы, что в свою очередь помогает избежать привязки клиента к конкретному вендору, технологии или инструменту.

OpenStack реализует концепцию программно-определяемого центра обработки данных (SDDC), предоставляя простой и стандартизированный доступ к различным вычислительным ресурсам, сетям данных, СХД и дополнительным функциям [2]:

1. Балансировка нагрузки (LBaaS).

2. Защита периметра (FaaS).

3. Объектное хранение данных.

Основные преимущества OpenStack заключаются в том, что это открытая платформа, которая позволяет создавать облака с любым необходимым количеством сервисов и почти неограниченной масштабируемостью [3]. OpenStack – эффективный способ объединить, унифицировать и виртуализировать целую инфраструктуру и предоставить ее в виде сервисов.

Для того, чтобы понять различия между облаком OpenStack и традиционной архитектуры необходимо определить разницу в их дизайнах.

Инфраструктуры, которые строятся на традиционных технологиях виртуализации, таких как платформа VMware vSphere [4] (или аналоги, например, *Hyper-V* или *Red Hat Enterprise Virtualization*) предлагают консолидировать серверы разных размеров, но более ориентированы на хостинг небольшого количества, в сравнении с облаком, довольно крупных виртуальных машин, потому что, как правило, большинство серверов приложений имеют монолитную архитектуру (*Oracle, Microsoft Exchange*) и каждый экземпляр такого типа находится на одной ВМ и растет за счет расширения на одном физическом сервере, который работает под управлением гипервизора.

Для того, чтобы обеспечить надежную работу этих приложений в традиционных системах предлагается запускать сервера приложений в, так называемых, кластерах/доменах с использованием функций повышения отказоустойчивости [5], например, VMware HA и VMware vMotion (рис. 2).

Эти решения работают при достаточных условиях, таких, как наличие высокой пропускной способности сети или разделяемой системы хранения данных, что в свою очередь, накладывает сложности, связанные с масштабированием.

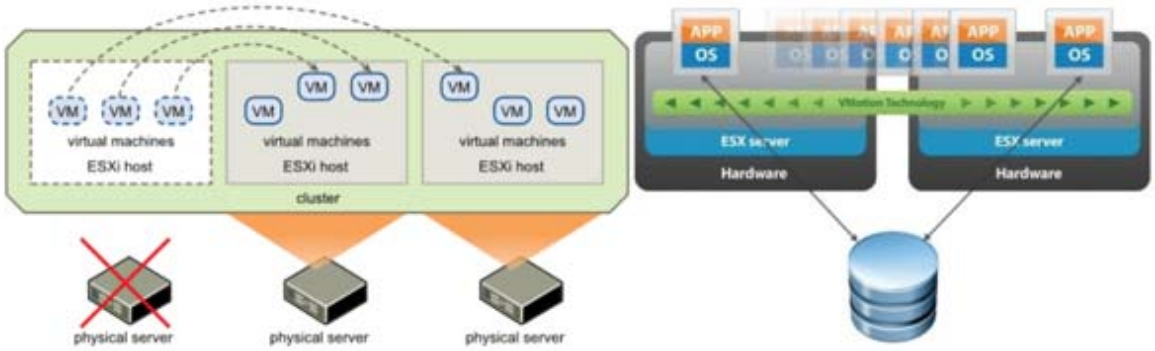


Рис. 2. Реализации высокой доступности на примере VMware vSphere (HA и *vMotion*)

Облачные инфраструктуры, наподобие OpenStack, предназначены для работы с приложениями, спроектированными для горизонтального масштабирования (например, *MongoDB, Hadoop* или *Apache Cassandra*) и устойчивы к падению виртуальных машин [6]. Ресурсы в такой системе расширяются за счет добавления новых экземпляров приложений на одинаковых виртуальных серверах с балансировкой нагрузки. Таким образом приложения самостоятельно обеспечивают собственную отказоустойчивость на уровне приложения, независимо от основной инфраструктуры и функций гипервизора (табл., см. ниже).

Выводя отказоустойчивость на уровень приложения, облачная платформа позволяет отказаться от специализированного, дорогостоящего оборудования (СХД, сервера и т. п.).

Рассматривая любое достаточно крупное технологическое решение следует иметь четкое представление о том, что могут предложить эти решения и какими возможностями они обладают. Анализируя облачную архитектуру OpenStack, необходимо понимать, что данная архитектура подходит для высокомасштабируемых приложений следующего поколения, где отказ всегда ожидаем, но компенсируется наличием большого количества однотипных экземпляров приложения, а традиционная – наоборот, направлена на избежание любого рода неисправностей или выхода из строя, тем самым поддерживая непрерывную работу крупного монолитного приложения [8, 9].

Исходя из этого следует сделать вывод, что не стоит рассматривать эти типы облачных архитектур как конкурирующие решения, так как каждое из них обладает определенной спецификой и в рамках отдельной задачи необходимо принимать решение в зависимости от требований. Таким обра-

зом, для реализации инфраструктуры внутри компании облачная технология OpenStack позволяет создать облако, избегая издержек на дорогостоящее оборудование и временных затрат, которое требуется для реализации традиционной архитектуры. Необходимо отметить, что также часто используются гибридные системы, использующие преимущества обоих решений.

ТАБЛИЦА. Краткое сравнение концепции облака OpenStack и традиционной архитектуры виртуализации

Параметры	Традиционная виртуализация	Облачные ВМ [7]
Средний тип сервера	Крупная stateful ВМ	Небольшая stateless ВМ
Размещение приложения	1 приложение на 1 виртуальную машину	1 приложение на многих виртуальных машинах
Средняя продолжительность жизни	Несколько лет	Месяцы, недели, дни
Метод масштабирования приложения	Вертикальное масштабирование (увеличение производительности ВМ)	Горизонтальное масштабирование (увеличение количества ВМ)
Реагирование на выход из строя виртуальной машины	При отказе ВМ, выходит из строя и приложение. Необходимо обеспечить отказоустойчивость	В случае сбоя ВМ она удаляется, а затем создается новая ВМ
Способ обеспечения отказоустойчивости	SLA требует обеспечения доступности приложения со стороны инфраструктуры (Live Migration, High Availability, Fault Tolerance и аналогов)	SLA требует возможности удаления/добавления экземпляров виртуальных машин для поддержания доступности приложения

Примечание: SLA (Service Level Agreement) – соглашение об уровне услуг.

Список используемых источников

1. Программно-определяемый ЦОД: зачем это нужно в практике сисадмина [Электронный ресурс]. URL: https://habr.com/ru/company/croc/blog/278929/ (дата обращения 25.02.2020).

2. V. K. Cody Bumgardner, Jay Pipes, OpenStack in Action, 2016.

3. Облако OpenStack: мифы и реальность [Электронный ресурс]. URL: https://habr.com/ru/company/jetinfosystems/blog/247087/ (дата обращения 01.03.2020).

4. VMware cloud foundation: the simplest path to the hybrid cloud [Электронный ресурс] URL: https://www.vmware.com/content/dam/digitalmarketing/vmware/en/pdf/ whitepaper/products/vmware-cloud-foundation-whitepaper.pdf (дата обращения 05.03.2020).

5. Andrea Mauro, Paolo Valsecchi, Karel Novak, Mastering VMware vSphere 6.5, 2016.

6. Tom Filfield, Diane Fleming, Anne Gentle, Lorin Hochstein, Jonathan Proulx, Everett Toews, Joe Topjian, OpenStack Operations Guide, 2014.

7. Преимущества облака OpenStack [Электронный ресурс] URL: https://habr.com/ru/company/icl_services/blog/280428/ (дата обращения 18.03.2020).

8. Чмутов М. В., Ковцур М. М., Ушаков И. А., Пестов И. А. О действующей инфраструктуры организации для последующего перехода к облачной архитектуре // Информационная безопасность регионов России (ИБРР-2017): материалы конференции. 2017. С. 535–537.

9. Shterenberg S. I., Poltavtseva M. A. A distributed intrusion detection system with protection from an internal intruder // Automatic Control and Computer Sciences. 2018. Т. 52. No 8. PP. 945–953.

Статья представлена заведующим кафедрой ЗСС СПбГУТ, кандидатом технических наук, доцентом А. В. Красовым.

УДК 004.654
ГРНТИ 20.53.17

АРХИТЕКТУРА СИСТЕМЫ ВЕРИФИКАЦИИ ПОЛИТИК РАЗГРАНИЧЕНИЯ ДОСТУПА К ИНФОРМАЦИИ В ОБЛАЧНЫХ ИНФРАСТРУКТУРАХ

С. А. Агеев, Д. С. Левшун, И. Б. Саенко

Санкт-Петербургский институт информатики и автоматизации Российской академии наук

Рассматривается архитектура системы верификации политик разграничения доступа к информации в облачных инфраструктурах, ориентированная на модель контроля доступа ABAC и инструментальное средство верификации UPPAAL. Определен состав модулей в предложенной архитектуре. Проведены результаты реализации архитектуры в конкретной предметной области.

верификация, политика, разграничение доступа, облачная инфраструктура

Облачные инфраструктуры лежат в основе как больших информационных систем коллективного пользования, так и многих киберфизических систем (умный город, умный дом, автоматизированное производство, робототехника и т. д.) [1, 2]. Однако заинтересованность злоумышленников в критически важных данных подобных систем обуславливает постоянный рост числа атак на них. Одним из способов противодействия злоумышленникам такого рода и, следовательно, обеспечения компьютерной и сетевой безопасности в облачных инфраструктурах является разграничение доступа, которое предполагает, что пользователи должны обладать разными

полномочиями по выполнению различных действий над информационными ресурсами [3]. Поэтому исследования по решению задач разграничения доступа, включая верификацию политик разграничения доступа к информации, являются достаточно актуальными.

Для решения задач разграничения доступа в этих системах разработано несколько моделей контроля доступа, которые считаются традиционными. Такими моделями являются: дискреционное управление доступом (*Discretionary Access Control*, DAC), мандатное управление доступом (*Mandatory Access Control*, MAC), а также управление доступом на основе ролей (*Role-Based Access Control*, RBAC) [4]. Однако опыт использования традиционных моделей контроля доступа показал, что в условиях высокой динамики изменения требуемых полномочий, возникающих при изменении характеристик (атрибутов) пользователей, ресурсов или среды, данные модели становятся неэффективными. Возникает потребность в использовании новых, более гибких моделей контроля доступа. Одной из таких достаточно гибких моделей контроля доступа, которая появилась сравнительно недавно и считается наиболее приемлемой для облачных инфраструктур, является модель разграничения доступа на основе атрибутов (*Attribute-Based Access Control*, ABAC) [5].

Модель ABAC может успешно заменить традиционные модели контроля доступа [6]. Разрешение на выполнение тех или иных действий над ресурсами (объектами) в этой модели выдается на основании проверки корректности выполнения множества логических условий (правил), которые определяют используемую политику контроля доступа. Правила формируются в виде логических выражений, в которых используются значения атрибутов. Все множество атрибутов состоит из трех групп: атрибутов пользователей (субъектов), атрибутов ресурсов (объектов) и атрибутов компьютерного окружения. К последней группе относится время. По этой причине ABAC модель является более гибкой, чем другие модели контроля доступа, и способной быстро реагировать на изменения.

Однако, в отличие от традиционных моделей DAC, MAC и RBAC, модель ABAC еще во многом находится на исследовательском уровне. Многие вопросы, касающиеся разработки и использования политик на основе модели ABAC, еще не до конца исследованы. Поэтому разработчики средств защиты еще не перешли к широкому внедрению этой модели в своих продуктах. Одним из таких проблемных вопросов является верификация политик, основанных на ABAC. Задачами верификации ABAC политик является нахождение противоречий в правилах контроля доступа и способов устранения этих противоречий.

В настоящей работе исследуется возможность применения для верификации ABAC политик подхода на основе метода «проверки на модели» (*Model Checking*) и предлагается архитектура системы верификации

политик разграничения доступа к информации в облачных инфраструктурах, ориентированная на модель ABAC. Метод «проверки на модели» осуществляется с использованием темпоральной логики и ориентирован на анализ множества возможных состояний логической системы. Для практической реализации разработано множество программных средств, которые нашли успешное применение при решении задач верификации во многих сценариях. Однако для верификации политик ABAC данный метод еще не исследовался.

Суть метода «проверки на модели» применительно к модели ABAC и основанной на нем процедуры верификации политик разграничения доступа к информации заключается в следующем.

Пусть даны множество пользователей (U), ресурсов (R) и операций (O), которые пользователи могут выполнять над ресурсами. Атрибуты разделяются на два типа: для пользователей (A_u) и ресурсов (A_r). Атрибут a пользователя u или ресурса r может принимать пустое значение или значение из своего домена D_a. Это значение обозначается с помощью отношений $a(u)$ или $a(r)$. Правило политики $p = <e; o>$ в модели ABAC задается выражением, которое определяет условие применимости (e) и выполняемое действие (o).

Продемонстрируем это на следующем примере. Пусть атрибут пользователя A_u имеет имя «Отдел» – «*Department*» ($A_u = Department$) и атрибут ресурса A_r имеет имя «Владелец» – «*Owner*» ($A_r = Owner$). Пользователь u может выполнять над ресурсом r действие $o = read$, если выполняется одно из двух условий: либо пользователь u работает в отделе управления («*Management*»), либо он является владельцем ресурса r. Формальное представление этого правила имеет следующий вид:

$$p = < A_u = Management \text{ OR } A_r = u; read\ (u, r) >,$$

где $read\ (u, r)$ – операция чтения, выполняемая пользователем u над ресурсом r.

Процедура верификации политик разграничения доступа включает в себя следующие этапы [7]:

1) построение модели информационной системы (множества информационных ресурсов) во внутреннем формате системы верификации в виде конечного автомата;

2) построение спецификации на проверяемую систему, задающей свойства корректности на языке темпоральной логики;

3) вычисление модели с помощью программного средства;

4) обработка результатов верификации и построенных контрольных примеров, показывающих, каким образом система может перейти в некорректное состояние;

5) сравнение и оценка результатов верификации в соответствии с требованиями к их эффективности.

Рассмотренное содержание процедуры верификации политик разграничения доступа к информации позволяет обосновать следующую архитектуру системы, реализующую этот процесс для облачной инфраструктуры. В самом общем виде она должна состоять из следующих модулей (см. рис. ниже):

1) модуль описания модели информационной системы;
2) модуль описания политик разграничения доступа;
3) модуль проверки модели информационной системы;
4) модуль обработки результатов на контрольных примерах;
5) модуль оценки результатов.

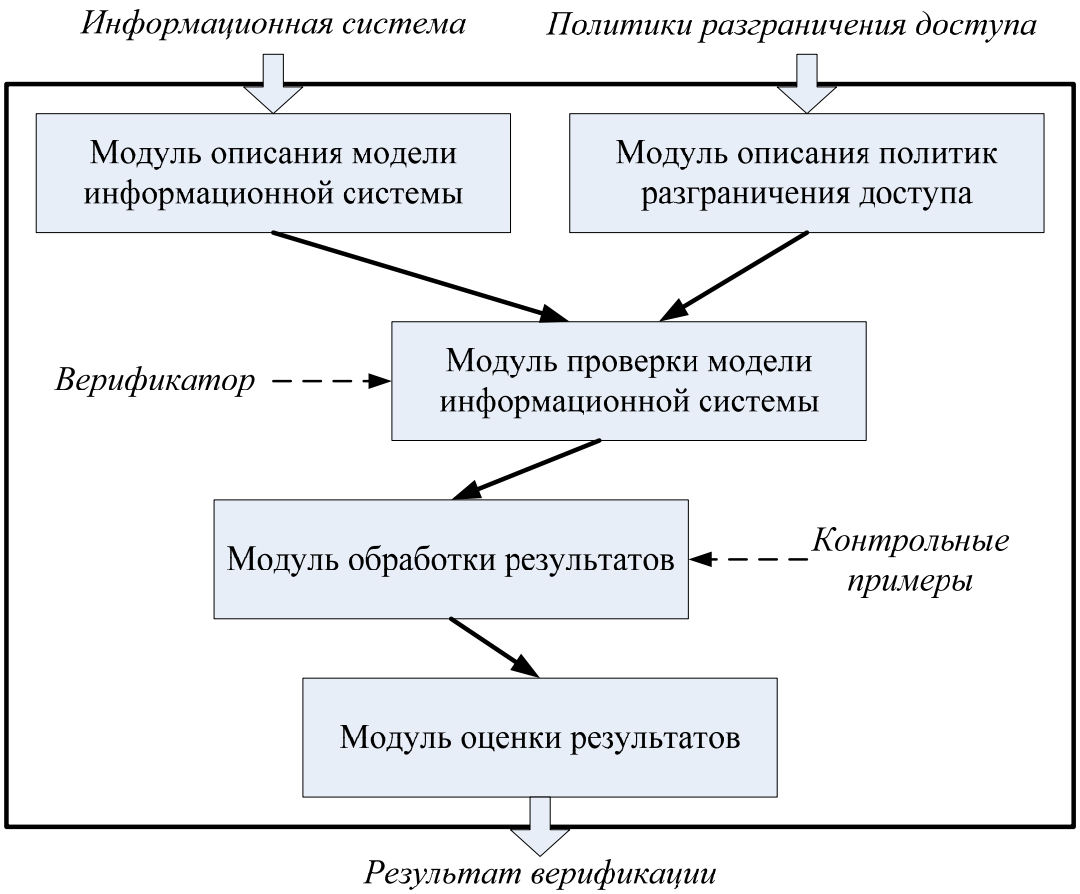


Рис. Обобщенная архитектура системы верификации политик разграничения доступа в облачных инфраструктурах

В *модуле описания модели информационной системы* при использовании метода верификации «проверка на модели» используется, как правило, модель Крипке [8]. Она состоит из множества состояний, множества переходов между состояниями и функции, которая помечает каждое состояние набором свойств, истинных в этом состоянии. На вход этого модуля поступает описание информационных ресурсов.

Модуль описания политик разграничения доступа содержит формальные описания этих политик, которые выполнены, как правило, на языке темпоральной логики. Описания политик разграничения доступа поступают на вход этого модуля.

Модуль проверки модели информационной системы, как правило, использует функциональные возможности специального программного средства (*Верификатора*), который проверяет модель на наличие или отсутствие противоречий. В качестве *Верификатора* в настоящее время могут выступать различные программные средства. Наиболее популярными являются SPIN, UPPAAL, Rabbit и другие.

Модуль обработки результатов осуществляет выявление «узких мест» в модели информационной системы, используя для этого контрольные примеры. Под «узкими местами» модели понимаются те ее элементы и взаимосвязи, которые могут способствовать переходу модели в некорректное состояние.

Модуль оценки результатов осуществляет финальную оценку результатов верификации, обеспечивая вычисление показателей эффективности верификации. Как правило, состав показателей эффективности и процедура их вычисления обусловливаются функциональными возможностями *Верификатора*.

Предложенная архитектура в настоящей работе была реализована с использованием верификатора UPPAAL. В качестве предметной области было выбрано описание информационных ресурсов и процессов, характеризующих работу сотрудников организации (пользователей) с конфиденциальными файлами и иерархическую подчиненность этих пользователей. Описание сотрудников и файлов в модели информационной системы было выполнено в виде конечных автоматов. Конечные автоматы для сотрудников содержали пять состояний, а для файлов – четыре. Для верификации политики безопасности были проверены следующие параметры: переход сотрудников между отделами; возможность работы с созданными файлами. Верификация политики безопасности в системе, имеющей предложенную архитектуру, позволила обнаружить в ней недостатки, а также подтвердить, что после ее доработки обнаруженные недостатки устраняются, а новые недостатки отсутствуют.

Таким образом, в настоящей работе представлена архитектура системы верификации политик разграничения доступа к информации в облачных инфраструктурах, ориентированная на модель ABAC и инструментальное средство верификации UPPAAL. На примере конкретной предметной области продемонстрирована дееспособность предложенной архитектуры. В тоже время были выявлены ограничения при работе с политиками боль-

шой размерности и сложности. В ходе дальнейших исследований планируется сделать переход к инструментам, позволяющим верифицировать распределенные модели.

Работа выполнена при частичной финансовой поддержке проекта РФФИ № 18-07-01369 и бюджетной темы 0073-2019-0002.

Список используемых источников

1. Lopez J., Rubio J. E. Access control for cyber-physical systems interconnected to the cloud // Computer Networks. 2018. Vol. 134. PP. 46–54.

2. Котенко И. В., Саенко И. Б., Полубелова О. В. Перспективные системы хранения данных для мониторинга и управления безопасностью информации // Труды СПИИРАН. 2013. № 2 (25). С. 113–134.

3. Котенко И. В., Десницкий В. А., Чечулин А. А. Исследование технологии проектирования безопасных встроенных систем в проекте Европейского сообщества SecFutur // Защита информации. Инсайд. 2011. № 3 (39). С. 68–75.

4. Kotenko I., Saenko I. Improved genetic algorithms for solving the optimisation tasks for design of access control schemes in computer networks // International Journal of Bio-Inspired Computation. 2015.Vol. 7, No. 2. PP. 98–110.

5. Karatas G., Akbulut A. Survey on Access Control Mechanisms in Cloud Computing // Journal of Cyber Security and Mobility. 2018. Vol. 7, № 3. PP. 1–36.

6. Paci F., Squicciarini A., Zannone N. Survey on Access Control for Community-Centered Collaborative Systems // ACM Comput. Surv. 2018. Vol. 51, No. 1. Article 6, 38 pages.

7. Котенко И. В., Левшун Д. С., Саенко И. Б. Верификация политик разграничения доступа на основе атрибутов в облачных инфраструктурах с помощью метода проверки на модели // Системы управления, связи и безопасности. 2019. № 4. С. 421–436.

8. Clarke E. M., Grumberg O., Peled D. Model Checking. MIT Press, 2000.

УДК 654.078
ГРНТИ 49.33.29

СЕТЬ 6G С ПОДДЕРЖКОЙ ИСКУССТВЕННОГО ИНТЕЛЛЕКТА

А. Д. Агеева, Н. В. Бирюкова, В. С. Елагин

Санкт-Петербургский государственный университет телекоммуникаций им. проф. М. А. Бонч-Бруевича

По всему миру постепенно запускается сеть 5G, которая предоставит новую базовую технологию, поддерживающую будущую индустрию и общество, наряду с Искусственным Интеллектом и Интернетом Вещей. Но предполагается, что в связи с экспоненциальным ростом передачи данных, через несколько лет скорости и возможности 5G будет не хватать.

Технологии мобильной связи 6G могут стать прорывной технологией, которая сможет обеспечить скорость до 400 раз выше, чем 5G. Искусственный Интеллект будет играть критически важную роль в разработке и оптимизации архитектуры, протоколов и операций 6G. ИИ сможет предоставить способы реализации поиска знаний, интеллектуального управления ресурсами, автоматической настройки сети и интеллектуального предоставления услуг.

В данном докладе будет рассмотрена связь между сетью 6G и технологией Искусственного Интеллекта, а также использование методов искусственного интеллекта для эффективной и действенной оптимизации производительности сети.

6G, 5G, Artificial Intelligence, AI, Искусственный Интеллект, ИИ, Интернет Вещей, IoT.

В середине 2019 года стало известно, что некоторые крупные технологические компании начали работу над сетями шестого поколения (6G), но в основном исследования больше теоретические. Предполагается, что развёртывание 6G-сетей начнётся не раньше 2030 года [1]. Новая сеть должна не просто обеспечивать связь, а стать своего рода «сенсором, улавливающим изменение окружающей среды» и уметь революционизировать себя, реализовав интеллект для удовлетворения более жестких требований к будущему интеллектуальному информационному обществу, которые включают [2], [3]:

- пиковая скорость передачи данных до 1 Тбит/с;
- сверхнизкая сквозная задержка, менее 1 мс;
- сверхвысокая надежность;
- очень высокая мобильность, до 1000 км/ч;
- массивная связь, до 107 устройств/км^2;
- пропускная способность до 1 Гбит/ м^2;
- широкие полосы частот (например, 1–3 ТГц);
- связанный интеллект с возможностью машинного обучения.

Помимо небывалых скоростей и молниеносного доступа сети 6G должны будут обеспечивать возможность обслуживать гораздо больше конечных устройств, чем нынешние сети и сети 5G. Согласно господствующей концепции, для 6G потребуется сетевая инфраструктура с большим количеством малых сот, которые позволят быстро и с низкими затратами электроэнергии передавать очень большие объемы данных. Между собой такие соты будут соединяться высокоскоростными радиоканалами, использующими высокочастотные диапазоны [4].

Сеть 6G с поддержкой Искусственного Интеллекта

Искусственный интеллект или ИИ (*Artificial Intelligence*, AI) был использован в качестве новой парадигмы для проектирования и оптимизации сетей 6G с высоким уровнем интеллекта. Искусственный интеллект [5], обладающий сильными способностями к обучению, мощными способностями

к рассуждению и интеллектуальными способностями распознавания, позволяет архитектуре сетей 6G обучаться и адаптироваться для поддержки разнообразных услуг соответственно без вмешательства человека.

На рис. представлена архитектура сетей 6G с поддержкой ИИ, состоящая из четырех уровней: сенсорный уровень, уровень интеллектуального анализа данных и аналитики, уровень управления, прикладной уровень. Такая архитектура способна интеллектуально извлекать ценную информацию из массивных данных, изучать и поддерживать различные функции для самоконфигурирования, самооптимизации и самовосстановления в сетях 6G с целью решения задач оптимизированного проектирования физического уровня, принятия сложных решений, работы в сети, задач управления и оптимизации ресурсов [6].

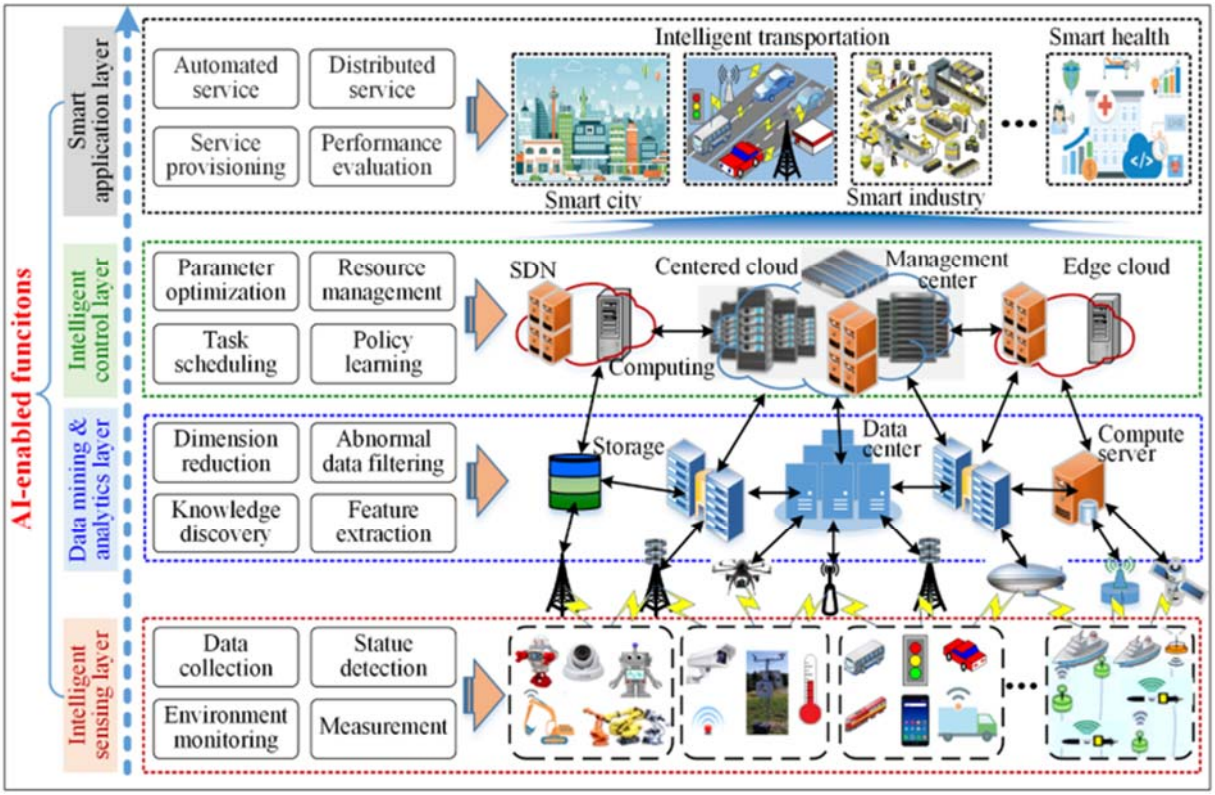


Рис. Архитектура интеллектуальных сетей 6G с поддержкой ИИ

Использование технологии Искусственного Интеллекта для 6G

Беспрецедентное преобразование беспроводных сетей сделает 6G существенно отличным от предыдущих поколений, поскольку оно будет характеризоваться высокой степенью неоднородности во многих аспектах. Кроме того, широкий спектр новых приложений потребует интеллектуального использования ресурсов связи, вычислений, управления и хранения данных от границы сети до ядра, а также для множества радиотехнологий и сетевых платформ. Наконец, объем и разнообразие данных, генерируемых

в беспроводных сетях, значительно растут. Это открывает большие возможности для планирования и эксплуатации сетей, управляемых данными, для достижения аддитивности в реальном времени к динамическим сетевым средам.

1 Аналитика больших данных для 6G

Первое естественное применение Искусственного Интеллекта – аналитика больших данных. Существует 4 типа аналитики, которые могут применяться к системам 6G, а именно: описательная, диагностическая, прогностическая и предписывающая аналитика [7]. Описательная аналитика анализирует исторические данные, чтобы получить представление о производительности сети, профиле трафика, условиях канала и т. д. для повышения осведомленности операторов. Диагностическая аналитика позволяет автономно обнаруживать сбои сети, тем самым повышая надежность и безопасность систем 6G. Прогностическая аналитика использует данные для прогнозирования будущих событий, таких как поведение и предпочтения пользователей, популярность контента и доступность ресурсов. Предписывающая аналитика использует преимущества прогнозов, чтобы предложить варианты решений для распределения ресурсов, виртуализации сети, размещения кэша, периферийных вычислений, автономного управления.

2 Оптимизация с замкнутым контуром с поддержкой ИИ

Традиционные методы оптимизации беспроводной сети могут быть не применимы в системах 6G. Беспроводные системы 6G будут чрезвычайно динамичными и сложными из-за масштаба, плотности и неоднородности сети. Моделирование таких систем очень сложно, если не невозможно.

Проблемы в беспроводных сетях традиционно решаются путем применения наборов правил, полученных из системного анализа с предшествующим знанием предметной области и опытом. Последние достижения в технологиях искусственного интеллекта, такие как обучение с подкреплением и обучение с глубоким подкреплением (DRL), могут создать петлю обратной связи между лицом, принимающим решения, и физической системой, так что лицо, принимающее решение, может итеративно усовершенствовать свое действие на основе обратной связи системы для достижения оптимальности [7].

3 Интеллектуальная беспроводная связь

Технологии Искусственного Интеллекта будут играть решающую роль в сквозной оптимизации всей цепочки обработки сигналов физического уровня, от передатчика до приемника. Сквозная система связи страдает от широкого спектра искажений. Поэтому вместо сквозной оптимизации

применяется метод, где цепочка действий делится на несколько независимых блоков, каждый из которых имеет упрощенную модель, не дающую точного или целостного представления о характеристиках реальных систем.

Технологии искусственного интеллекта открывают возможности для изучения наилучшего способа общения с помощью комбинаций аппаратных и канальных эффектов. Предполагается парадигма «интеллектуального уровня PHY» в 6G, где сквозная система способна к самообучению и самооптимизации благодаря сочетанию передовых методов зондирования и сбора данных, технологий искусственного интеллекта и подходов к обработке сигналов в конкретных областях [7].

Тенденции и проблемы внедрения 6G для приложений с Искусственным Интеллектом

Искусственный Интеллект достиг значительных успехов во многих областях применения. Задачи искусственного интеллекта требуют больших вычислительных ресурсов. Они обучаются, разрабатываются и развертываются в центрах обработки данных со специально разработанными серверами. Учитывая быстрый рост интеллектуальных мобильных гаджетов и устройств Интернета вещей, ожидается, что в ближайшем будущем на границе беспроводных сетей будет развернуто большое количество интеллектуальных приложений.

Беспроводная сеть 6G будет спроектирована таким образом, чтобы использовать передовые технологии с поддержкой ИИ на различных современных мобильных устройствах.

Емкость и задержка беспроводных каналов являются ключевыми узкими местами мобильных приложений ИИ по трем причинам. Во-первых, для защиты конфиденциальности некоторые приложения ИИ требуют хранения данных на мобильных устройствах вместо их загрузки в облако. Это стимулировало исследовательский интерес к федеративному обучению [8], где для обновления моделей необходимы частые коммуникации между вычислительными устройствами. Во-вторых, чтобы преодолеть ограничение ресурсов, распределенные вычисления на устройстве предоставляют новые возможности, объединяя вычислительные ресурсы и ресурсы хранения множества мобильных устройств. В этом случае перестановка данных является ключевым компонентом для обмена вычисленными промежуточными значениями между мобильными устройствами для обеспечения возможности распределенного вывода на устройстве [9]. В-третьих, гетерогенная смесь облачных, периферийных и конечных вычислительных устройств обеспечивает рассеянную вычислительную среду как для обучения, так и для вывода глубоких нейронных сетей. Предполагается, что для

обеспечения повсеместного и диверсифицированного мобильного Искусственно Интеллектуального сервиса 6G предоставит гибкие платформы для разработки передовых технологий связи и вычислений.

Выводы

Развитие технологий связи зависит напрямую от роста трафика. Как уже было сказано, сети 6G должны будут обеспечить возможность обслуживать огромное количество конечных устройств. Использование технологии Искусственного Интеллекта в будущих сетях является ключевым. ИИ может использоваться во всех областях системы радиосвязи и, возможно, при проектировании самого радиоинтерфейса.

В этой статье была представлена архитектура, наделенная полномочиями Искусственного Интеллекта, и методы использования технологии ИИ для сетей 6G. Также в статье были выявлены тенденции и проблемы внедрения 6G для приложений с Искусственным Интеллектом.

Список используемых источников

1. Лебедева В. Мобильной связи готовят смену поколений // Газета «Коммерсантъ». № 185 от 10.10.2019. С. 7.

2. David K., Berndt H. 6G Vision and Requirement // IEEE Vehic. Teh. Mag. PP. 72–80.

3. Zhang Z. et al. 6G Wireless Networks: Vision, Requirements, Architecture, and Key Technologies // IEEE Vehic. Teh. Mag., PP. 28–41.

4. Тыренко А. 6G может перебить аппетит к 5G // Издание CNews Телеком от 15.10.2019.

5. Russel S. J. l and Norvig P. Artificial Intelligence – A Modern Approach. Pearson Education, 2010.

6. Yang H., Alphones A., Xiong Z., Niyato D., Zhao J., Wu K. Senior Member. Artificial Intelligence-Enabled Intelligent 6G Networks // IEEE Access.

7. Letaief K. B., Chen W., Shi Y., Zhang J., Ying-Jun A. Zhang. The Roadmap to 6G – AI Empowered Wireless Networks // IEEE Access, 2019.

8. B. McMahan, E. Moore, D. Ramage, S. Hampson, B. A. y Arcas. Communication-efficient learning of deep networks from decentralized data: in Proc. Int. Conf. Artificial Intell. Stat. (AISTATS). Vol. 54. PP. 1273–1282.

9. Yang K., Shi Y., Ding Z. Low-rank optimization for data shuffling in wireless distributed computing // In Proc. IEEE Int. Conf. Acoustics Speech Signal Process. (ICASSP), Calgary, Alberta, Canada, 2018.

УДК 004.77
ГРНТИ 49.33.29

ПРИМЕНЕНИЕ БЕСПИЛОТНЫХ ЛЕТАТЕЛЬНЫХ АППАРАТОВ В СЕТЯХ 5G

А. А. Х. Алзагир, А. С. А. Мутханна

Санкт-Петербургский государственный университет телекоммуникаций им. проф. М. А. Бонч-Бруевича

Технология 5G будет расследовать задачи, которые включают в себя транспортное средство, беспроводные медицинские услуги, коммунальные приложения и промышленную автоматизацию, услуги виртуальной и дополненной реальности, а также первичные услуги широкополосного доступа. Кроме того, 5G будет учитывать критерии производительности для низкой задержки, высокой скорости, повышенной надежности, пиковой пропускной способности на соединение, спектральной эффективности системы, плотности соединения и емкости, а также низкого энергопотребления. Беспилотный летательный аппарат будет решать задачи с реализацией всех этих приложений. В статье рассматривается примеры использования БПЛА и проблемы реализации в 5G.

беспилотный летательный аппарат, дроны, БПЛА, 5G.

Введение

Развитие технологий сегодня меняет наш мир. Кроме того, это повлияло на беспроводную индустрию, чтобы сделать шаги в направлении будущего поколения сетевых технологий. Ожидается, что появление технологии 5G будет способствовать соединению всего мира универсальной коммуникацией, которая связывает всех и вся во все времена и всеми средствами, независимо от сервиса, устройства, географического существования или сети. Он также будет учитывать критерии производительности для высокой скорости, низкая латентность, повышенной надежности, спектральной эффективности системы, пиковой пропускной способности на соединение, плотности подключения и емкости, а также низкого энергопотребления [1].

Беспилотные летательные аппараты (БПЛА) становятся неотъемлемой частью 5G и, вероятно, будут играть важную роль в дальнейшем функциональном разнообразии 5G связи.

БПЛА были рассмотрены как обнадеживающая новая модель для упрощения трех основных сценариев использования будущих беспроводных сетей, другими словами, сверхширокополосная мобильная связь (eMBB), сверхнадежная межмашинная связь с низкими задержками (URLLC) и мас-

совая межмашинная связь (mMTC). Например, БПЛА может играть центральную роль в обеспечении восстановления сетевых служб в пострадавшем от стихийного бедствия регионе, укреплении сетей общественной безопасности или обработке других чрезвычайных ситуаций, когда требуется URLLC и eMBB [2].

В этой статье рассматриваются некоторые примеры использования БПЛА в сетях 5G в области связи, коллекция данных и общественных служб.

Интеграция летающей и наземной сетевой архитектуры

БПЛА связи могут помочь существующей сотовой связи для быстрого восстановления обслуживания и предлагают выгрузку трафика из чрезвычайно людных районов экономически эффективно [3]. В настоящее время широко распространено мнение, что индивидуально существующая сеть не может удовлетворить потребность в обработке больших объемов данных и выполнении больших приложений, таких как IoT, облачные вычисления и большие данные. Поэтому среди научных сообществ растет потребность в разработке интегрированной сетевой архитектуры на основе сети воздушного базирования и наземной сети.

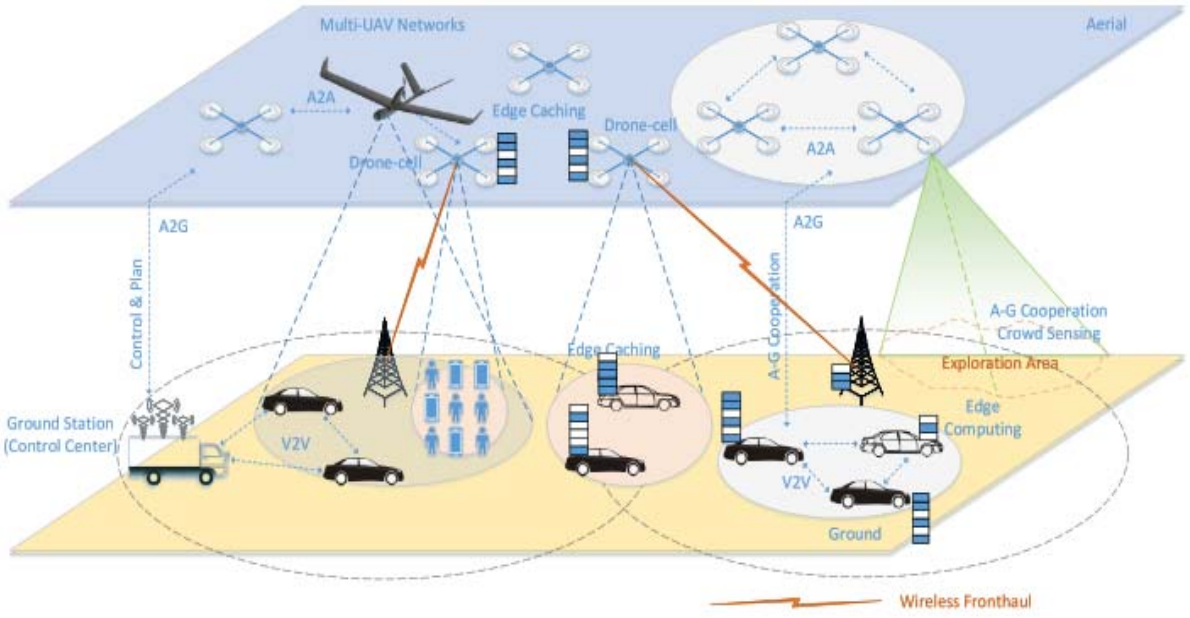


Рис. 1. Воздушная наземная интегрированная сеть [4]

Общая архитектура интегрированной сети воздух-земля представлена на рис. 1 для обеспечения пользовательских устройств улучшенными и гибкими сквозными сервисами, которые подразделяются на два сегмента: воздушный и наземный слои.

В сети воздушного базирования беспилотник оснащен приемопередатчиками для обеспечения гибкого доступа в Интернет для группы наземных пользователей, а беспилотная ячейка является соответствующей зоной покрытия. Размер ячейки дрона определяется высотой полета БПЛА, его местоположением, мощностью передачи и факторами окружающей среды. Кроме того, целый рой БПЛА соединяется путем установления связей между БПЛА и БПЛА для совместного предоставления услуг.

В наземной сети гетерогенная сеть радиодоступа, состоящая из макроячеек и малых ячеек, обслуживает мобильных пользователей, таких как мобильные телефоны, самоуправляемые автомобили, устройства Интернета вещей и т. д., что создаст сосуществующую систему проблемных технологий для беспроводных сетей 5G [5].

Возрастающая вычислительная способность мобильных устройств может быть понята для мобильных периферийных вычислений (MEC), где БПЛА могут планировать вычислительные задачи, в то время как бортовые компьютеры выполняют эти задачи. Кроме того, популярное содержимое может кэшироваться на беспилотных летательных аппаратах или наземных устройствах и передаваться по дрон-ячейкам или через D2D-связь между конечными устройствами. В частности, каналом передачи в интеграции воздушной сети и наземной сети является канал передачи данных LoS. Канал передачи данных LoS используется для передачи с БПЛА на наземную станцию управления.

Примеры применения БПЛА в сетях 5G

БПЛА-вспомогательные коммуникационные сети, полезные для неожиданных, многолюдных и временных событий. Использование роя беспилотных летательных аппаратов по требованию, оснащенных небольшими ячейками 5G, может решить эту проблему, обеспечив лучшее покрытие, что приведет к меньшему количеству сброшенных звонков и лучшему подключению к интернету людей, посещающих мероприятия [6]. На рис. 2 (см. ниже) показан сценарий использования БПЛА в качестве летающих базовых станций, где эти БПЛА обычно оснащаются различными полезными нагрузками для приема, обработки и передачи сигналов, стремясь дополнить ранее существовавшие сотовые системы, обеспечивая дополнительную пропускную способность горячих точек во время временных событий.

Этот сценарий был рассмотрен как один из пяти ключевых сценариев, с которыми сталкиваются будущие сотовые сети [6, 7].

Внедрение и анализ полевых измерений для коллекции данных с помощью БПЛА при его полетах и подключении к коммерческой сети Long-Term Evolution (LTE). Исследователи в работе [1] предлагают результаты моделирования, чтобы подчеркнуть производительность сети, когда она обслу-

живает множество дронов одновременно на большой площади. Представленные в их статье исследования расширяют понимание применимости и эффективности обеспечения мобильной связи беспилотными летательными аппаратами на малых высотах. Цель статьи-предоставить практическую, актуальную информацию, полевые измерения, современные результаты моделирования и лучшие отраслевые практики для беспилотных летательных аппаратов, подключенных к мобильной сети. В статье также описывается, как связаны задержка и распределение физических ресурсов для подключения беспилотных летательных аппаратов.

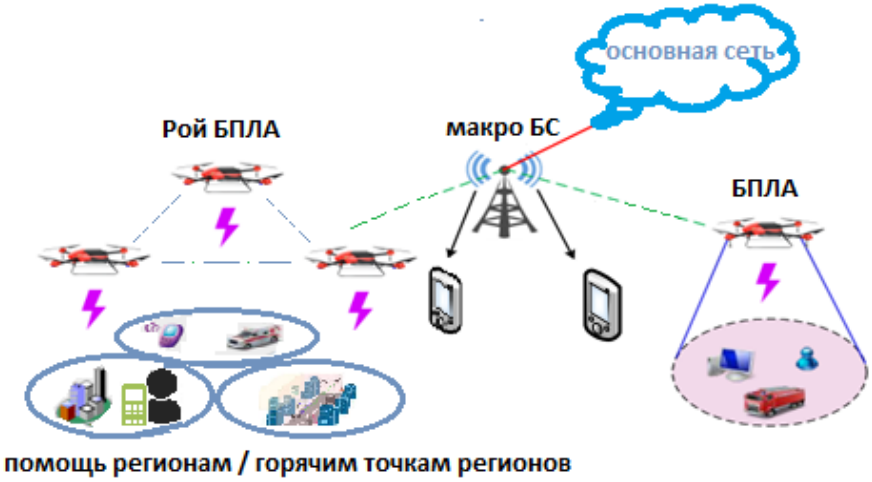


Рис. 2. БПЛА в качестве базовых станций

Беспилотные летательные аппараты могут играть жизненно важную роль в оценке ущерба и оказании помощи, поскольку они имеют возможность взять на себя роль там, где спасатели и пилотируемые транспортные средства не справляются. В статье [5] предложены коммуникационные и сетевые технологии, которые могут способствовать созданию систем управления аварийными ситуациями БПЛА в таких ситуациях, как система раннего предупреждения, поисково-спасательные работы, сбор данных, обеспечение сетевого покрытия при аварийной связи и логистической доставке.

Заключение

В ходе исследования были рассмотрены различные варианты использования интеграции БПЛА с сетью 5G в области связи, сбора данных и общественных работ.

Это показывает, что применение БПЛА с 5G является более эффективным, поскольку оно облегчает и ускоряет выполнение различных задач техники и общественных работ.

Список используемых источников

1. Lin, Xingqin, et al. Mobile network-connected drones: Field trials, simulations, and design insights // IEEE Vehicular Technology Magazine 14.3 (2019): 115–125.
2. Luo, Chunbo, et al. Unmanned aerial vehicles for disaster management // Geological Disaster Monitoring Based on Sensor Networks. Springer, Singapore, 2019. PP. 83–107.
3. Маколкина М. А., Атея А. А., Мутханна А. С. А., Кучерявый А. Е. Метод выгрузки трафика приложений дополненной реальности в многоуровневой системе граничных вычислений // Электросвязь. 2019. № 6. С. 36–42.
4. Cheng, Nan, et al. Air-ground integrated mobile edge networks: Architecture, challenges, and opportunities // IEEE Communications Magazine 56.8 (2018): 26–32.
5. Атея А. А., Мутханна А. С., Кучерявый А. Е. Интеллектуальное ядро для сетей связи 5g и тактильного интернета на базе программно-конфигурируемых сетей // Электросвязь. 2019. № 3. С. 34–40.
6. Li, Bin, Zesong Fei, and Yan Zhang. UAV communications for 5G and beyond: Recent advances and future trends // IEEE Internet of Things Journal 6.2 (2018): 2241–2263.
7. Shakhatreh, Hazim, et al. Unmanned aerial vehicles (UAVs): A survey on civil applications and key research challenges // IEEE Access 7 (2019): 48572–48634.

УДК 004.056.52
ГРНТИ 81.93.29

РАЗРАБОТКА МОДУЛЯ РАЗГРАНИЧЕНИЯ СЕТЕВОГО ТРАФИКА ДЛЯ ПОВЫШЕНИЯ УРОВНЯ ЗАЩИТЫ В ПЛАТФОРМЕ ВИРТУАЛИЗАЦИИ VMWARE VSPHERE

В. А. Альшаев, А. Ю. Цветков

Санкт-Петербургский государственный университет телекоммуникаций им. проф. М. А. Бонч-Бруевича

В данной статье был рассмотрен вопрос, касающийся повышения защиты информации в виртуальной инфраструктуре. В виду быстрого развития виртуализации, этот вопрос является очень актуальным. Большинство крупных IT-компаний плавно переходят в виртуальную сферу и, соответственно, им нужна качественная защиты своей информации. Существует несколько методов для повышения безопасности в VMware vSphere. Эти технологии позволят компаниям решить многие проблемы, связанные с кражей или утратой конфиденциальных данных. Передовые технологии способны предоставить защиту информации любой компании, т. к. в них может использоваться очень гибкий алгоритм, представляющий уникальное решение.

виртуализация, защита, VMware vSphere, домен безопасности, виртуальные машины, метка конфиденциальности, уровни.

Платформа vGate предназначена для обеспечения безопасности виртуальной инфраструктуры, развернутой с использованием системы виртуализации VMware vSphere [1].

Существует 4 домена безопасности: совершенно секретно, секретно, для служебного пользования и не конфиденциально. Прежде всего, в продукте есть разделение ресурсов на следующие категории, для которых можно управлять доступом с точки зрения конфиденциальности:

- защищаемый ESX-сервер;
- хранилище ВМ;
- виртуальная машина;
- физический сетевой адаптер;
- виртуальная сеть

Отдельной сущностью идет администратор VMware vSphere. Его учетной записи назначается определенная метка конфиденциальности. А при выполнении ряда стандартных операций с объектами виртуальной инфраструктуры осуществляется сравнение меток конфиденциальности ресурсов и учетных записей администраторов [2].

Метка конфиденциальности – это принадлежность ресурса или пользователя к какой-либо категории (отдел или класс информации, например, секретно). Существует три типа меток конфиденциальности, которые «накладываются» на ресурсы и учетные записи пользователей:

- *Иерархическая метка* – это метка, которая содержит уровень конфиденциальности. Уровень конфиденциальности – это сущность, которая строго определяет возможность доступа пользователей к ресурсам друг к другу. То есть, пользователь с уровнем «Для служебного пользования» не сможет работать с секретными и совершенно секретными ресурсами, а секретные виртуальные машины не могут находиться на не конфиденциальных хранилищах. Наоборот же, например, на уровень ниже пользователь или ресурс сможет работать с ресурсами, но только если для него установлено соответствующее разрешение (например, для хоста: «Может исполнять машины с меньшим уровнем»). Как становится понятным, этот вариант защиты от НСД больше всего востребован государственными структурами (государственная тайна) или организациями, обрабатывающими персональные данные.
- *Не иерархическая метка* – это метка, которая содержит категорию конфиденциальности. В инфраструктуре может быть сколько угодно категорий, при это все они будут находиться на одном уровне иерархии. Поэтому механизм прост – если у ресурса есть такая метка (категория), то пользователь из этой категории может его использовать. На одном ресурсе может быть несколько меток. Значит, что несколько категорий пользователей могут использовать его. Становится понятно, что данная модель защиты от НСД вполне подходит коммерческим компаниям.

– *Составная метка* – это метка, которая содержит одновременно один уровень конфиденциальности и одну или несколько категорий конфиденциальности. Например, они могут пригодиться для работы с совершенно секретными данными (уровень), но с которыми работают разные отделы (категория) [2].

Чтобы назначить метку, в интерфейсе vGate R2 необходимо выбирать объект виртуальной инфраструктуры (например, виртуальная машина) и нажать «Назначить метку» (рис. 1).

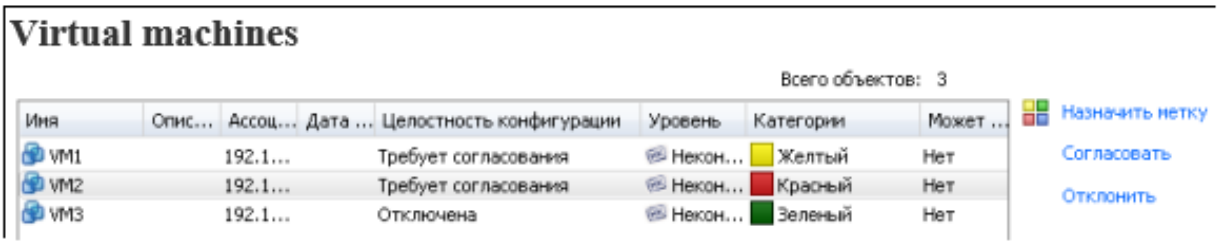


Рис. 1. Назначение метки

Далее выбирается тип метки, назначается уровень или категория (рис. 2).

Если выбирается и уровень, и категория – метка получается составная. По умолчанию, все ресурсы находятся на уровне «не конфиденциально», поэтому нужно учитывать это при работе с конфиденциальной информацией.

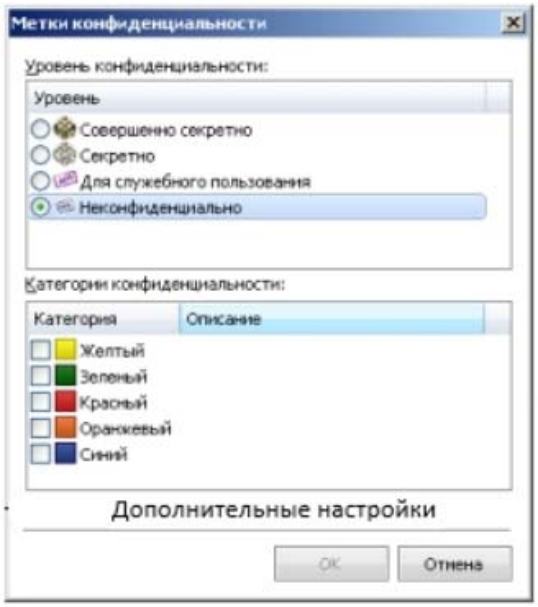


Рис. 2. Выбор метки

Иногда имеет смысл настроить составные метки (уровень и категория), но нужно запретить определенные их комбинации (например, нельзя делать метку «совершенно секретно и отдел новичков»). Для этого есть настраиваемая матрица сочетаний. Есть возможность делать любые комбинации (рис. 3, см. ниже).

Преимущественно, конфигурация уровней состоит из трёх «доменов безопасности: секретно, для служебного пользования и не конфиденциально». А также 3 пользователя, каждый из которых может работать только со своим типом ресурсов, которые могут быть расположены даже на одном хост-сервере VMware ESX / ESXi. Соответственно ресурсы между собой взаимодействуют тоже в рамках своего уровня или ниже, если задано в дополнительных настройках [3].

Шаблон – это копия виртуальной машины (VM) с упорядоченными папками и управляемая разрешениями для доступа к ней. Они полезны,

так как выступают как защищенные версии модели VM, которая может быть использована при создании новой виртуальной машины. Так как шаблон – это оригинальный и совершенный образ определенной VM, они не могут быть запущены как самостоятельные VM.

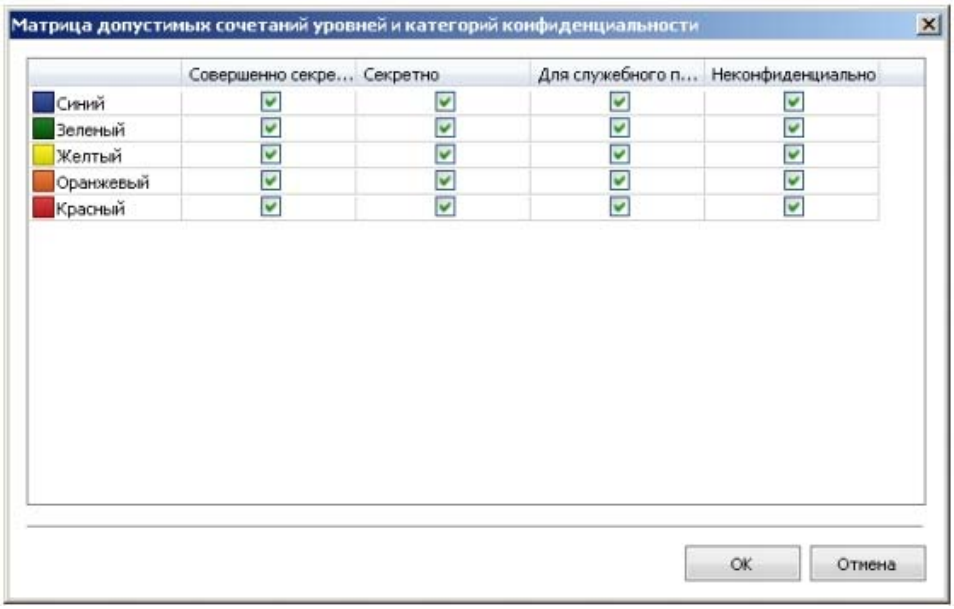


Рис. 2. Допустимые сочетания

Есть 2 способа преобразовать существующую виртуальную машину в шаблон. Её можно сконвертировать в шаблон или клонировать в шаблон. Если выбрано «Convert to template», то выбирается существующая виртуальная машина и конвертируется в шаблон. Данную VM больше нельзя использоваться как виртуальную машину, т. к. она теперь является, из которого будут создаваться новые VM. Если выбрано «Clone to Template», то выбирается существующая VM и из неё создаётся шаблон. Отличие от «Convert to template» лишь в том, что выбранную виртуальную машину можно использовать не только как шаблон, но и как полноценную VM. Также необходимо выбрать хост или кластер для развёртывания шаблона, а затем хранилище для него [4].

В данной работе был описан метод разграничения сетевого трафика и создание шаблонов в VMware vSphere. Принцип разграничения заключается в создании отдельных групп, каждой из которых предоставлены определённые пользовательские права. Ресурсы могут взаимодействовать друг с другом в рамках своего уровня или ниже его. Использование шаблонов сильно уменьшает временные затраты. Назначив определенные разрешения, можно позволить опытным пользователям или младшим администраторам развертывать новые виртуальные машины из шаблонов. Таким образом, разграничение сетевого трафика и создание шаблонов в VMware vSphere с является

очень удобным и простым способом повышения безопасности виртуальной инфраструктуры.

Список используемых источников

1. Создание и использование шаблонов VMware ESX Server [Электронный ресурс]. URL: http://guruadmin.ru/page/sozdanie-i-ispolzovanie-shablonov-vmware-esx-server (дата обращения 22.03.2020).

2. Компания «Код безопасности» Средство защиты информации vGate R2. Руководство администратора. Принципы функционирования; 2016. С. 6.

3. Принципы разграничения доступа к конфиденциальным ресурсам VMware vSphere в vGate R2 [Электронный ресурс]. URL:https://www.vmgu.ru/articles/vgate-r2-vmware-securing-virtual-env (дата обращения 22.03.2020).

4. Возможности vGate R2 для защиты инфраструктуры VMware vSphere 5 [Электронный ресурс]. URL:https://www.vmgu.ru/articles/vgate-r2-2012-all-features (дата обращения 22.03.2020).

Статья представлена заведующим кафедры ЗСС СПбГУТ, кандидатом технических наук, доцентом А. В. Красовым.

УДК 681.7
ГРНТИ 49.44.31

ВЛИЯНИЕ ИЗГИБА ОПТИЧЕСКОГО КАБЕЛЯ В ВОЛОКОННО-ОПТИЧЕСКИХ СИСТЕМАХ ВИДЕОНАБЛЮДЕНИЯ И АБОНЕНТСКОГО ДОСТУПА СО СПЕКТРАЛЬНЫМ УПЛОТНЕНИЕМ: ЭКСПЕРИМЕНТ

Д. П. Андреев[1], Е. И. Андреева[2], А. Н. Сергеев[2], В. Р. Сумкин[1]

[1]НПП «ИТС»
[2]Санкт-Петербургский государственный университет телекоммуникаций им. проф. М. А. Бонч-Бруевича

Экспериментально испытана методика измерения спектральной зависимости потерь в оптическом кабеле, вызванных его изгибом. Проведено сравнение применения для этих целей источников с одночастотными лазерами и лазерами типа Фабри-Перо. Качественная оценка может быть сделана при помощи тестеров с дополнительными источниками, работающими на вспомогательных длинах волн.

волоконно-оптические сети, волоконный световод, оптические потери, изгибные потери.

Потери оптической мощности на макроизгибах оптического кабеля могут оказывать существенное влияние на такие рабочие характеристики, как отношение сигнал/шум на выходе системы, помехозащищенность, срок службы и т. п. [1, 2, 3]. Устойчивость к изгибу зависит как от параметров самого волоконного световода, защитных покрытий, так и рабочей длины волны передаваемого сигнала. Расчет устойчивости к изгибу, как правило, представляет собой довольно сложную задачу. Поэтому представляет интерес методика экспериментального измерения спектральной зависимости потерь на изгибе выбранного оптического кабеля и сравнение ее результатов с экспресс-тестом с помощью портативных рабочих средств измерений, таких, как оптический тестер.

Предложенная методика измерения потерь была испытана на оптических кабелях для внутренней прокладки со световодами стандартов G.652 и G.657 в соответствии с рекомендациями [4, 5, 6].

Исследование проводилось с использованием цилиндрических оправок диаметром d = 15, 12.5 и 10 мм. Для исследования использовались образцы волоконных световодов в буферном и 3 мм защитном покрытии:

– SSMF G.652 в 900-мкм покрытии;
– SSMF G.652 в 3-мм покрытии;
– SMF G.652 D в 3-мм покрытии;
– SMF G.657 A2 в 3-мм покрытии.

С целью уменьшения влияния обратных отражений использовались разъемы SC/APC.

Для исследования использовались стандартные волоконные световоды в 3-мм защитном и 900-мкм буферном покрытии. На оправку диаметром d = 15 мм укладывалось 5 витков, так что длина световода на оправке составляла 0,24 м. Результаты измерений представлены на рис. 1. В ходе испытаний подтвердилось, что потери, вызванные изгибами, увеличиваются экспоненциально при увеличении значения длины волны.

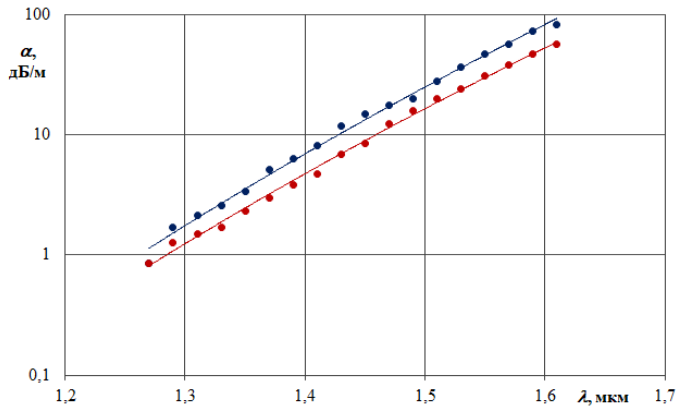


Рис. 1. Изгибные потери для ВС (SSMF G.652) в 900-мкм буферном покрытии (1) и 3-мм защитном покрытии (2) при диаметре изгиба d = 15мм, измеренные с помощью одночастотных источников оптического излучения

На следующем шаге проводилось исследование световодов G.652.D с улучшенными характеристиками при изгибе (рис. 2). Изгиб на оправке диаметром d = 15мм приводил к малому уровню потерь, поэтому использовалась оправка с меньшим диаметром: d = 12,5 мм, длина световода на оправке при укладке 5 витков составила 0,2 м.

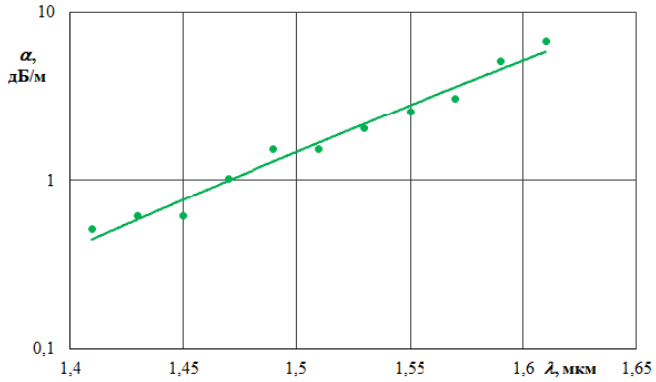


Рис. 2. Изгибные потери для ВС 3-мм защитном покрытии стандарта G.652 D при диаметре изгиба d = 12,5 мм

Световод стандарта G.657 A2 продемонстрировал высокую устойчивость к изгибу. На рис. 3 представлены результаты измерений спектральной зависимости изгибных потерь световода стандарта G.657 A2 при намотке на оправку диаметром d = 10 мм.

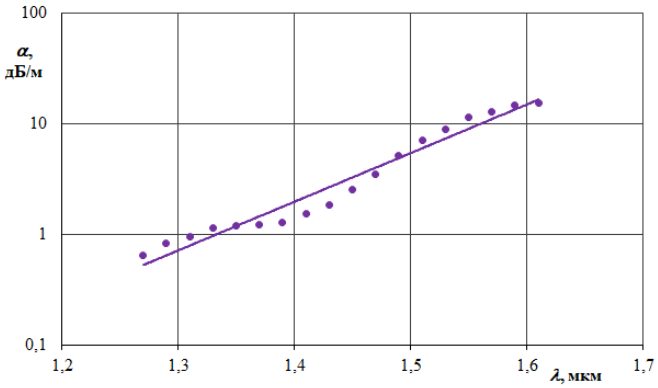


Рис. 3. Изгибные потери для ВС 3-мм защитном покрытии стандарта G.657 A2 при диаметре изгиба d = 10 мм

При испытаниях на оправке малого диаметра (10 мм) явно наблюдался эффект интерференции между распространяющимися и излучаемыми модами. При данном эффекте распространяющийся оптический сигнал излучается из сердцевины изогнутого волокна и отражается обратно от искривленных границ раздела за пределами сердцевины (например, сердцевина-оболочка или оболочка-покрытие или покрытие-воздух, так же как при так называемом эффекте галереи шепота), таким образом интерферируя

с распространяющейся модой. В процессе измерении изгибных потерь возникли осцилляции зависящие от значения длины волны при малом радиусе изгиба. Обработка результатов измерений проводилась методам аппроксимации в соответствии с рекомендациями [4].

Таким образом, экспериментально подтверждено, что устойчивость к изгибу ВС в буферном и 3-мм защитном покрытии значительно превосходит устойчивость к изгибу ВС в первичном покрытии, и световоды стандарта G.657 A2 имеют значительно более улучшенные изгибные характеристики, чем стандартные световоды (SSMF G.652).

Для тестирования оптической сети необходимо использовать портативные рабочие средства измерений, например, Рубин-123. Спектр источника отличается от использованного ранее (рис. 2). Результаты измерений с помощью тестера Рубин-123 представлены на рис. 4. Полученные результаты оказались в хорошем соответствии с проведенными ранее с использованием одночастотных источников оптического излучения. Некоторое отличие касается точек 1,31 и 1,55 мкм: разница в величине изгибных потерь оказалась больше, чем в предыдущем случае. Это связано с влиянием «крыльев» спектра источника.

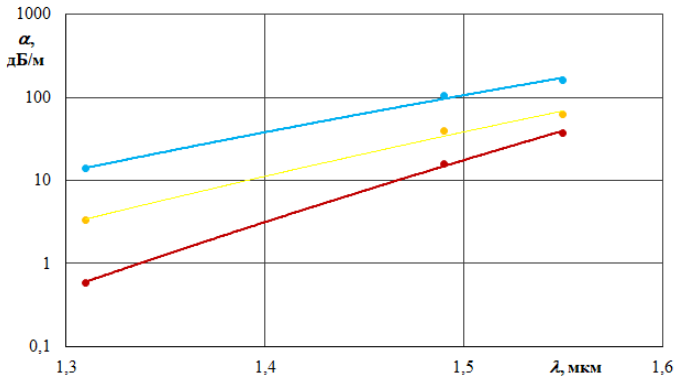


Рис. 4. Изгибные потери для ВС стандарта G.652 в 3-мм защитном покрытии, измеренные с помощью оптического тестера Рубин-123 при диаметре изгиба d = 10 мм (1), 12 мм (2) и 15 мм (3)

Можно сделать вывод, что более точные результаты измерения изгибных потерь могут быть получены с использованием первого метода. Однако более наглядный результат дает измерение с помощью портативного тестера типа Рубин-123.

При проведении исследования контролировалось качество передаваемого видеосигнала (рис. 5, см. ниже) [7, 8, 9]. Пока суммарное ослабление сигнала не превышало энергетический бюджет линии (при использовании видео-модемов марки ОМД – 16 дБ [2, 3]), регистрируемый сигнал оставался стабильным и достаточно четким.

Список используемых источников

1. Андреева Е. И., Купцов В. Д., Валюхов В. П., Сумкин В. Р. Волоконно-оптическая система видеонаблюдения производственного объекта: функции охраны и технологического контроля. Часть 2. Тестирование // Актуальные проблемы инфотелекоммуникаций в науке и образовании. VII Международная научно-техническая и научно- методическая конференция: сб. науч. ст. в 4-х т. СПб. : СПбГУТ, 2018. Т. 1. С. 61–66.

2. Андреева Е. И., Купцов В. Д., Валюхов В. П. Волоконно-оптическая система видеонаблюдения производственного объекта: функции охраны и технологического контроля. Часть 1. Активное оборудование // Актуальные проблемы инфотелекоммуникаций в науке и образовании. VII Международная научно-техническая и научно-методическая конференция: сб. науч. ст. в 4-х т. СПб. : СПбГУТ, 2018. Т. 1. С. 57–61.

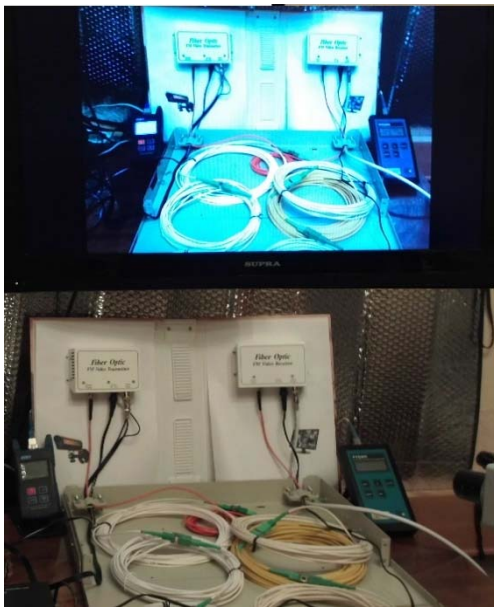


Рис. 5. Сегмент экспериментального стенда с волоконно-оптическими модемами для передачи видеосигнала по оптическому кабелю

3. Андреева Е. И., Валюхов В. П., Купцов В. Д., Сумкин В. Р. Система видеонаблюдения на волоконной оптике с использованием спектрального уплотнения. // Актуальные проблемы инфотелекоммуникаций в науке и образовании. VIII Международная научно-техническая и научно-методическая конференция: сб. науч. ст. в 4-х т. СПб. : СПбГУТ, 2019. Т. 1. С. 60–65.

4. МЭК 60793-1-47-2014 Волокна оптические. Часть 1-47. Методы измерений и проведение испытаний. Потери, вызванные макроизгибами (IEC 60793-1-47:2009 Optical fibres – Part 1-47: Measurement methods and test procedures – Macrobending loss).

5. МЭК 60793-1-1 Волокна оптические. Часть 1-1. Методы измерений и проведение испытаний. Общие положения и руководство (IEC 60793-1-1, Optical fibres – Part 1-1: Measurement methods and test procedures – General and guidance).

6. МЭК 60793-1-40 Волокна оптические. Часть 1-40. Методы измерений и порядок проведения испытаний. Затухание волокна (IEC 60793-1-40, Optical fibres – Part 1-40: Measurement methods and test procedures – Attenuation).

7. Купцов В. Д., Валюхов В. П. Чувствительность фотоприемного устройства на основе интегратора фототока // Электромагнитные волны и электронные системы. 2014. Т. 19. №7. С. 16–23.

8. Купцов В. Д., Валюхов В. П. Чувствительность фотоприёмных устройств волоконно-оптических линий связи // Научно-технические ведомости Санкт-Петербургского государственного политехнического университета. Информатика. Телекоммуникации. Управление. 2010. № 6 (113). С. 31–36.

9. Андреева Е. И., Купцов В. Д., Валюхов В. П. Передача высококачественного видеосигнала по волоконно-оптической сети с CWDM // Актуальные проблемы инфотелекоммуникаций в науке и образовании. VIII Международная научно-техническая и научно-методическая конференция: сб. науч. ст. в 4-х т. СПб. : СПбГУТ, 2019. Т. 1. С. 56–60.

УДК 621.39; 629.05; 629.735
ГРНТИ 49.44

К ВОПРОСУ О ПРИМЕНЕНИИ ВОЛОКОННОЙ ОПТИКИ ДЛЯ БОРТОВЫХ КАБЕЛЬНЫХ СЕТЕЙ

В. А. Андреев, А. В. Бурдин, В. А. Бурдин

Поволжский государственный университет телекоммуникаций и информатики

В представленной работе предложено решение для волоконно-оптических бортовых кабельных сетей, включающее способ прокладки оптических кабелей на борту, специализированное многомодовое оптическое волокно с увеличенным диаметром сердцевины и модульное сетевое транспортное оборудование для передачи данных.

оптическое волокно, оптический кабель, бортовые кабельные сети, пневмопрокладка, защитный трубопровод, оборудование передачи данных.

Задача замены медножильных кабелей бортовых информационных сетей на оптические волокна стояла практически с этапа разработки оптических волокон с приемлемыми потерями. Интерес к данной проблеме сохранился до настоящего времени. Причем в последние годы проблема замены медножильных бортовых кабелей оптическими волокнами стала особенно актуальной. Это, в первую очередь, обусловлено двумя факторами. Перспективами внедрения беспилотных аппаратов и разработкой электромагнитного оружия на базе СВЧ-установок, способных выводить из строя электронное оборудование практически любой цели на расстоянии до 10 км и более.

Экранирование не исключает выход из строя бортовых электронных систем при действии электромагнитного импульса (ЭМИ). При этом металлические проводники кабелей, собственно, и являются тем путем, по которому ЭМИ поступает к электронной аппаратуре. Соответственно кардинальным средством защиты бортовой электроники от ЭМИ является замена кабелей с металлическими проводниками на оптические волокна.

Отказ электронного оборудования под действием ЭМИ делает борт неуправляемым. И если наземный транспорт, плавсредства при воздействии ЭМИ только теряют управление, сохраняя живучесть, по крайней мере до ракетного удара, то для летательных аппаратов такое воздействие связано с потерей живучести. Неуправляемый летательный аппарат не может держаться в воздухе. Сегодня беспилотные летательные аппараты (БЛА) поставлены на вооружение и все шире применяются как для разведки,

так и для атаки на объекты противника. Основным средством защиты от действий БЛА являются средства радиоэлектронной борьбы. Не случайно по оценкам экспертов, беспилотные авиационные системы – самый быстрорастущий рынок военной продукции для волоконной оптики [1]. Согласно прогнозу Forecast International, объем мирового рынка БЛА за период 2015–2024 гг. достигнет уровня чуть менее $ 71 млрд. Системы fly-by-light (управления полетом по оптоволокну) обсуждались годами, но воплотятся в жизнь в первую очередь благодаря применению на борту БЛА [1].

Следует отметить, что тенденции изменения электромагнитной обстановки, в частности в условиях города и промышленных предприятий, делают актуальной задачу защиты от электромагнитных воздействий и для наземного транспорта. Особенно для беспилотных средств передвижения.

При этом, оптимизация прочностных параметров конструкций с целью улучшения массогабаритных характеристик приводит к снижению толщин металлических экранирующих элементов, их перфорированности или применению неметаллических композитных материалов, что приводит к увеличению влияния излучаемых помех на аппаратуру и кабели.

Увеличение количества электронных устройств, средств связи, навигации, автоматизированных систем, внедрение цифровых электронных систем управления, применение новых материалов приводит к усложнению бортовых кабельных сетей. Плотность упаковки при размещении элементов и устройств, электронных блоков и систем различного назначения на борту приводит к необходимости решения задач электромагнитной совместимости оборудования внутри транспортного средства.

И наконец, немаловажным фактором, определяющим необходимость перехода к бортовым волоконно-оптическим сетям, является рост потребностей в уменьшении задержек на сети и увеличении объемов передаваемой в этих сетях информации. Развитие и совершенствование бортового радиоэлектронного оборудования современных транспортных средств характеризуется широким внедрением информационно-телекоммуникационных технологий. Специализированные бортовые целевые радиоэлектронные комплексы, размещаемые на борту современных транспортных средств, чаще всего представляют собой распределенные информационно-вычислительные системы. Бортовые сети таких систем с одной стороны должны удовлетворять требованиям минимизации средних задержек при передаче управляющих команд, а с другой стороны обеспечивать передачу по сети исходных видеопотоков на скоростях до десятков Гбит/с без сжатия и с минимальными задержками [2]. Требования минимизации средних задержек при передаче управляющих команд необходимы для устойчивой работы контуров управления внутри радиоэлектронных комплексов и обеспечения

точности привязки обнаруживаемых аномалий и признаков к навигационным данным с учетом высокой скорости движения. Вторая группа требований обусловлена необходимостью передачи видеопотоков без сжатия и, как следствие, высокими нагрузками на видеосеть при очень жестких требованиях к задержкам передаваемого трафика. Вышеперечисленные требования в [2] были сформулированы для бортовой сети летательных аппаратов, однако, как показывают тенденции развития современного транспорта, им должны соответствовать бортовые сети и других транспортных средств, в частности автомобилей [3]. Особенно это касается беспилотных аппаратов.

Таким образом, можно отметить следующие основные преимущества волоконно-оптических бортовых сетей перед сетями на основе многожильных кабелей с металлическими проводниками.

– Нечувствительность к воздействию электромагнитных импульсов и высокочастотных помех и, как следствие, высокая надежность передачи данных и повышение живучести самого борта.

– Снижение требований по экранированию позволяет упростить задачу размещения оборудования на борту, увеличить долю композиционных материалов в составе корпуса транспортного средства и комплектующих и, тем самым, уменьшить его массу и стоимость.

– Пропускная способность, которую не могут обеспечить симметричные или коаксиальные кабели.

– Снижение массы и простота конструкции волоконно-оптического кабеля.

В данной работе рассмотрено комплексное решение для бортовых волоконно-оптических кабельных систем. Решение включает альтернативный способ прокладки оптического кабеля на борту, применение кабеля, многомодовое оптическое волокно которого имеет увеличенный диаметр сердцевины и профиль показателя преломления, оптимизированный для выравнивания дифференциальной модовой задержки, а также модульное сетевое оборудование с функциями мониторинга и управления.

Предлагаемое решение учитывает принятый при разработке бортовых кабельных сетей порядок приоритетов:

– обеспечение безопасности (проектирование надежности и безопасности);

– обеспечение экономической эффективности производства;

– уменьшение трудоёмкости;

– обеспечение удобства обслуживания, демонтажа и замены компонентов.

Список используемых источников

1. Репин А. В. Волоконная оптика в авиации: наступившее завтра [Электронный ресурс] // Национальная оборона. 2016. № 1. URL: http://www.oborona.ru/includes/periodics/defense/2016/0118/143817620/detail.shtml (дата обращения 04.10.2019).
2. Никульский И. Е., Овчарова Л. В., Кротов А. В. Особенности построения информационно-телекоммуникационных сетей на борту современных летательных аппаратов // Информация и Космос. 2014. № 2. С. 6–11.
3. Perlicki K., Wilczewski G. Fiber optics transmission for vehicle applications // Measurement Automation Monitoring. 2015. Vol. 61 (3). P. 81–83.

УДК 654.1
ГРНТИ 49.33.29

МОДЕЛЬ ПРОГНОЗА СРОКА СЛУЖБЫ ОПТИЧЕСКОГО КАБЕЛЯ, ВВЕДЕННОГО В ЭКСПЛУАТАЦИЮ

В. А. Андреев, В. А. Бурдин, А. О. Нижгородов

Поволжский государственный университет телекоммуникаций и информатики

В представленной работе предложена модель прогноза срока службы оптического кабеля, введенного в эксплуатацию. Модель учитывает «историю жизни» оптического волокна в кабеле и случайный характер механических воздействий на оптическое волокно при производстве кабеля, строительстве и технической эксплуатации кабельной линии.

оптическое волокно, оптический кабель, надежность, срок службы.

Оценки срока службы оптического кабеля на введенных в эксплуатацию линиях связи востребованы как производителями, так и потребителями кабельной продукции. Известно два основных подхода к прогнозу надежности оптических кабелей, из которых более предпочтителен базирующийся на прогнозе оценок срока службы кабеля [1]. Наиболее перспективными полагаются прогнозирующие стратегии технического обслуживания кабельных линий [2, 3]. При этом, для определения оценок срока службы оптического кабеля в процессе эксплуатации кабельных линий предлагается комплексный подход, включающий анализ статистики повреждения кабеля на линии, данные мониторинга и результаты специальных измерений параметров кабеля, в частности, используя импульсный рефлектометр обратного рассеяния Мандельштама-Бриллюэна [4]. Однако, даже если известны ста-

тистика повреждений кабеля на линии, данные мониторинга параметров оптических волокон, результаты измерений распределений механических напряжений волокон кабеля и т. п., возникает вопрос о том, как применить эти данные для прогноза срокам службы оптического кабеля. В отличие от оптического волокна, для которого рекомендуемые методики ожидаемой продолжительности жизни регламентированы и подробно описаны [5], для оптического кабеля такая детальная утвержденная методика прогноза отсутствует.

Функции, для которых собственно и предназначен оптический кабель, выполняются оптическим волокном. Все остальные кабельные элементы должны защищать оптические волокна от внешних воздействий, чтобы обеспечить их работоспособность в условиях эксплуатации кабеля. Это дает возможность предположить, что срок службы оптического кабеля определяется временем жизни оптического волокна в кабеле. В этом случае для прогнозирования срока службы оптического кабеля можно использовать метод прогнозирования срока службы оптического волокна на основе результатов его испытаний на растяжение с учетом воздействия на оптическое волокно в процессе изготовления кабеля, строительство, а затем во время эксплуатации кабельной линии, как испытания оптического волокна под нагрузкой. Для этого необходимо знать характер внешнего воздействия и нагрузку на волокно, а также временной интервал, в течение которого оно приложено. Очевидно, что для процесса производства кабеля и, кроме того, для строительства и эксплуатации кабельных линий можно оперировать только вероятностными оценками этих параметров, определение которых требует большого объема статистических исследований. Один из вариантов вышеупомянутого подхода для прогноза срока службы оптического кабеля модульной конструкции был рассмотрен в работе. Авторы рассмотрели основные технологические процессы производства оптического кабеля и предложили использовать оценки эквивалентных значений нагрузки и времени ее воздействия на оптическое волокно при изготовлении кабеля, при строительстве кабельной линии. Был представлен анализ характера воздействий, оценки средних значений нагрузок и длительности отдельных технологических операций. На основе физического моделирования были получены оценки нагрузок на оптическое волокно в процессе строительства. Приведен пример прогнозирования срока службы оптического кабеля на вновь построенной кабельной линии. Вместе с тем, длительность процессов и нагрузка на волокно полагались детерминированными величинами. Очевидно, что это допустимо для процесса тестирования оптического волокна под нагрузкой. В этом случае нагрузка на волокно и время загрузки строго контролируются. Однако на более поздних этапах производства кабеля, а тем более при строительстве и эксплуатации кабельной линии, эти значения являются случайными величинами.

В данной работе предложены модель и алгоритм прогноза срока службы оптического кабеля по данным измерений распределений напряжений в оптических волокнах кабеля на исследуемой длине кабельной линии, учитывающая случайный характер нагрузок на оптические волокна в процессе производства кабеля, строительства и эксплуатации кабельной линии.

Как и в известной работе [6] здесь предлагается прогнозировать срок службы оптического волокна на будущее, рассматривая нагрузки, которым подвергалось оптическое волокно в кабеле в прошлом как процесс тестирования волокна под нагрузкой. Но, в отличие от [6] предлагаемая модель позволяет учитывать случайный характер этих нагрузок. Предлагается оценивать вероятность безотказной работы оптического волокна на кабельной линии протяженностью L при постоянной нагрузке σ_a, в течении интервала времени t_f как:

$$P_f = \int_{X_m}^{X_{\max}} P_p(X) \cdot P_X^{\alpha}(X)\, dX,$$

$$\ln \frac{1}{P_X} = \left[(X+1)^{m_s} - 1 \right],$$

$$P_p(X) = \frac{a}{X_m} \left(\frac{X_m}{X} \right)^{a+1},$$

$$X_m = \frac{t_f \sigma_a^n + \sum_{i=1}^{N} \sigma_i^n t_i \left(\frac{L}{L_i} \right)^{\frac{1}{m_S}}}{t_p \sigma_p^n},$$

$$\alpha = L / L_p .$$

Параметр закона Парето принимается равным a = 1..2.

Интеграл вычисляется численными методами. Очевидно, что данное выражение позволяет вычислять прогнозируемые оценки срока службы кабеля при условии, что известна нагрузка на оптическое волокно в кабеле в будущем и история нагрузок на оптическое волокно в прошлом. При этом, данные этой история должны позволять определять параметр X_m. А это, в свою очередь, требует знания статистических характеристик технологических процессов производства кабеля, строительства и технической эксплуатации кабельной линии. Естественно, что погрешность оценок будет существенно зависеть от погрешностей оценок статистических характеристик технологических процессов. И, наконец, в перспективе предлагаемый подход позволяет учитывать при прогнозе срока службы оптического кабеля старение элементов его конструкции. Однако, это требует исследования и формализации зависимостей нагрузки на оптическое волокно в кабеле от степени старения элементов конструкции оптического кабеля.

Список используемых источников

1. Ларин Ю. Т. Сравнительный анализ двух подходов к надежности оптических кабелей // Наука и техника. 2009. № 2 (315). С. 3–7.

2. Бурдин В. А., Воронков А. А., Шафигуллин Л. Н. Эффективность применения прогнозирующих стратегий технического обслуживания ОК // Вестник связи. 2012. № 7. С. 5–8.

3. Andreev V. A., Voronkov A. A., Shafigullin L. N. Strategy choice for fiber optic transmission lines maintenance // Optical Technologies for Telecommunications 2010 / edited by V. A. Andreev, V. A. Burdin, A. H. Sultanov, O. G. Morozov. Proceedings of SPIE Vol.7992 (SPIE, Bellingham, WA, 2011) P. 79920F.

4. Koga H., Kuwabara T., Mitsunaga Y. Future maintenance systems for optical fiber cables // ICC-91 Proceedings. 1991. PP. 0323–0329.

5. IEC/TR 62048:2014. Optical fibres-Reliability-Power law theory. 2014. 70 p.

6. Da Silva A. C., Hirose F. N., Neto J. A. M., Furtado J. M. I. Optimization of Loose Tube Optical Cable Manufacture Process Based on Optical Fiber Mechanical Behavior // Proceedings of the 50th IWCS. 2001. PP. 249–252.

УДК 681.7
ГРНТИ 49.44.31

ВЛИЯНИЕ ИЗГИБА ОПТИЧЕСКОГО КАБЕЛЯ В ВОЛОКОННО-ОПТИЧЕСКИХ СИСТЕМАХ ВИДЕОНАБЛЮДЕНИЯ И АБОНЕНТСКОГО ДОСТУПА СО СПЕКТРАЛЬНЫМ УПЛОТНЕНИЕМ: МЕТОДИКА

Е. И. Андреева[1], В. П. Валюхов[2], В. Д. Купцов[2], К. Р. Копалин[1], В. Р. Сумкин[3]

[1]Санкт-Петербургский государственный университет телекоммуникаций им. проф. М. А. Бонч-Бруевича
[2]Санкт-Петербургский политехнический университет Петра Великого
[3]ООО «НПП «ИТС»

Для идентификации изгиба оптического кабеля может быть использована методика измерения спектральной зависимости потерь. Проведено сравнение применения для этих целей источников с одночастотными лазерами и лазерами типа Фабри-Перо. Показано, что для более точного измерения спектральной зависимости потерь на макроизгибах оптического кабеля дает методика с использованием одночастотных лазеров.

волоконно-оптические сети, волоконный световод, оптические потери, изгибные потери.

В последнее время значительно увеличился объем волоконной оптики в сетях абонентского доступа, системах видеонаблюдения, компьютерных сетях и т. п. [1, 2, 3]. В таких системах условия прокладки и эксплуатации оптического кабеля сопряжены с их многократным изгибом. Прямым следствием такой эксплуатационной особенности является значительное возрастание вероятности увеличения потерь оптического излучения на изгибе световода. Эти потери обусловлены вытеканием энергии основной моды световода из области сердцевины в отражающую оболочку. Прокладка оптического кабеля в таких сетях отличается повышенными требованиями к соблюдению норм на допустимый радиус изгиба оптического кабеля.

В случаях, когда избежать малых радиусов изгиба оптического кабеля не удается, используется специальный кабель с повышенной устойчивостью к изгибу. Данный тип оптоволоконных кабелей изготавливается с волокном BLIF, Bending Loss Insensitive Fiber. Основной их особенностью является значительное снижение потерь на изгиб и уменьшение допустимого радиуса изгиба, что дает преимущество при прокладке внутриобъектных и локальных вычислительных сетей.

В любом случае при тестировании оптической кабельной системы необходимо найти и устранить факты изгиба оптического кабеля, не укладывающиеся в нормативные допуски, если при монтаже не удалось их полностью исключить. Своевременное устранение нарушений правил монтажа, касающихся изгиба световода, позволяет избежать возможного его разрушения и продления срока службы всей волоконно-оптической сети. Одним из основных критериев идентификации изгиба оптического волокна с малым радиусом является спектральная зависимость потерь, вносимых изгибом. Это обусловлено зависимостью размера модового пятна ω от длины волны λ передаваемого оптического излучения. Для стандартного волоконного световода (SSMF, *Standard Single Mode Fiber*, G.652) диаметр модового пятна $\omega \sim 7\lambda$. Это означает, что с увеличением длины волны λ передаваемого оптического сигнала доля его энергии, распространяющаяся за пределами сердцевины, возрастает, и в случае изгиба с малым радиусом большая доля оптического излучения уходит из световода. Это обстоятельство может быть использовано для выявления фактов изгиба оптического кабеля при соответствующей методике его тестирования.

Оптический волоконный световод G.652 имеет высокий уровень надежности. Передача данных по данному волокну осуществляется на скорости до 10 Гбит/с. Эти световоды наиболее широко используются при построении оптических сетей. Для сетей абонентского доступа разработаны световоды класса G.652.D, характеризующиеся пониженным уровнем затухания и повышенной устойчивостью к изгибу.

Для специальных применений разработаны световоды с уменьшенной чувствительностью к изгибу (Рекомендации G.657). Это световоды с депрессированной оболочкой, с уменьшенным диаметром модового поля и т. д. В этих конструкциях потери на изгибе уменьшаются как за счет уменьшения диаметра модового пятна, так и за счет ограничения поля волны кольцами с сильно уменьшенным показателем преломления.

Рекомендации ITU-T (МСЭ–Т) регламентируют характеристики волоконных световодов, в том числе – с повышенной устойчивостью к изгибу: G.657. Этот тип оптических волокон BLIF, формально похожий на стандартное волокно типа G.652.D, но предназначенное для сетей доступа, локальных сетей, кабельного телевидения и т. д. Основная особенность – существенно сниженные потери при макроизгибах и уменьшенный допустимый радиус изгиба (до 7,5 мм минимум), что дает преимущество при прокладке внутриобъектовых и локальных сетей. Кроме того, это волокно имеет более жесткие механические допуски. Существует две модификации рекомендаций: G.657.A и G.657.B (G.657 A1 и G.657 A2).

Измерения проводились в соответствии с ГОСТ Р МЭК 60793-1-47-2014 [4, 5, 6]. При проведении испытаний использовался *метод контроля мощности*, при помощи которого измеряют увеличение затухания в волокне вследствие изменения положения волокна из прямого в изогнутое.

Выбор длины кабелей не менее 3 м обеспечивал рекомендованное накопление избыточного волокна на радиусе изгиба не менее 140 мм и свободную укладку волокна за пределами оправки. Диаметр оправки выбирался для обеспечения достаточного отношения S/N во всем спектральном диапазоне, намотка осуществлялась без нежелательного натяжения, скручивания, без петель на относительно длинном отрезке волокна, используемого при проведении измерений.

Так как для одномодовых волокон затухание возрастает по линейному закону с увеличением числа витков, причем в соответствии с рекомендациями должно быть использовано не более 5–10 оборотов, на оправку укладывалось по 5 витков.

Последовательность испытаний в соответствии с рекомендациями проводилась перемоткой волокна с оправки большого радиуса (вносящей незначительные потери вследствие макроизгибов) на оправку требуемого меньшего радиуса.

Учитывая, что на результаты измерения могут влиять различные источники, один из которых – отражения, все разъемы были стандарта APC. Испытуемые кабели были соединены последовательно, непосредственно к источнику и измерителю оптической мощности подключались посредством измерительных кабелей.

Для исследования влияния изгиба волоконного световода на его характеристики был собран стенд, блок-схема которого представлена на рис. 1.

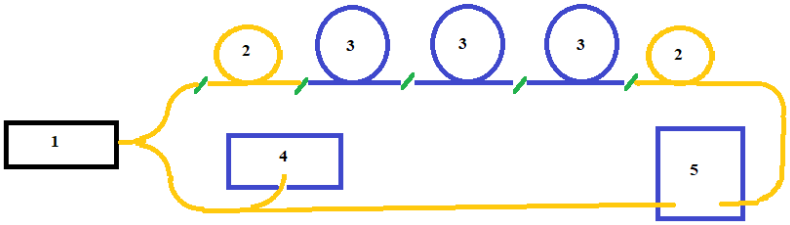


Рис. 1. Блок-схема измерительной установки: 1 – источник оптического излучения на заданной длине волны, 2 – измерительный волоконный световод, 3 – тестируемые волоконные световоды, 4 – оптический анализатор спектра, 5 – измеритель оптической мощности

Экспериментальное исследование уровня изгибных потерь проводилось методом замещения. Тестирование проводилось в 2 этапа. На первом этапе снималась спектральная зависимость уровня внесенных потерь в широком диапазоне длин волн: от 1270 до 1610 нм. В качестве источников излучения использовались CWDM SFP-модули (*Smal Form-Factor Pluggable*). Регистрация оптического сигнала осуществлялась дифференциальным методом с учетом спектральной чувствительности фотоприемника [7, 8, 9]. Измерения оптической мощности проводились с помощью стационарного измерителя оптической мощности Рубин-300. Параметры источников контролировались с помощью анализатора оптического спектра Yokogawa AQ6370C.

На втором этапе продемонстрирован качественный экспресс-тест на чувствительность оптических миникабелей к изгибу с помощью оптического тестера, оснащенного тремя источниками и дающего возможность измерения уровня потерь на трех длинах волн. Измерения проводились с помощью портативного оптического тестера Рубин-123. Качественное сравнение спектров сигналов представлено на рис. 2.

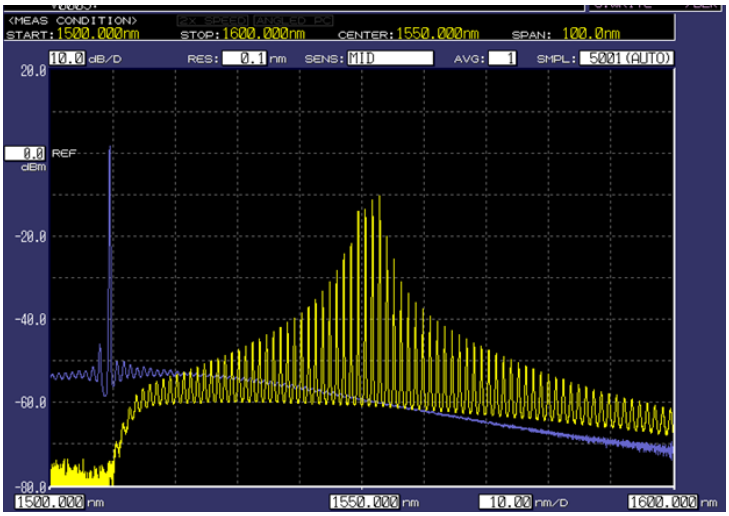


Рис. 2. Спектр одночастотного источника SFP-модуля (слева) и лазера с резонатором типа Фабри-Перо с центральной длиной волны 1550 нм

Таким образом предложена методика измерения спектральной зависимости потерь на макроизгибах волоконных световодов и оптических миникабелей с помощью одночастотных лазерных источников. Проведено сравнение результатов исследований с помощью одночастотных лазеров и лазеров с широким спектром.

Список используемых источников

1. Андреева Е. И., Купцов В. Д., Валюхов В. П., Сумкин В. Р. Волоконно-оптическая система видеонаблюдения производственного объекта: функции охраны и технологического контроля. Часть 2. Тестирование // Актуальные проблемы инфотелекоммуникаций в науке и образовании. VII Международная научно-техническая и научно-методическая конференция: сб. науч. ст. в 4-х т. СПб. : СПбГУТ, 2018. Т. 1. С. 61–66.

2. Андреева Е. И., Купцов В. Д., Валюхов В. П. Волоконно-оптическая система видеонаблюдения производственного объекта: функции охраны и технологического контроля. Часть 1. Активное оборудование // Актуальные проблемы инфотелекоммуникаций в науке и образовании. VII Международная научно-техническая и научно-методическая конференция: сб. науч. ст. в 4-х т. СПб. : СПбГУТ, 2018. Т. 1. С. 57–61.

3. Андреева Е. И., Валюхов В. П., Купцов В. Д., Сумкин В. Р. Система видеонаблюдения на волоконной оптике с использованием спектрального уплотнения // Актуальные проблемы инфотелекоммуникаций в науке и образовании. VIII Международная научно-техническая и научно-методическая конференция: сб. науч. ст. в 4-х т. СПб. : СПбГУТ, 2019. Т. 1. С. 60–65.

4. МЭК 60793-1-47-2014 Волокна оптические. Часть 1-47. Методы измерений и проведение испытаний. Потери, вызванные макроизгибами (IEC 60793-1-47:2009 Optical fibres – Part 1-47: Measurement methods and test procedures – Macrobending loss).

5. МЭК 60793-1-1 Волокна оптические. Часть 1-1. Методы измерений и проведение испытаний. Общие положения и руководство (IEC 60793-1-1, Optical fibres – Part 1-1: Measurement methods and test procedures – General and guidance).

6. МЭК 60793-1-40 Волокна оптические. Часть 1-40. Методы измерений и порядок проведения испытаний. Затухание волокна (IEC 60793-1-40, Optical fibres – Part 1-40: Measurement methods and test procedures – Attenuation).

7. Купцов В. Д., Валюхов В. П. Чувствительность фотоприемного устройства на основе интегратора фототока // Электромагнитные волны и электронные системы. 2014. Т. 19. № 7. С. 16–23.

8. Купцов В. Д., Валюхов В. П. Чувствительность фотоприёмных устройств волоконно-оптических линий связи // Научно-технические ведомости Санкт-Петербургского государственного политехнического университета. Информатика. Телекоммуникации. Управление. 2010. № 6 (113). С. 31–36.

9. Андреева Е. И., Купцов В. Д., Валюхов В. П. Передача высококачественного видеосигнала по волоконно-оптической сети с CWDM // Актуальные проблемы инфотелекоммуникаций в науке и образовании. VIII Международная научно-техническая и научно-методическая конференция: сб. науч. ст. в 4-х т. СПб: СПбГУТ, 2019. Т. 1. С. 56–60.

УДК 654.9
ГРНТИ 47.53.31

ВОЛОКОННО-ОПТИЧЕСКИЙ ДАТЧИК АКУСТИЧЕСКОГО ВОЗДЕЙСТВИЯ ДЛЯ СИСТЕМЫ КОНТРОЛЯ БЕЗОПАСНОСТИ ОБЪЕКТА

Е. И. Андреева[1], В. П. Валюхов[2], В. Д. Купцов[2], С. О. Спиридонов[1]

[1]Санкт-Петербургский государственный университет телекоммуникаций им. проф. М. А. Бонч-Бруевича
[2]Санкт-Петербургский политехнический университет Петра Великого

Волоконно-оптические датчики широко используются при обслуживании разветвленной волоконно-оптической сети. Исследованный волоконно-оптический датчик акустического воздействия показал высокую чувствительность в заданном спектральном диапазоне. Потенциальное удобство такого датчика в возможности интеграции в комплексную систему сбора данных, в том числе со спектральным уплотнением.

охранные системы, видеосистемы, оптические датчики.

Волоконно-оптические системы находят все более широкое применение в самых разных областях. Одно из важных преимуществ таких систем является возможность интегрировать данные различных устройств и осуществлять их передачу на значительные расстояния в ситуациях, когда применение других способов затруднено или невозможно, например, в зоне высоких электромагнитных помех, в том числе техногенного происхождения, высоких температур, высокой взрыво- и пожарной опасности и т. д.

Для контроля над ситуацией на территории объекта применяются методы видеонаблюдения [1, 2, 3], контроля температуры, давления и других параметров [4], концентрации опасных химических веществ [5, 6] и т. д. Использование волоконной оптики дает возможность удаленного и в тоже время оперативного и надежного наблюдения территории распределенного объекта.

Когерентные волоконно-оптические системы обладают наиболее высокой чувствительностью, большим динамическим диапазоном регистрации сигнала, разнообразием форм чувствительного элемента, возможностью интеграции в комплексные информационные системы, передачи данных на большие расстояния [4]. Одним из вариантов исполнения является волоконно-оптический датчик давления.

Экспериментально исследовался волоконно-оптический датчик давления фазового типа с селективно избирательной частотной характеристикой

в заданном спектральном диапазоне. Для этого использовался тонкостенный акустический экран.

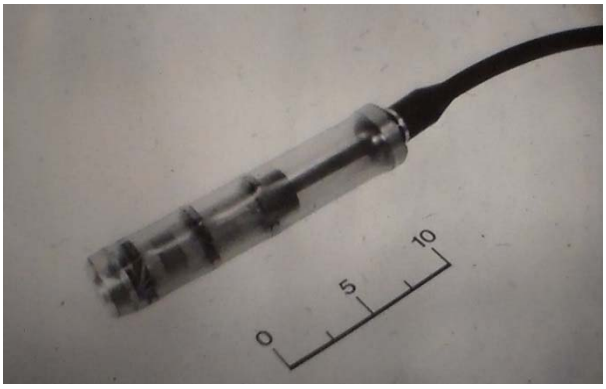


Рис. Внешний вид чувствительного элемента акустического волоконно-оптического датчика, погруженного в воду

Использование в конструкции специальных материалов для каркаса позволило достичь достаточно высокого значения чувствительности к давлению при минимизированной восприимчивости к флуктуациям температуры. Параметры конструкции рассчитывались по методу импедансов [7]. При создании датчика использовались анизотропные волоконные световоды, удерживающие состояние поляризации, типа PANDA. Параметры схемы обработки регистрируемого сигнала подбирались в соответствии с заданным рабочим диапазоном [8, 9, 10, 11].

Измерения характеристик датчика проводились в условиях, приближенных к естественным. Волоконно-оптический датчик помещался в бассейн, где создавалось акустическое поле определенной частоты.

Представленный на рисунке датчик обеспечивал регистрацию внешнего акустического воздействия в диапазоне 1…10 кГц. Динамический диапазон линейного режима датчика составил 50 дБ, чувствительность S = 2,5 мВ/Па при мощности оптического излучения на выходе 1,5 мкВт.

Данный волоконно-оптический датчик акустического воздействия, практически нечувствительный к низкочастотным шумам, обладающий высокой чувствительностью в рабочем спектральном диапазоне, может использоваться и как одиночный приемник, и в мультиплексной сенсорной системе, например, со смещенными частотными фильтрами. Представляет интерес также удобство интеграции в комплексную волоконно-оптическую систему со спектральным уплотнением [3].

Список используемых источников

1. Андреева Е. И., Купцов В. Д., Валюхов В. П., Пономарев Л. В. Волоконная оптика в системах видеонаблюдения и охранной сигнализации // Сети. Network world. 2000. № 3.

2. Андреева Е. И., Купцов В. Д., Валюхов В. П. Волоконно-оптическая система видеонаблюдения производственного объекта: функции охраны и технологического контроля // Актуальные проблемы инфотелекоммуникаций в науке и образовании. VII Международная научно-техническая и научно- методическая конференция: сб. науч. ст. в 4-х т. СПб. : СПбГУТ, 2018. Т. 1. С. 57–66.

3. Андреева Е. И., Купцов В. Д., Валюхов В. П. Передача высококачественного видеосигнала по волоконно-оптической сети с CWDM // Актуальные проблемы инфотелекоммуникаций в науке и образовании. VIII Международная научно-техническая

и научно-методическая конференция: сб. науч. ст. в 4-х т. СПб. : СПбГУТ, 2019. Т. 1. С. 56–65.

4. Волоконно-оптические датчики / Под ред. Удда Э. М. : Техносфера. 2008. 520 с.

5. Купцов В. Д., Кянджециан Р. А., Кателевский В. Я., Валюхов В. П. Газоанализаторы на основе эффекта молекулярных ядер конденсации // Научно-технические ведомости СПбГПУ. Информатика. Телекоммуникации. Управление. 2010. № 6. С. 145–150.

6. Kuptsov V. D., Valyukhov V. P., Katelevsky V. Y., Rybin E. N. Light scattering by aerosol particles and air in the molecular condensation nuclei (MCN) detector // Proceedings of SPIE - The International Society for Optical Engineering 4. 2014. P. 92050Q.

7. Andreeva E. I., Smirnova N. Yu. ISFOC'91 Proceedings 25–29 March 191. V. 2. p. 63.

8. Aladov A. V., Chernyakov A. E., Zakgeim A. L., Kuptsov V. D., Valyukhov V. P. Spatial distribution of current density and thermal resistance of high-power alingan vertical and face-up light-emitting diodes // Proceedings of SPIE – The International Society for Optical Engineering 7. Сер. "Optical Design and Testing VII". 2016. P. 100210X.

9. Купцов В. Д., Валюхов В. П. Чувствительность фотоприемных устройств волоконно-оптических линий связи // Научно-технические ведомости СПбГПУ. 2010. Т. 113. № 6. С. 31–37.

10. Купцов В. Д., Валюхов В. П. Чувствительность фотоприемного устройства на основе интегратора фототока // Электромагнитные волны и электронные системы. 2014. Т. 19. №7. С. 16–23.

11. Андреева Е. И., Сергеев А. Н. Измерители мощности для волоконно-оптических систем // Мир связи Connect. 2001. №10. С.78–83.

УДК 004.056.5
ГРНТИ 20.15.05

DLP-СИСТЕМА ДЛЯ ЗАЩИТЫ КОРПОРАТИВНЫХ ИЛИ ПЕРСОНАЛЬНЫХ ДАННЫХ

В. И. Андрианов, Д. В. Бахтин, С. И. Штеренберг

Санкт-Петербургский государственный университет телекоммуникаций им. проф. М. А. Бонч-Бруевича

Потеря информации – это одна из основных проблем современности. В настоящее время в компаниях всё больше внимания уделяют внешним угрозам, однако внутренние угрозы могут нанести компании куда более значительный ущерб, чем злоумышленники за ее пределами.

Термин DLP (Data Loss Prevention) система – это программный продукт, созданный для предотвращения утечек конфиденциальной информации за пределы корпоративной сети. Принцип работы DLP-системы состоит в анализе всех данных: входящей, исходящей и непосредственно данных внутри компании. Система с помощью определенных алгоритмов анализирует, что это за данные и в при необходимости, если они критичные и отправляются туда куда им не следует, блокирует передачу и/или сообщает об этом ответственного сотрудника.

DLP, DLP-системы, Data leak prevention, средства защиты информации, информационная. безопасность.

Комплексный программный продукт SecureTower предназначен для обеспечения внутрикорпоративной информационной безопасности посредством перехвата и анализа сетевого трафика, данных, переданных на внешние устройства, локальные сетевые ресурсы, облачные хранилища, локальные и сетевые принтеры. Система осуществляет контроль и анализ активности пользователя на компьютере (нажатия клавиш клавиатуры, содержимое буфера обмена и т. п.) и поддерживает возможность мониторинга аудиопотоков со звуковых устройств и видео с рабочих столов и веб-камер компьютеров, а также контроль изменений файловых систем компьютеров в режиме реального времени (рис. 1, см. ниже) [1, 2, 3, 4, 5].

Данное решение позволяет контролировать утечку и нежелательное распространение конфиденциальной информации через Интернет, перехватывая входящие и исходящие сообщения электронной почты, переписку в программах мгновенных сообщений, переданные документы, файлы, веб-страницы и т. д.

В системе поддерживаются функции блокирования исходящего сетевого трафика, переданного по HTTP, SMTP, MAPI и их шифрованным аналогам, а также возможность контроля доступа и использования внешних устройств, облачных хранилищ, локальных сетевых ресурсов и приложений [6, 7, 8, 9, 10].

Клиентская часть продукта содержит Консоль администратора и Консоль пользователя и служит в качестве графического интерфейса пользователя (рис. 2–3, см. ниже).

1) Центральный сервер сохраняет всю поступившую от других компонентов информацию в базы данных, настроенные для этих целей.

2) Сервер индексирования производит построение индексов информации, находящейся в базе данных, с последующим сохранением индексов в свое хранилище. В дальнейшем поиск будет осуществляться только по файлам поискового индекса, а не по всему объему информации, хранимой в базе данных. При обнаружении голосовых сообщений и изображений, а также документов других форматов, требующих распознавания текстовой информации и печатей, Сервер индексирования передает такие данные свободному Серверу распознавания. Результаты распознавания Сервер индексирования запрашивает у Сервера распознавания и производит их индексирование.

3) Сервер позволяет управлять данными о пользователях локальной сети, создавать карточки пользователей, объединять пользователей по определенным группам, а также отвечает за аутентификацию пользователей при доступе в систему.

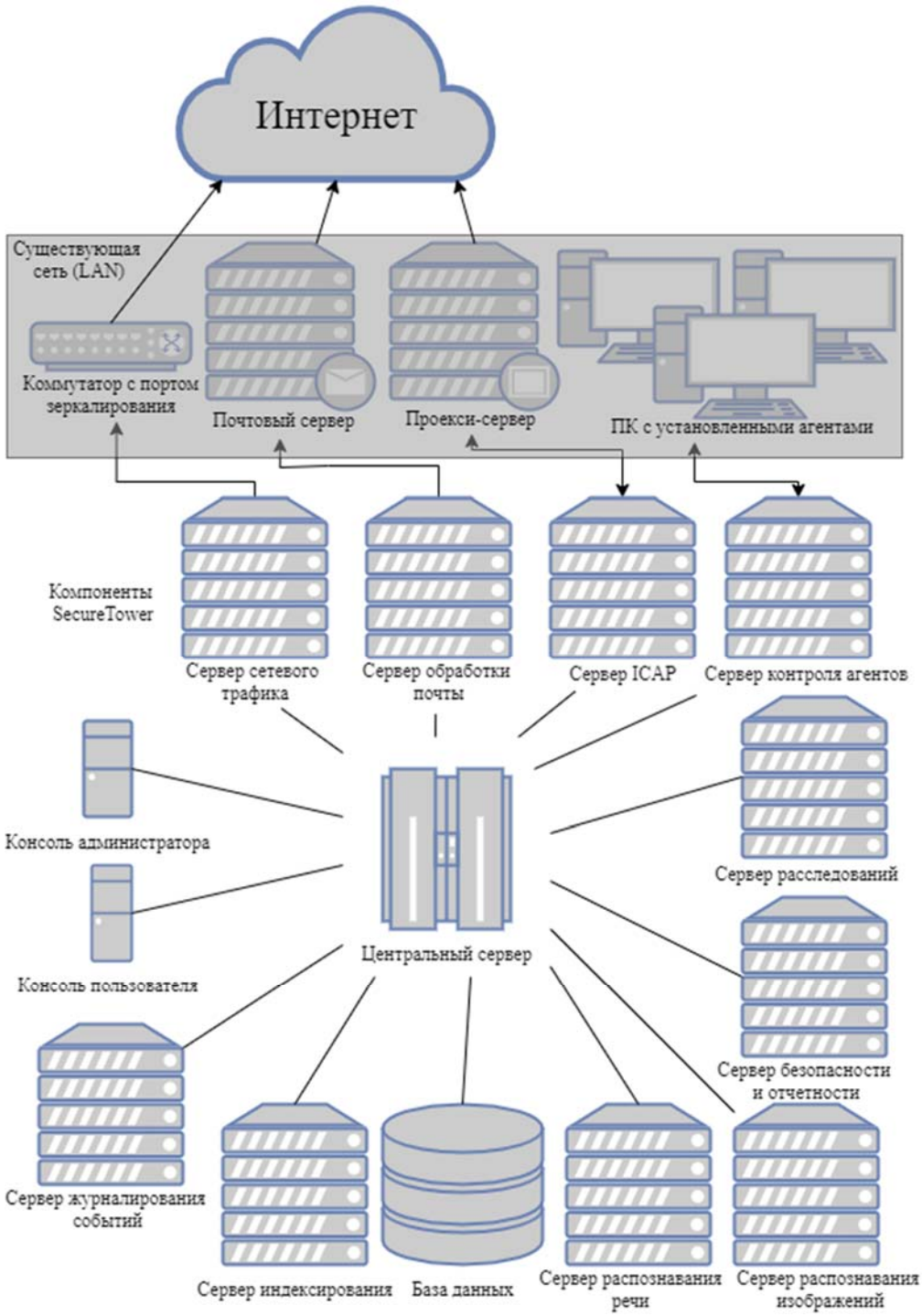


Рис. 1. Схема взаимодействия компонентов DLP-системы Falcongaze SecureTower 6.0

4) Сервер контроля агентов производит удаленную установку агентов на компьютеры локальной сети. Агенты отслеживают данные, которыми обмениваются пользователи программ Skype, Telegram, Microsoft Lync, Viber, Google Hangouts, WhatsApp или передающиеся по шифрованным каналам и на подключенные устройства, и отправляют их серверу для обработки. Сервер, в свою очередь, направляет полученную от агентов информацию на Центральный сервер для сохранения во внешнем хранилище данных.

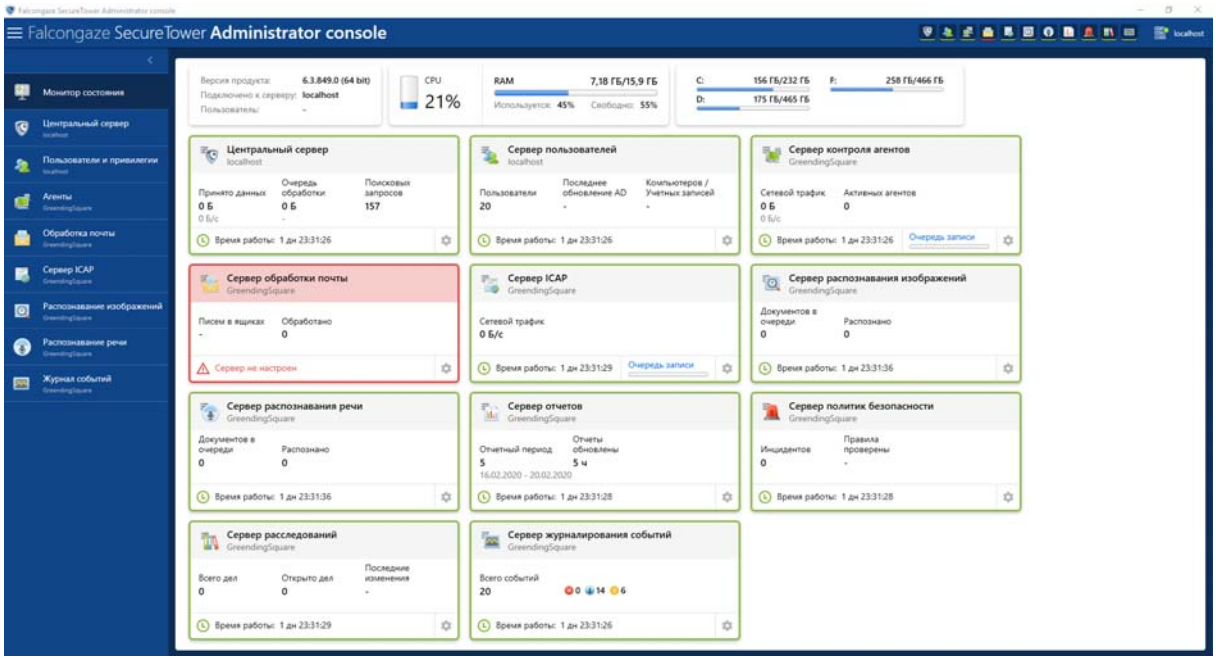


Рис. 2. Консоль администратора

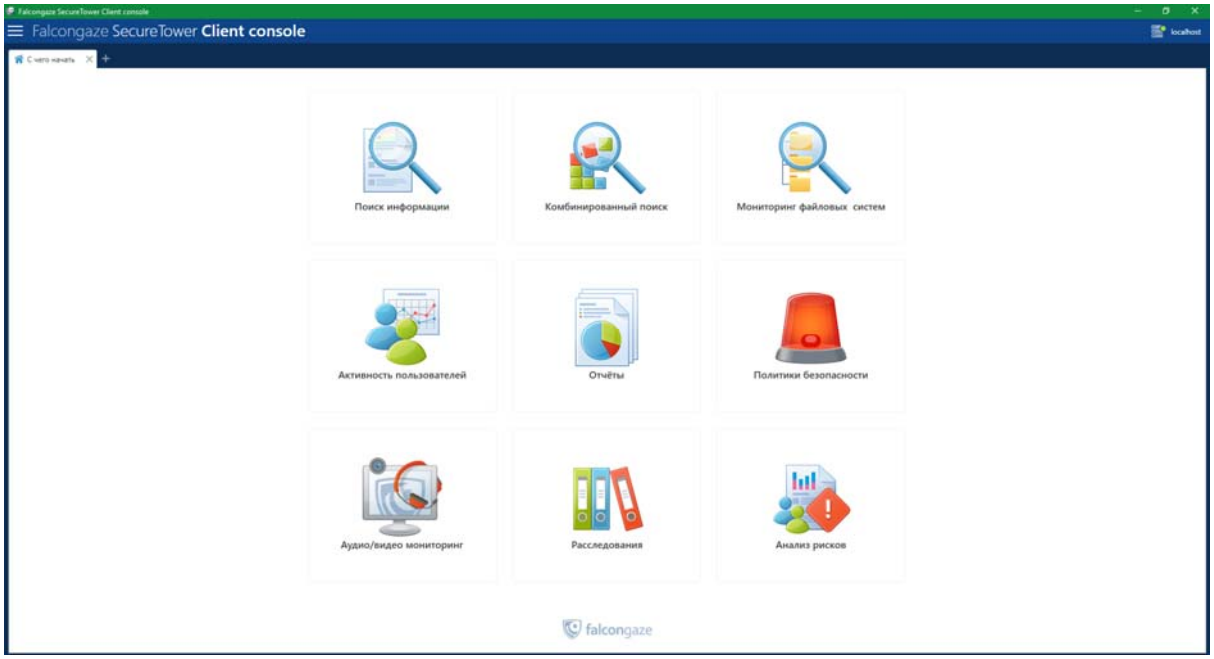


Рис. 3. Консоль пользователя

5) Сервер обработки почты перехватывает почтовые сообщения с почтовых серверов компании и передает их на Центральный сервер для сохранения во внешнем хранилище данных.

6) Весь внешний трафик дублируется и направляется к Серверу сетевого трафика при помощи коммутатора с портом зеркалирования. На Сервере сетевого трафика осуществляется анализ полученного трафика, в ходе которого выделяется необходимая информация (электронные письма,

файлы, сообщения и т. д.) и передается на Центральный сервер для сохранения во внешнем хранилище данных.

7) ICAP-сервер анализирует и перехватывает HTTP-трафик, передаваемый через прокси-сервер организации, и передает полученные результаты на Центральный сервер для сохранения во внешнем хранилище данных.

8) Сервер распознавания изображений обрабатывает получаемые от Сервера индексирования документы и распознает в них фрагменты текста и печати.

9) Сервер распознавания речи обрабатывает получаемые от Сервера индексирования документы и распознает голосовые коммуникации в фрагменты текста.

10) Сервер расследований организует работу в рамках расследований инцидентов безопасности. Он позволяет создавать дела и структурировать в группы информацию по отдельным расследованиям, прикреплять лиц, причастных к расследованию, а также документы из результатов поиска и внешние файлы, сохранять неограниченное время архивы и согласно внутренним стандартам организации оформлять дела для сдачи во внешний архив. Сервис предоставляет возможность вести досье, распечатывать и экспортировать дела для передачи другим сотрудниками, а также совместно работать с документами в реальном времени.

С учетом известных особенностей утечек информации, а также факторов, формирующих эту картину, наиболее приемлемым подходом следует признать создание и использование таких систем защиты, которые позволяют контролировать конкретных типы информации ограниченного доступа, проводить «глубокий» мониторинг «проблемных» каналов передачи информации. Кроме того, необходимо акцентировать внимание на всестороннем применении анализа поведения сотрудников в жесткой привязке к их роли в компании, объему прав доступа к информации. В идеальном случае такая защита дополняется решением для противодействия внешним атакам.

Список используемых источников:

1. Боридько И. С. Забелинский А. А. Коваленко Ю. И. Применение DLP-систем для защиты персональных данных // Безопасность информационных технологий. 2012. С. 20–24.

2. Боридько И. С. Забелинский А. А. Коваленко Ю. И. DLP-система: Защита от инсайдеров // Безопасность информационных технологий. 2013. С. 82–84.

3. Каскинов И. И. Галимов Р. Р. Анализ эффективности DLP-систем // Современные информационные технологии в науке, образовании и практике. 2014. С. 128–130.

4. Ихсанова А. А. Умутбаев Э. И. Файрузов Р. А. Обзор современных DLP-систем // Роль и место информационных технологий в современной науке. 2015. С. 26–30.

5. Ихсанова А. А. Умутбаев Э. И. Файрузов Р. А. Исследование рынка DLP-систем // Международная молодежная конференция «XXII Туполевские чтения (Школа молодых ученых)». 2015. С. 104–109.

6. Каширина Е. А. DLP-системы как средство защиты информации // Роль и место информационных технологий в современной науке. 2016. С. 17–19.

7. Израилов К. Е. Методика оценки эффективности средств алгоритмизации, используемых для поиска уязвимостей // Информатизация и связь. 2014. № 3. С. 44–47.

8. Буйневич М. В., Щербаков О. В., Владыко А. Г., Израилов К. Е. Архитектурные уязвимости моделей телекоммуникационных сетей // Научно-аналитический журнал Вестник Санкт-Петербургского университета Государственной противопожарной службы МЧС России. 2015. № 4. С. 86–93.

9. Шемякин С. Н., Гельфанд А. М., Холоденко В. Ю., Орлов Г. А., Ходжаев Ш. А. У. Описание разнообразных ddos атак с использованием botnet // Colloquium-journal. 2019. № 23–2 (47). С. 52–53.

10. Виткова Л. А. Исследование распределенной компьютерной системы адаптивного действия // Наукоемкие технологии в космических исследованиях Земли. 2015. Т. 7. № 5. С. 44–48.

УДК 004.056.57
ГРНТИ 20.15.05

АНАЛИЗ СУЩЕСТВУЮЩИХ ПЕНТЕСТ ЛАБОРАТОРИЙ

В. И. Андрианов, В. В. Стасюк, С. И. Штеренберг

Санкт-Петербургский государственный университет телекоммуникаций им. проф. М. А. Бонч-Бруевича

На данный момент на базе кафедры ЗСС нет как таковой пентест-лаборатории, которая могла бы использоваться в целях постоянного обучения и развития навыков у сотрудников и студентов. Студенты сами разворачивают инструменты и уязвимые системы для тестирования, что отнимает большое количество времени на установку, настройку и начало эксплуатации временной лаборатории. Учебный курс на кафедре ЗСС направлен на изучение уязвимостей персональных компьютеров под управлением операционных систем Windows 7 и Windows XP, уязвимостей беспроводных сетей с защитой WPA и ниже и уязвимостей web-страниц. Инструментом для тестирования являлся комплекс из Raspberry Pi 3 или стационарного персонального компьютера и операционная система Kali Linux со стандартным инструментарием.

Pentest, Kali-linus, Penetration test, Пентест, информационная. безопасность.

Объектами изучения были уязвимости в области пользователей, операционные системы windows, простая беспроводная сеть с пониженной защитой и web-сайт back-end которого написан на старых версиях языков программирования, которые имели множество уязвимостей. Данные объекты позволили ознакомится с основами пентеста, но из-за их слабости в защите,

отсутствовал аспект вариативности и поиска уязвимости, который и закладывается в основу тестирования на проникновение (рис. 1) [1, 2, 3].

На данный момент большинство сервисов переходит в web-пространство, Microsoft преобразует свои продукты в web-сервисы (Office), Google развивает свои Web-сервисы (Документы, Почта, Календарь и т. п.)

Рис. 1. Инструменты тестирования

В связи с этим развиваются действия и подходы злоумышленников относительно web-среды. Стандартный web-сервис состоит из сервера, обрабатывающего запросы и выдающего результат, хранилище данных, это может быть база данных реляционная или не-реляционная, или хранилища браузера, находящиеся на стороне пользователя, back-end-части, которая обрабатывает запросы пользователя и производит расчеты для вывода результата и front-end-часть, которая производит отрисовку визуальной составляющей сервиса и принимает запросы пользователя (фильтры, кнопки, изменение информации).

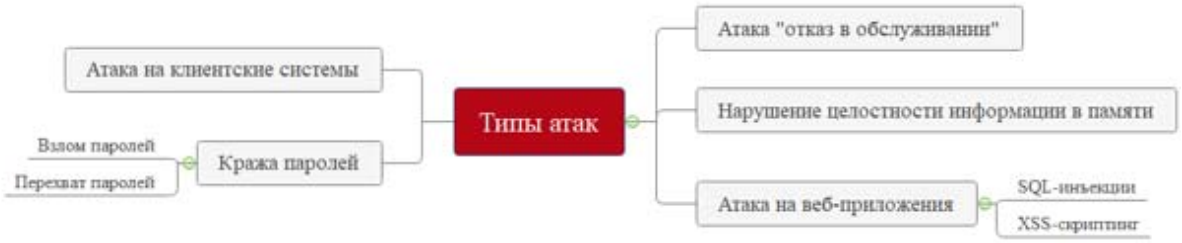


Рис. 2. Типы атак со стороны злоумышленника

Соответственно, злоумышленники стараются воздействовать на одну из этих компонентов в текущее время используя новые подходы и методы. Существуют следующие типы атак, используемые злоумышленниками (рис. 2).

В мире, в основном, компании делают свои площадки для развития сотрудников, и они закрыты, но есть немного общедоступных лабораторий, созданные энтузиастами и обновляющиеся относительно запросов пользователей и актуальности проблем на данный момент времени [3, 4, 5].

На данный момент есть следующие открытые пентест лаборатории:

1) Pentestit Test Lab v.N.
2) HackTheBox.
3) GhostSec`s.
4) Enigma.

Pentestit. Каждый год компания Pentestit запускает новую лабораторию для тестирования на проникновение «Test Lab» (рис. 3).

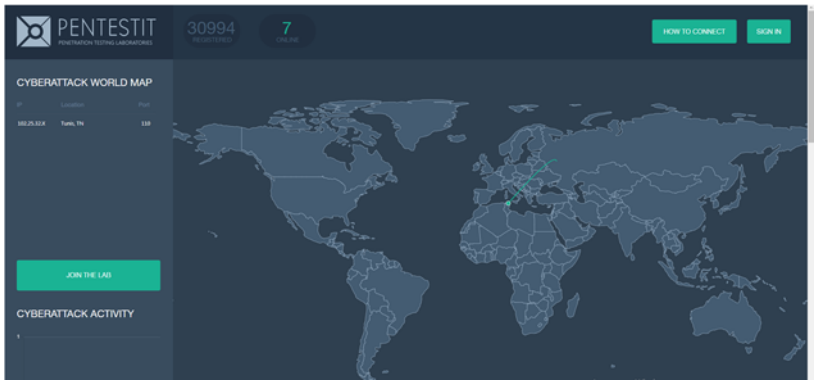


Рис. 3. Главная страница лаборатории

Лаборатория находится удаленно и для подключения к ней, требуется настроить VPN подключение, инструкция находится на этом же сайте. После подключения, пользователь получает возможность изучать систему, что в ней находится и производить некие действия, никакой информации изначально не дается, система представляет собой изначально «черный ящик», который мы можем исследовать.

В лаборатории можно изучить разные аспекты тестирования, начиная от изучения сети, заканчивая изучением скриптовых файлов на серверах для получения информации о хранящихся файлах и предназначении сервера.

Enigma. Компания Enigma Group, аналогично Pentestit проводит открытые пентест лаборатории с некой периодичностью (рис. 4).

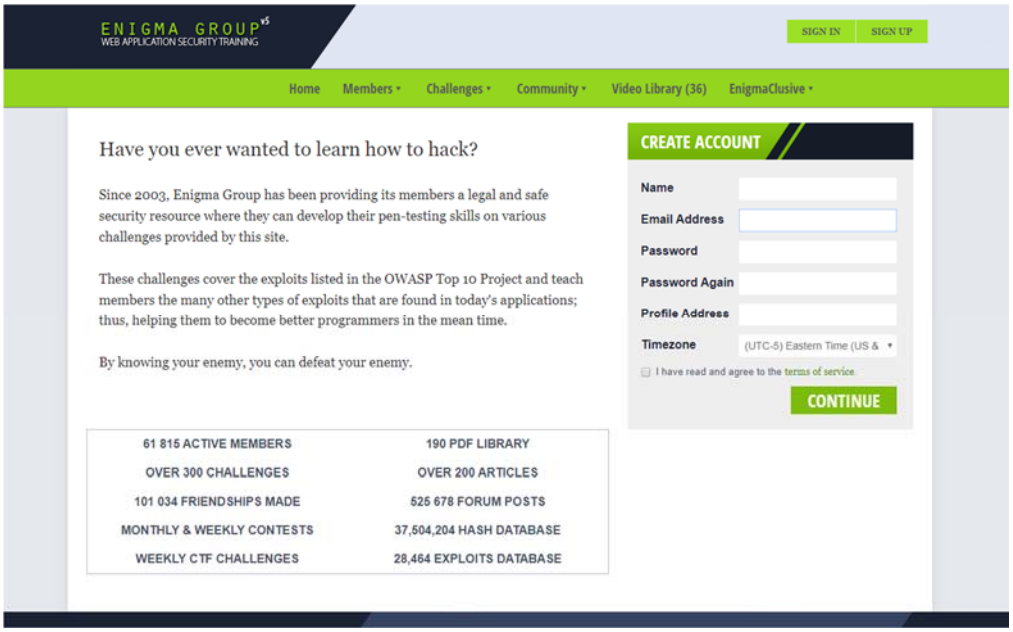


Рис. 4. Главная страница Enigma Group

Данная лаборатория направлена на изучение уязвимостей именно web-систем и технологий. Кроме пентест лаборатории, у Enigma Group есть так же и «челенджи» – задания, которые позволяют от начала и до конца изучить особенности тестирования на проникновения web-сервисов (рис. 5).

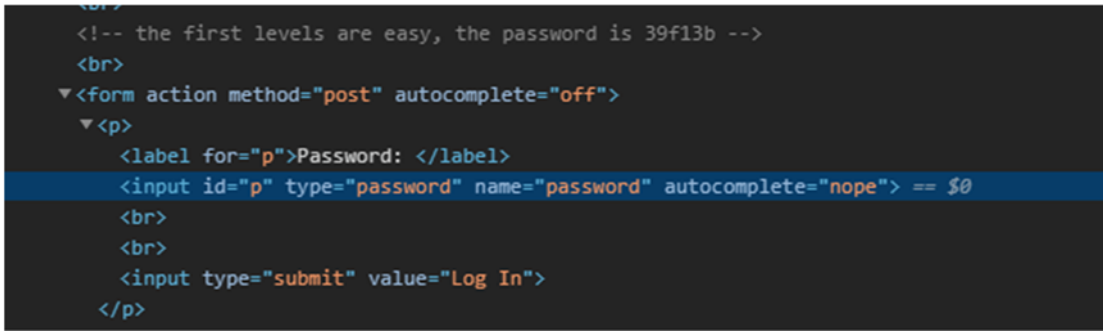


Рис. 5. Пример одного из первых заданий Enigma

GhostSec`s. Лаборатория общедоступна, никаких заданий в себе не имеет, на официальном сайте только страница с подключением к лаборатории, периодически бывает не доступна, по не понятным причинам т. к. нету информаирования от создателей (рис. 6).

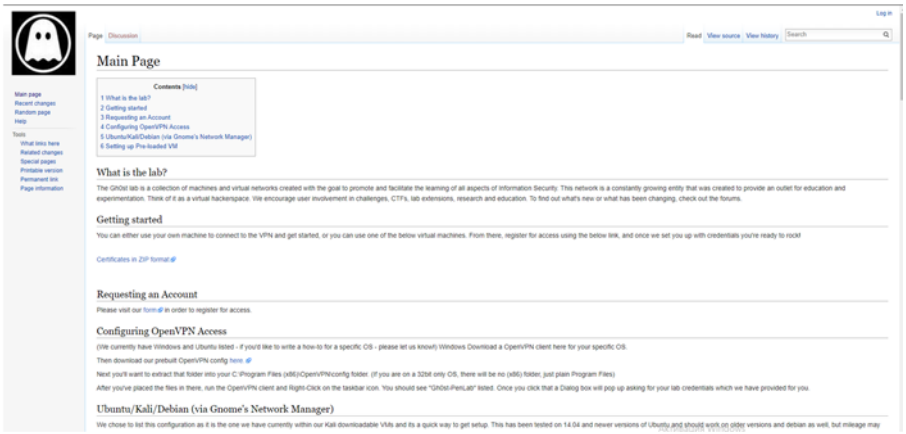


Рис. 6. Стартовая страница лаборатории

HackTheBox платформа с заданиями, соревновательным элементом и 30 подготовленными сегментами ИТ инфраструктуры для пентеста. Доступ к лаборатории доступен по инвайт-регистрации аккаунта, в системе, реализована связь между заданиями и аккаунтом пользователя (рис. 7) [6, 7, 8].

Подводя итог рассмотрение общедоступных пентсест лабораторий, можно выразить характеристики, которыми лаборатория должна обладать:

1) Свободный доступ из любого места, позволяющий пользователю производить обучение удаленно.

2) Современные объекты исследования, лаборатория должна иметь актуальные версии ОС, сетевых устройств и инструментов создания сайтов.

Рис. 7. Стартовая страница HackTheBox

3) Использование соревновательного или целевого компонента, для структурирования обучения пользователя и наличия аспекта мотивации.

4) Задания должны приводить к результату, применяемому моментально на практике.

5) Наличие готового инструментария для тестирования.

Список используемых источников

1. Казыханов А. А. Байрушин Ф. Т. Pentest как основа обеспечения безопасности на средних и крупных предприятиях // Символ науки. 2016. С. 50–51.

2. Галиева Л. Д. Аюпова А. Р. Что такое «Pentest» и для чего он нужен? // Достижения и приложения современной информатики, математики и физики. 2018. С. 562–567.

3. Переспелов А. В. Дубинина К. В. Матросова С. А. Проведение атаки ARP в Kali Linux для пентестинга безопасной передачи пакетов // Устойчивое развитие науки и образования. 2019. С. 114–116.

4. Пасюков А. А. Якимов А. С. Николаев С. В. Баженов Р. И. Использование Пентеста для обучения специалистов в направлении информационной безопасности // Постулат. 2017. С. 119.

5. Евтеев А. В. Ильин Д. В. Тестирование информационных систем на уязвимости // Информатика и вычислительная техника. 2019. С. 88–92.

6. Сторожук Н. Л., Зюзин А. Н., Ясинский С. А. Формализованный подход к применению метода наложения для принятия решения на модернизацию и развитие транспортных сетей связи // Информация и космос. 2018. № 4. С. 15–19.

7. Красов А. В., Сахаров Д. В., Тасюк А. А. Проектирование системы обнаружения вторжений для информационной сети с использованием больших данных // Наукоемкие технологии в космических исследованиях Земли. 2020. Т. 12. № 1. С. 70-76.

8. Душин, С. Е., Красов А. В., Литвинов Ю. В. Моделирование систем и комплексов. СПб. : СПбГУ ИТМО, 2011. 178 с.

УДК 004.031.43
ГРНТИ 49.43.29

ПРИМЕНЕНИЕ ГИБРИДНЫХ СИСТЕМ ПОЗИЦИОНИРОВАНИЯ В КОНЦЕПЦИИ ИНДУСТРИАЛЬНОГО ИНТЕРНЕТА ВЕЩЕЙ

А. С. Анисимов, Д. С. Кукунин

Санкт-Петербургский государственный университет телекоммуникаций им. проф. М. А. Бонч-Бруевича

Системы внутреннего позиционирования – технология, направленная на отслеживание местоположения объектов в реальном времени, сбор и анализ полученных данных для повышения безопасности труда и увеличения эффективности предприятия. Произведен обзор технологий, методов и подходов, применяемых в системах внутреннего позиционирования. Были выявлены недостатки существующих решений применительно к индустриальному интернету вещей.

системы позиционирования, индустриальный интернет вещей, Bluetooth Low Energy, Wi-Fi.

В настоящее время активно развивается индустриальный интернет вещей – концепция использования Интернета вещей, появившаяся благодаря переосмыслению индустриальных процессов и началу четвертой промышленной революции. Она характеризуется отсутствием границ между цифровой и производственной сферами. Ключевыми особенностями революции являются цифровизация и роботизация производств. Индустриальный интернет вещей помогает компаниям принимать правильные решения для повышения рентабельности производств, минимизировать производственные риски, сочетает в себе сбор данных через множество датчиков, объединенных в единую сеть, и аналитику этих данных, что позволяет по-новому взглянуть на методы оптимизации бизнес-процессов.

Системы внутреннего позиционирования – системы, предоставляющие информацию о текущем местоположении объекта, позволяя отслеживать перемещение и использовать полученную информацию в различных ситуациях: от создания оптимального маршрута в музеях, анализируя перемещение туристов, до прокладывания безопасных путей для AGV (Автоматически управляемых транспортных средств), оценивая передвижение рабочих и оптимальный маршрут самой AGV.

Отличие систем внутреннего позиционирования от систем GPS (системы глобального позиционирования) заключается в корректном предо-

ставлении данных на открытой местности и зачастую с высокой погрешностью (более 5 метров). Внутри помещений же погрешность может достигать десятков метров. Для таких ситуаций и используются системы внутреннего позиционирования.

В системах внутреннего позиционирования широко используется несколько основных технологий – Wi-Fi, Bluetooth Low Energy, DECT, nanoLOC, ZigBee.

Применяемые технологии используют следующие методы позиционирования [1], представленные в таблице 1.

ТАБЛИЦА 1. Методы позиционирования

Название	Описание
Received Signal Strength (RSS)	Оценка местоположения строится на основании мощности сигналов базовых станций.
Angle of Arrival (AoA)	Позиция объекта определяется в пределах площади треугольника, получаемого в результате пересечения осей диаграмм направленности антенн трех ближайших базовых станций (аналог метода триангуляции).
Time of Flight (ToF)	Положение определяется временем прохождения сигнала с линейно-частотной модуляцией от объекта до базовой станции.
Time of Arrival (ToA)	Позиция оценивается по разнице между временем отправки сигнала объектом и временем получения его базовой станцией.
Time Difference of Arrival (TDoA)	Местоположение определяется исходя из отличия времени доставки сигнала, отправленного объектом, до нескольких базовых станций.
Round Trip Time (RTT)	Базовая станция отправляет сигнал объекту, после чего дожидается его ответа. Позиция оценивается по общему времени доставки и получения сигнала.
Location Patterning Techniques (LPT)	Положение объекта определяется на основании распознавания ранее записанных образов радиосигналов. Часто применяется совместно с методом RSS.
Inertial Measurement Unit (IMU)	Применяются методы инерциальной навигации с использованием датчиков движения объекта – акселерометра и гироскопа.

Основные преимущества и недостатки указанных технологий приведены в таблице 2 (см. ниже) [2, 3].

ТАБЛИЦА 2. Преимущества и недостатки технологий локального позиционирования

Название	Преимущества	Недостатки
DECT	Можно использовать существующую беспроводную сеть.	Масштабирование требует прокладывания проводной сети до каждой новой станции.
Wi-Fi	1) Можно использовать существующую беспроводную сеть. 2) Большое количество поддерживаемых устройств.	1) Необходимость увеличения базовых станций для обеспечения требуемой точности. 2) Сложная процедура настройки. 3) Высокое энергопотребление.
Bluetooth Low Energy	1) Малое энергопотребление. 2) Низкая стоимость модулей. 3) Высокая точность.	Ограниченное количество поддерживаемых топологий (точка-точка и точка-многоточка).
ZigBee	1) Малое энергопотребление. 2) Высокая отказоустойчивость за счет full-mesh топологии.	1) Закрытый протокол. 2) Необходимость построения отдельной сети позиционирования.
nanoLOC	1) Малое энергопотребление. 2) Высокая отказоустойчивость за счет full-mesh топологии. 3) Открытый протокол.	1) Небольшой радиус действия базовых станций. 2) Необходимость построения отдельной сети позиционирования.

Из таблицы 2 видно, что каждая технология имеет свои преимущества, но наибольшее распространение получили технологии Bluetooth Low Energy и Wi-Fi.

Системы, основанные на Wi-Fi имеют меньшую точность, но позволяют использовать существующую беспроводную локальную сеть предприятия (WLAN).

Bluetooth Low Energy имеет большую точность, но требует оснащения помещений дополнительными маячками.

Гибридные системы, сочетающие в себе несколько технологий позиционирования, позволяют нивелировать недостатки применяемых решений, используя необходимые преимущества отдельных технологий для достижения требуемой точности и энергопотребления в задачах позиционирования объектов в помещениях.

Существующие работы рассматривают использование технологий по отдельности [1, 4, 5] либо относительно офисных помещений, где дополнительная технология используется только для повышения точности позиционирования [6, 7, 8].

Произведен обзор существующих технологий, методов и подходов, используемых в системах внутреннего позиционирования. Были выявлены недостатки описанных решений применительно к индустриальному интернету вещей.

Авторами предполагается рассмотреть использование гибридных систем внутреннего позиционирования применительно к индустриальному интернету вещей в рамках выпускной квалификационной работы. Авторами планируется решение задачи организации системы позиционирования применительно к существующему производству с целью достижения наиболее эффективного управления ресурсами складского помещения, в частности оптимизация маршрутов AGV и повышение безопасности труда рабочих. Авторы считают, что особое внимание должно быть уделено энергоэффективной составляющей, которую обходят стороной многие исследователи данного вопроса.

Список используемых источников

1. Ассур О. С. Исследование и разработка методов повышения точности определения местоположения объектов в пространстве с использованием технологий беспроводных сетей: дисс. ... канд. техн. наук: 05.13.01 / Ассур Олег Сергеевич. М., 2017.

2. Овчинников С. Технологии локального позиционирования // Технологии и средства связи. 2014. № 3. – С. 26–30.

3. Поникар А. В., Евсеев О. В., Анциперов В. Е., Мансуров Г.К. Исследование возможности локального позиционирования в беспроводных сетях IEEE 802.15.4 // Материалы IV Всероссийской конференции «Радиолокация и радиосвязь» – ИРЭ РАН, 2010. Т. 29. С. 914–918.

4. Hengyotmark S. Indoor Localization Based on Round-Trip Time of Bluetooth Low Energy Beacons: дис. – Thammasat University, 2016.

5. Rida M. E. et al. Indoor location position based on bluetooth signal strength // 2015 2nd International Conference on Information Science and Control Engineering. IEEE, 2015. PP. 769–773.

6. Chen Y. C. et al. Sensor-assisted wi-fi indoor location system for adapting to environmental dynamics // Proceedings of the 8th ACM international symposium on Modeling, analysis and simulation of wireless and mobile systems. 2005. PP. 118–125.

7. Ассур О. С., Филаретов Г. Ф. Разработка комплексного метода позиционирования объектов по данным беспроводных сетей Wi-Fi и устройств BLE (Bluetooth Low Energy) // Известия Института инженерной физики. 2015. № 2. С. 2–10.

8. Baniukevic A., Jensen C. S., Lu H. Hybrid indoor positioning with Wi-Fi and Bluetooth: architecture and performance // Proceedings of the IEEE 14th International Conference on Mobile Data Management (MDM). 2013. V. 1. PP. 207–216.

УДК 004.732
ГРНТИ 49.43.29

ИССЛЕДОВАНИЕ РАБОТЫ WI-FI В МЕТРО САНКТ-ПЕТЕРБУРГА

Д. Г. Анисимов, Р. А. Дунайцев

Санкт-Петербургский государственный университет телекоммуникаций им. проф. М. А. Бонч-Бруевича

Три года назад на оранжевой (четвертой) линии Петербургского метрополитена была запущена в эксплуатацию бесплатная сеть Wi-Fi MT_FREE. К настоящему времени точками доступа оснащены все поезда и станции метро Санкт-Петербурга. В статье представлены результаты радиообследования сети MT_FREE. Приводятся данные по расположению точек доступа, используемым частотным диапазонам и задействованным каналам в подвижном составе и на платформах станций.

MT_FREE, Wi-Fi, беспроводная локальная сеть, радиообследование, точка доступа.

30 мая 2017 г. в метро Санкт-Петербурга прошла официальная церемония запуска бесплатной сети Wi-Fi [1]. Ввод в эксплуатацию проходил поэтапно с 30 мая по 6 декабря 2017 г.: сперва сеть заработала на Лахтинско-Правобережной (также известной как оранжевая) линии, в июне – на Фрунзенско-Приморской (фиолетовой), в августе – на Невско-Василеостровской (зеленой), в сентябре – на Московско-Петроградской (синей) и, наконец, в декабре была подключена Кировско-Выборгская (красная) линия [2]. Построением сети Wi-Fi занималась компания «МаксимаТелеком» [3], несколькими годами ранее развернувшая сеть бесплатного Wi-Fi в Московском метрополитене [4, 5]. В настоящее время «МаксимаТелеком» является крупнейшим оператором городского Wi-Fi, управляя Единой городской сетью Wi-Fi в Москве, сетями Wi-Fi в наземном городском пассажирском транспорте Москвы и Санкт-Петербурга, Казани и Магадана, а также в региональных аэропортах России [6]. Компания постоянно занимается расширением и модернизацией своей инфраструктуры [7, 8], а в январе 2020 г. В составе консорциума обеспечила запуск высокоскоростной сети Wi-Fi в подвижном составе метрополитена Дели [9]. Стоит отметить, что в Московском и Петербургском метро «МаксимаТелеком» зарабатывает на показе рекламы, которая загружается при подключении пользователя к сети MT_FREE. При этом ни городской, ни федеральный бюджеты не несут никаких расходов на строительство и обслуживание сети Wi-Fi [10, 11], а метрополитен даже получает от компании арендную плату за использование своей инфраструктуры. С целью компенсации затрат на создание сети Wi-Fi «МаксимаТелеком» также предлагает услуги таргетированной

рекламы для малого и среднего бизнеса [12, 13], в результате срок окупаемости проекта должен составить примерно 6–8 лет.

При первичном подключении к сети MT_FREE пользователю необходимо пройти обязательную идентификацию через подтверждение номера мобильного телефона или авторизацию на портале госуслуг. В дальнейшем пользователям, уже зарегистрированным в единой сети MT_FREE, повторное прохождение идентификации не требуется. В Петербургском метро беспроводная сеть является открытой, поэтому данные, передаваемые между точками доступа (ТД) и мобильными устройствами пользователей, не шифруются. Однако в скором времени ситуация может измениться в лучшую сторону: 3 сентября 2019 г. оператор сообщил о начале тестирования в Московском метро закрытой беспроводной сети с шифрованием [14]. Использование технологии Hotspot 2.0 позволит обеспечить конфиденциальность передаваемой информации, а также предотвратить автоматическое подключение к фишинговой ТД, запущенной злоумышленником для развлечения или кражи данных. Ожидается, что защищенный Wi-Fi останется бесплатным, а монетизация будет по-прежнему происходить за счет рекламы [15].

Целью исследования было определить расположение ТД в вагонах, используемые частотные диапазоны и каналы. Для этого была выбрана программа Ekahau Site Survey версии 9.0.3, устанавливаемая на ноутбуке. Радиообследование проводилось в непрерывном (continuous) режиме [16].

Подвижной состав состоит из нескольких промежуточных и двух головных вагонов. В зависимости от линии метрополитена длина составов варьируется от 6 до 8 вагонов. В каждом вагоне установлено по одной двухдиапазонной ТД Cisco AIR-CAP2702i 802.11a/b/g/n/ac со встроенными всенаправленными антеннами и поддержкой MIMO. Управление ТД внутри состава осуществляется виртуальным контроллером, запущенным на промышленном компьютере в кабине головного вагона. Расположение ТД внутри вагонов крайне редко можно определить визуально, так как обычно они скрыты под обшивкой.

На рис. 1 представлен тот редкий случай, когда ТД находится на виду. Однако эксперименты с измерением уровня сигнала от ТД внутри вагона показали, что ТД всегда располагается в противоположенной от приборной панели части вагона (рис. 2).

Рис. 1. ТД в одном из вагонов Кировско-Выборгской линии

В ходе работы был проведен ряд пассивных радиообследований подвижных составов разных моделей. На рис. 3 (см. ниже) в качестве примера представлен

случай, когда в одном из вагонов поезда (втором) по каким-то причинам не работала ТД. Но даже в этой ситуации мощности сигнала от соседних ТД из первого и третьего вагонов оказалось достаточно, чтобы обеспечить приемлемое покрытие почти во всем втором вагоне. Там же, где ТД работают исправно, уровень сигнала составляет от –65 дБм и выше.

Рис. 2. Уровень сигнала рядом с приборной панелью составляет примерно –61 дБм, тогда как в противоположном конце вагона от той же ТД – уже около –46 дБм

В подвижном составе Петербургского метрополитена все ТД в диапазоне 2,4 ГГц используют исключительно каналы 1, 6 и 11 шириной 20 МГц. В диапазоне 5 ГГц используются каналы шириной 80 МГц из блоков UNII-1, UNII-2 и UNII-3. На рис. 3 (см. ниже) можно отметить корректную работу виртуального контроллера данного поезда, организовавшего чередование непересекающихся каналов как в диапазоне 2,4 ГГц, так и в диапазоне 5 ГГц. Однако в некоторых составах наблюдалась ситуация, когда ТД соседних вагонов работали на одной и той же частоте, создавая внутриканальную интерференцию. Также следует отметить, что в сети MT_FREE активно используется механизм динамического распределения беспроводных клиентов по диапазонам – так называемый Band Steering.

Измерения уровня шума (*noise floor*) в каналах, проведенные с помощью анализатора спектра MetaGeek Wi-Spy DBx, показали следующие значения. В диапазоне 2,4 ГГц средний уровень шума составляет около –87 дБм, а в диапазоне 5 ГГц – примерно –93 дБм.

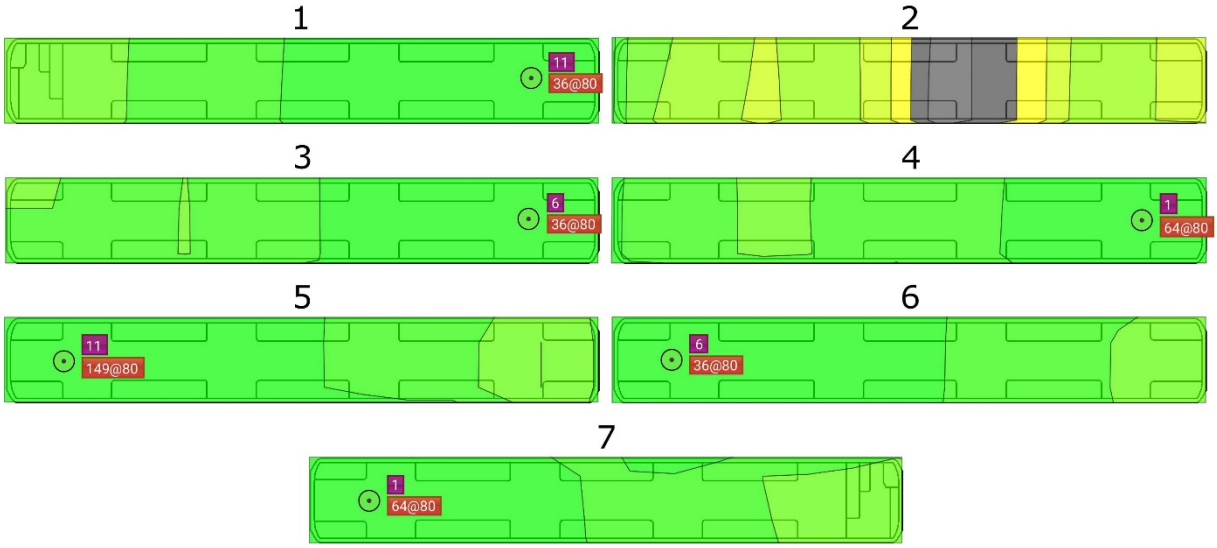


Рис. 3. Карта радиопокрытия в поезде Лахтинско-Правобережной линии

В настоящий момент подключиться к сети Wi-Fi можно не только в вагонах поездов, но и на платформах 62 станций из 72 действующих. Как правило, ТД находятся в отдельных стойках посередине платформ. В редких случаях ТД могут располагаться на стене под потолком (рис. 4, см. ниже). Однако расположение ТД на платформах не всегда можно назвать удачным. На платформах десяти станций (Волковская, Горьковская, Международная, Московские ворота, Новочеркасская, Обводный канал, Пионерская, Приморская, Сенная площадь, Электросила) ТД расположены не самым лучшим образом, из-за чего к ним происходит не так много подключений. На платформах еще семи станций (Гостиный двор, Достоевская, Лиговский проспект, Невский проспект, Площадь Александра Невского 2, Площадь Ленина, Спасская) ТД и вовсе «спрятаны» от пассажиров. Порой это, конечно, может быть оправданно колоссальным пассажиропотоком, как, например, на станции метро «Гостиный двор», но в остальных случаях такое расположение представляется нерациональным. С плохой работой Wi-Fi на станциях и переходах как раз и связано основное число жалоб пользователей [17].

Рис. 4. ТД на платформах Петербургского метрополитена

Список используемых источников

1. MT_FREE: в петербургском метро появился бесплатный Wi-Fi [Электронный ресурс]. URL: https://nevnov.ru/486358-mtfree-v-peterburgskom-metro-poyavilsya-besplatnyi-wi-fi (дата обращения 30.03.2020).

2. Беспроводной интернет теперь доступен на всех Линиях метрополитена [Электронный ресурс]. URL: http://www.metro.spb.ru/news/item/id/1464 (дата обращения 30.03.2020).

3. Wi-Fi под Невой: как мы построили сеть в самом глубоком метро мира [Электронный ресурс]. URL: https://habr.com/ru/company/maximatelecom/blog/348420/ (дата обращения 30.03.2020).

4. Бесплатный Wi-Fi в метро [Электронный ресурс]. URL: https://mosmetro.ru/info/wifi-v-metro/ (дата обращения 30.03.2020).

5. WI-FI в метро: архитектура сети и подземные камни [Электронный ресурс]. URL: https://habr.com/ru/company/maximatelecom/blog/332538/ (дата обращения 30.03.2020).

6. О компании МаксимаТелеком [Электронный ресурс]. URL: https://maximatelecom.ru/about.html (дата обращения 30.03.2020).

7. Столичный Wi-Fi пройдет фильтрацию. Москва выбрала оператора городской сети беспроводной связи [Электронный ресурс]. URL: https://www.kommersant.ru/doc/3868330 (дата обращения 30.03.2020).

8. Скорость Wi-Fi в метро Москвы увеличится до 200 Мбит/с в течение года [Электронный ресурс]. URL: https://www.m24.ru/news/mehr-Moskvy/31012020/105797 (дата обращения 30.03.2020).

9. МаксимаТелеком обеспечила запуск Wi-Fi в поездах метро Дели [Электронный ресурс]. URL: https://maximatelecom.ru/news/339/maksimatelekom-obespechila-zapusk-wi-fi-v-poezdah-metro-deli (дата обращения 30.03.2020).

10. Совладелец «МаксимаТелеком» объяснил, почему только его компания раздает Wi-Fi в метро Петербурга [Электронный ресурс]. URL: https://www.dp.ru/a/2017/07/04/Soosnovatel_kompanii_Ma (дата обращения 30.03.2020).

11. Петербургский депутат попросил убрать рекламу при подключении к Wi-Fi в метро [Электронный ресурс]. URL: https://www.interfax.ru/russia/630939 (дата обращения 30.03.2020).

12. Оператор Wi-Fi московского метро запустит таргетированную рекламу [Электронный ресурс]. URL: https://iz.ru/news/593058 (дата обращения 30.03.2020).

13. Прошли мимо кафе, а вам тут же показали его рекламу? Это не паранойя [Электронный ресурс]. URL: https://meduza.io/feature/2018/10/24/proshli-mimo-kafe-a-vam-tut-zhe-pokazali-ego-reklamu-eto-ne-paranoyya (дата обращения 30.03.2020).

14. «МаксимаТелеком» шифрует Wi-Fi в метро [Электронный ресурс]. URL: https://www.comnews.ru/content/121793/2019-09-04/maksimatelekom-shifruet-wi-fi-v-metro (дата обращения 30.03.2020).

15. В метро Москвы заработал закрытый Wi-Fi с шифрованием [Электронный ресурс]. URL: http://www.tadviser.ru/index.php/Проект:Единая_Wi-Fi-сеть_"Московский_транспорт"_(MT_FREE) (дата обращения 30.03.2020).

16. Дунайцев Р. А., Лебедева Н. А. Об особенностях радиообследования сетей Wi-Fi // Актуальные проблемы инфотелекоммуникаций в науке и образовании. VIII Международная научно-техническая и научно-методическая конференция : сб. науч. ст. в 4-х т. СПб. : СПбГУТ, 2019. Т. 1. С. 423–428.

17. Wi-Fi в метро Петербурга: ловит хорошо, но не везде [Электронный ресурс]. URL: https://www.spb.kp.ru/daily/26767/3799969/ (дата обращения 30.03.2020).

УДК 004.71
ГРНТИ 50.39.02

СТАНДАРТ ПЕРЕДАЧИ ДАННЫХ RS485

А. В. Ануфренко, И. С. Русин, А. В. Щукин

Военная Академия Связи имени Маршала Советского Союза С. М. Буденного

В статье рассматривается стандарт передачи данных RS485. Данный интерфейс является наиболее распространенным интерфейсом физического уровня модели OSI для создания информационных сетей. Приводится подробное описание стандарта RS485, так же в статье размещены схемы со способами подключения различных устройств. Описаны достоинства и недостатки стандарта RS485.

протоколы сетей, виды соединений, рекомендованный стандарт, разработка, типы соединений, протокол обмена, приём данных, витая пара.

Интерфейс RS485 (*Recommended Standard* 485) – это один из наиболее широко используемых интерфейсов физического уровня модели OSI, используемый для формирования инфокоммуникационных сетей.

Основными достоинствами RS485 являются относительная простота реализации, высокая помехозащищённость, надежная передача данных на дальние расстояния, а также доступность высокоскоростного обмена данными. Исходя из определенных преимуществ совершается выбор в пользу данного интерфейса популярного во многих сферах деятельности (энергетике, промышленности, управлении процессами в производстве и других областях). Производители технических устройств предлагают множество датчиков, которые передают значения различных параметров (температура, влажность, давление и др.) с использованием этого интерфейса.

Часто RS485 предпочитают использовать для беспроводной передачи данных, что дает возможность надежно и быстро обмениваться информацией в сетях Wi-Fi или GSM. Беспроводная передача данных и ее применение увеличивает сферы использования устройств, оснащенных только интерфейсом RS485. Благодаря этому появляется возможность интегрировать их в современные системы сбора и передачи данных.

Поэтому производителям нет необходимости беспокоиться, его устройство еще долго будет оставаться актуальным и современным.

Широкое использованием наряду с регулярным производством новых семейств микросхем RS485 делает актуальным анализ данного интерфейса, чему и посвящена статья.

Разработкой двух ассоциаций: Ассоциации промышленности средств связи (TIA, *Telecommunications Industry Association*) и Ассоциации электронной промышленности (EIA, *Electronics Industries Association*) стал стандарт RS485.

RS485 – многоточечный последовательный интерфейс передачи данных работающий в полудуплексном режиме. С помощью дифференциальных сигналов по проводникам осуществляется передача данных. Зачастую используют единственную витую пару проводов для передачи и приёма данных. Стандарт RS485 охватывает только физический уровень и не включает:

– возможность объединения несимметричных и симметричных цепей;
– способы доступа к линии связи;
– аппаратную конфигурацию (среда обмена, кабель);
– типы соединителей, разъёмов, колодок, нумерацию контактов;
– протокол обмена;
– параметры качества сигнала, уровень искажений (%);
– качество источника питания (стабилизация, пульсация, допуск);
– отражённость и уровень сигнала.

Электрические и временные характеристики интерфейса:

– в текущий момент может быть активный только один передатчик;
– 32 приёмопередатчика при многоточечной конфигурации сети (на одном сегменте, максимальная длина линии в пределах одного сегмента сети: 1200 метров);
– ограничение по количеству сетевых узлов – 250 включая магистральные усилители.

Скорость обмена и длина линии связи:

– при длине 1200 м – 62,5 кбит/с;
– при длине 300 м –375 кбит/с;
– 500 кбит/с;
– 1000 кбит/с;
– при длине 100 м – 2400 кбит/с;
– при длине 10 м – 10000 кбит/с.

Для обмена данными со скоростью более 500 кбит/с в основном применяют экранированную витую пару [1].

Тип примененных в устройстве приемопередатчиков напрямую влияет на количество устройств, подключаемых к одной линии интерфейса.

Каждый передатчик имеет возможность управления 32 приемниками.

Значение входного сопротивления приемников может различаться: 1/2, 1/4, 1/8 от стандартного. При использовании таких приемников число устройств может увеличиваться: 64, 128, 256.

В некоторых случаях используют фреймы для отправки байтов данных (стартовый бит, биты данных, бит паритета, стоповый бит). Устройство, которое определили заранее является ведущим на магистрали и организует обмен запросами подчиненным устройствам, имеющим только разные логические адреса.

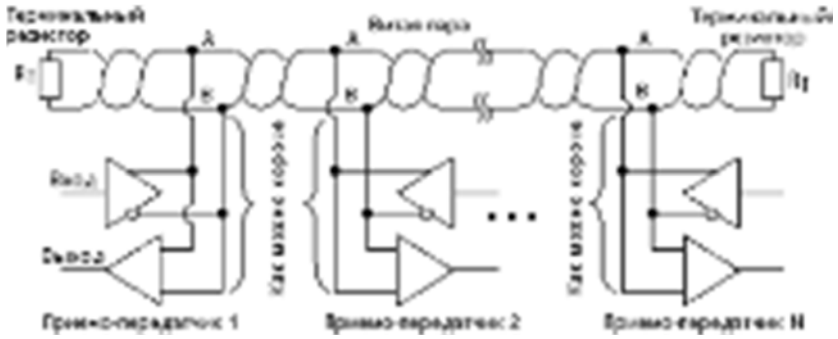


Рис. 1. Локальная сеть на основе интерфейса RS485,
с несколькими приемо-передатчиками

Витая пара является оптимальным решением для прокладки сети, т. к. хорошо защищена от наводок (рис. 1). В условиях, где повышены внешние помехи используют экранированную витую пару [2].

Достоинства стандарта RS485:

- хорошая защищенность от помех;
- большая дальность связи;
- однополярное питание;
- простая реализация драйверов;
- широковещательная передача;
- возможность многоточечного соединения.

Недостатки RS485:

- большое потребление энергии;
- отсутствие сервисных сигналов;
- возможность появления коллизий.

В сети может быть много передатчиков, так как они могут отключаются в режиме приема (рис. 2).

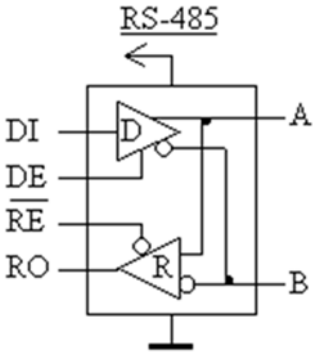


Рис. 2. Схема приемопередатчика
RS485

Описание контактов на схеме приёмопередатчика:

- Driver (D) – передатчик;
- Receiver (R) – приемник;
- Driver Input (DI) – контакт для подключения передатчика;
- Receiver Output (RO) – контакт для подключения приемника;
- Driver Enable (DE) – контакт для разрешения работы передатчика;
- Receiver Enable (RE) – контакт для разрешения работы приемника;

– A – контакт для подключения неинвертирующей линии сигнала;

– B – контакт для подключения инвертирующей линии сигнала.

Контакт для подключения приемника (RO) необходимо подключить к порту приемника UART (RX).

Контакт для подключения передатчика (DI) необходимо подключить к порту передатчика UART (TX). Так как на дифференциальной стороне соединены приемник вместе с передатчиком, то необходимо во время приема отключать передатчик, а когда происходит передача, то отключать приемник (рис. 3). Для этого предназначены управляющие контакты разрешения передатчика (DE) и разрешение приемника (RE). Для изменения приемника и передатчика с помощью одного сигнала с любого порта контроллера используется соединение с DE. При значении «0», устройство работает на прием, а при получении значения «1» – на передачу [3, 4].

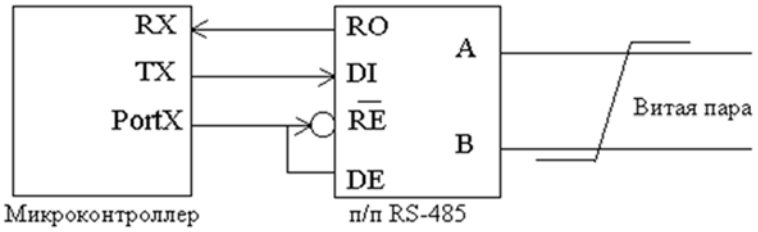


Рис. 3. Схема приемопередатчика RS485

На выходе RO переводит в цифровой сигнал в случае получением приемником на дифференциальных входах (AB) разность потенциалов.

Исходя из того, что передатчика имеет ограничения, отражается на количество приемников, которые могут быть подключенных к линии.

RS485 передатчик может вести до 32 приемников (с учетом согласующих резисторов).

Существует ряд микросхем с повышенным входным сопротивлением, что способствует подключению к линии более 32 устройств.

Стандарт RS485 – это основной стандарт первого физического уровня модели OSI передачи данных по последовательным асинхронным каналам связи.

Многие сетевые протоколы включают в себя стандарт RS485, например:

– Овен (НПО «Овен»);
– ModBus;
– DCON (ICP CON);
– ProfiBus DP;
– DH-485 (Allen Bradley);
– BitBus;

Многие международные и национальные стандарты его также поддерживают, например:

– CCITT V.10, CCITT V.11;
– IEEE 1118;
– DIN 66 259-3, DIN 66 259-4, DIN 66 348-2;
– ISO/IEC 8482.

Подводя итог анализа RS485, необходимо подчеркнуть, что информационная сеть, построенная с использованием данного интерфейса, делает систему безопасной и недорогой в реализации, что является конкурентным преимуществом для производителей. Регулярный выпуск современных семейств микросхем RS485, свидетельствует о его востребованности еще много лет.

Список используемых источников

1. Хелд Г. Технологии передачи данных. СПб. : БХВ, 2003. 720 с.
2. Калабеков Б. А. Микропроцессоры и их применение в системах передачи и обработки сигналов: М. : Радио и связь, 1988. 368 с.
3. Мячев А. А., Степанов В. Н., Щербо В. К. Интерфейсы систем обработки данных / Под ред. А. А. Мячева. М. : Радио и связь, 1989. 416 с.
4. Канаев А. К., Кудряшов В. А., Кузнецов В. Е., Лихачев А. М. Исследование и комплексное построение базовых подсистем электросвязи : монография. М. : ГОУ «Учебно-методический центр по образованию на железнодорожном транспорте», 2007. 253 с.

УДК 004.72, 004.77
ГРНТИ 49.34.01, 49.33.01

НАСТРОЙКА СТЕНДА ДЛЯ АНАЛИЗА СЕТЕВЫХ ХАРАКТЕРИСТИК BLOCKCHAIN СИСТЕМ

Е. А. Аптриева, В. С. Елагин, А. В. Спиркина

Санкт-Петербургский государственный университет телекоммуникаций им. проф. М. А. Бонч-Бруевича

В статье авторы рассказывают о настройке стенда для анализа сетевых характеристик, связанных с технологией Blockchain систем. Авторы описывают элементы сети Blockchain и структуру сети на экспериментальном стенде. Авторы показывают, какие ресурсы были задействованы, какой операционной системой пользовались, и на каких серверах был развернут стенд. В статье рассматриваются проблемы, связанные с передачей данных Blockchain на сети. Как трафик влияет на сеть, какую создают загрузку сети, можно ли с помощью данных Blockchain полностью загрузить сеть. Авторы представили результаты экспериментов и провели анализ по полученным

данным (графики результатов эксперимента и оценки эффективности экспериментальной сети).

Blockchain, Ethereum blockchain, DPI, Deep Packet Inspection.

В современном мире технология Blockchain является быстро развивающейся и распространяющейся технологией, поэтому возникает задача выяснения, каким образом данная технология влияет на сеть.

Технология Blockchain (дословно «цепь блоков») – это сеть с распределенной базой данных (реестром), в которой данные (в виде транзакций) записываются в блоки и выстраиваются по мере заполнения блоков цепочкой. Вся новая информация добавляется в новый блок и прикрепляется к предыдущему блоку. С помощью blockchain можно хранить любую информацию, например, информацию о кредитах, залогах, денежных переводах, бухгалтерию, тексты книг, информацию по оплате платежей.

Узел (*node*) – это устройство, которое клиент подключает к сети blockchain, с помощью которого выполняет задачи проверки и передачи транзакций. Также node получает копию blockchain, которая загружается автоматически при присоединении к сети.

В процессе обмена сообщениями технология blockchain генерирует дополнительный трафик, необходимый для обновления реестров на всех задействованных узлах. Таким образом, увеличивается объем служебного трафика, который появляется при шифровании данных и снижает долю полезного трафика. То есть то, что происходит на одном устройстве (узле) дублируется на все узлы, подключенные к сети, вследствие чего увеличивается количество передаваемых сообщений в n раз (где n – количество узлов, задействованных в сети). Такие данные передаются небольшими порциями в короткий промежуток времени, что приводит к резкому увеличению передаваемых сообщений и может негативно влиять на работу сети.

Существует множество платформ для реализации blockchain. На стенде была выбрана и развернута платформа Ethereum blockchain. Особенность сети Ethereum – особое построение, а создание блокчейна Ethereum возможно своими руками. В отличие от других криптовалют, авторы не ограничивают роль эфира платежами, а предлагают его, например, в качестве средства для обмена ресурсами или регистрации сделок с активами при помощи умных контрактов, в частности авторы назвали эфир «криптотопливом» для исполнения умных контрактов одноранговой сетью [1].

Для реализации стенда была выбрана платформа Qnet+. На ней было развернуто пять виртуальных клиентов [2]. На них было выделено 7 Гб, 4,7 Гб, 6,8 Гб, 5,9 Гб и 6,4 Гб памяти соответственно. На стенде используется система Linux Ubuntu 18.04 LTS. Сложность развернутой сети – 0×1.

Во время проведенных экспериментов первые четыре виртуальных клиента передавали транзакции пятому клиенту (рис. 1). Клиенты передавали транзакции с примерной скоростью – одна транзакция в секунду (от каждого виртуального клиента), при этом пятый клиент во время эксперимента транзакции не передавал.

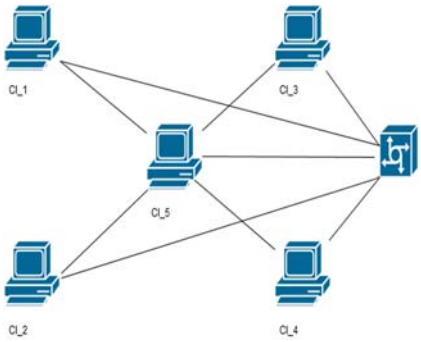


Рис. 1. Схема соединения виртуальных клиентов во время проведения эксперимента

В результате эксперимента были получены следующие статистические данные (рис. 2–6).

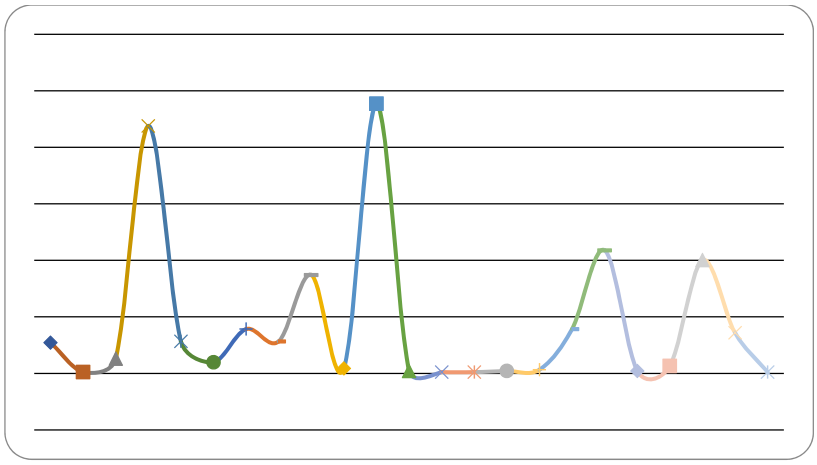


Рис. 2. График зависимости количества пакетов (в процентах) от длины пакета

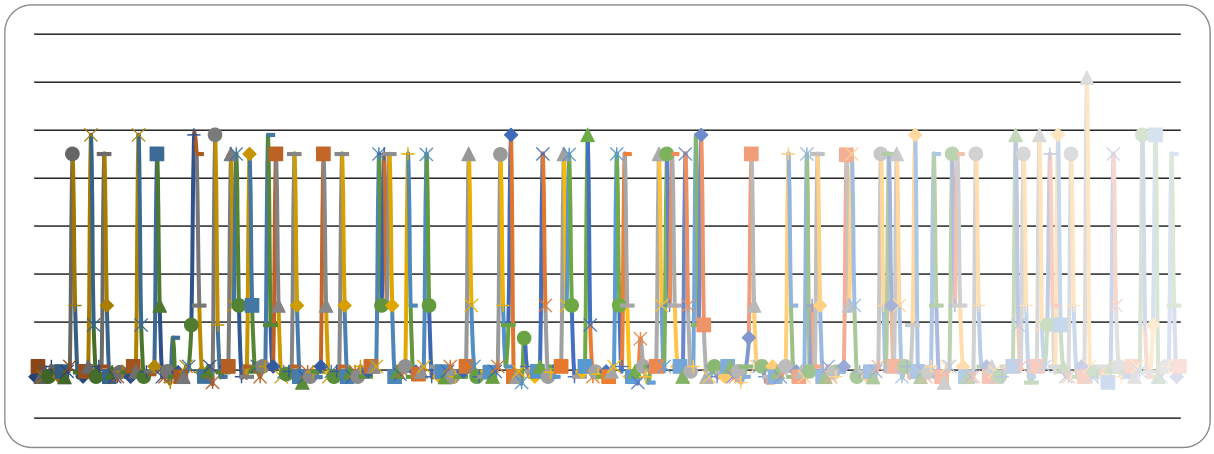


Рис. 3. График зависимости длины пакета от времени прихода пакета

По полученным графикам можно определить: каких пакетов определенной длины приходит больше, какое примерно время между пакетами, а также примерный сценарий прихода пакетов. Также можно заметить,

что 90 % пакетов приходит с разницей до 0,5 секунд, а если увеличить масштаб, то видно, что 90 % пакетов приходят с разницей 0,05 секунд. Все эти данные могут пригодиться для написания алгоритмов для проверки в системах DPI.

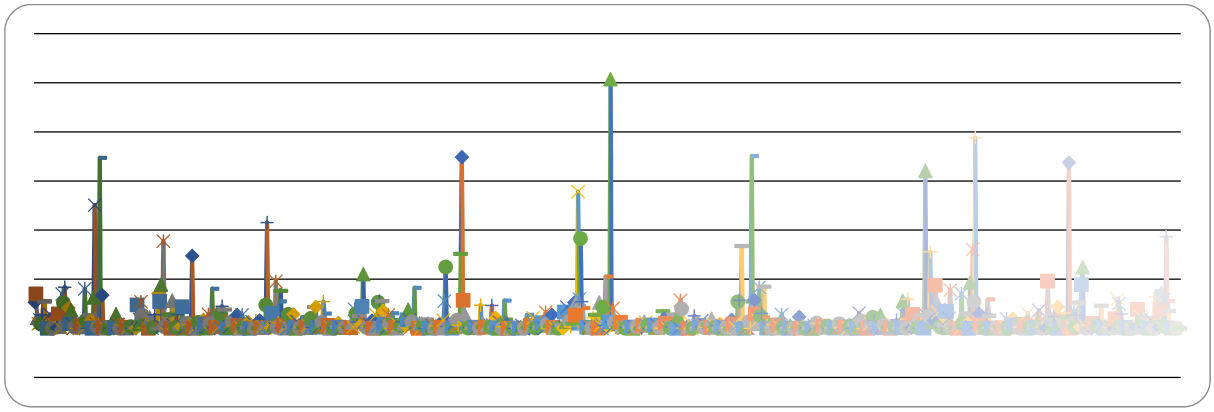


Рис. 4. График зависимости времени между пакетов от длины пакета

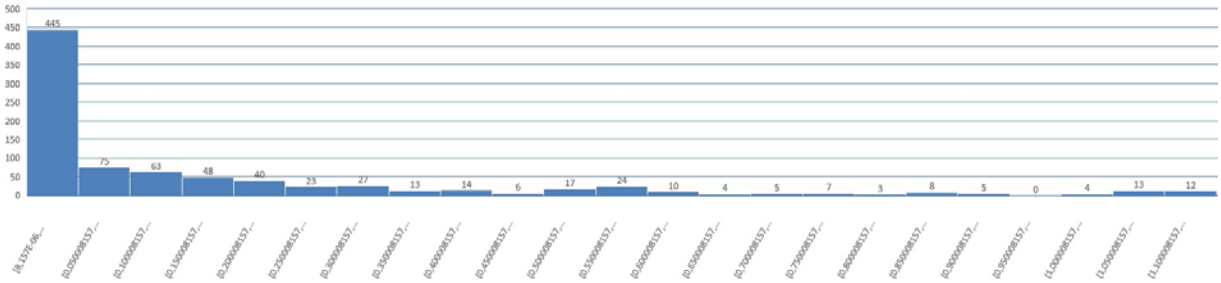


Рис. 5. Гистограмма распределения количества пакетов
от времени прихода между пакетами (шаг 0,05 с)

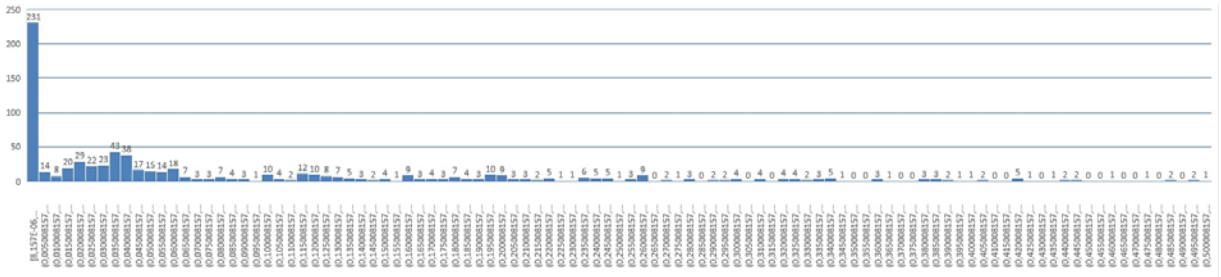


Рис. 6. Гистограмма распределения количества пакетов
от времени прихода между пакетами (шаг 0,005 с)

В ходе одного из экспериментов сеть была нагружена настолько, что сервера ненадолго вышли из строя, то есть, трафиком blockchain можно вывести сервера из строя, что является огромной проблемой для операторов связи. Так же в результате эксперимента было замечено, что после того, как первые четыре виртуальные клиенты перестают передавать транзакции

пятому клиенту, пятый ещё некоторое время (порядка 2–3 минут) обрабатывал транзакции, то есть возникала очередь обработки транзакции. Ещё одним важным наблюдением в ходе эксперимента было то, что пятый клиент во время эксперимента только обрабатывал транзакции, не создавая новых блоков несмотря на то, что сложность создания новых блоков была минимальна.

Что касается вопроса о качестве обслуживания трафика, необходимо чётко и однозначно дифференцировать трафик blockchain и трафик других приложений, что можно сделать с использованием DPI-системы. Определение класса обслуживания для трафика blockchain зависит от типа услуг, для которых он применяется. Поэтому, возникает необходимость исследования определения класса обслуживания, достаточного, для обеспечения приложений с трафиком критичным к задержкам. Тем не менее, существует ряд приложений, которые менее критичны к задержкам, для которых можно изменять класс обслуживания исходя из других значений данной услуги. Для улучшения качества распознавания трафика blockchain предлагаем добавлять различные метки в блоки от приложений, требующих разного уровня обслуживания.

Вариантами решения этого вопроса могут стать следующие подходы:

– использование комбинированных методов для повышения распознаваемости трафика, включая поведенческий и эвристический анализ;

– дополнительная проработка сигнатур.

Технология blockchain предполагает взаимодействие с сетью. Качество услуг, зависит от качества передачи и обработки данных, а работоспособность сети зависит от определенных параметров, появляющихся в результате работы приложений blockchain.

Из всего что сказано выше, можно сделать вывод о том, что необходимо создавать сигнатуры для систем DPI, чтобы снижать реальный трафик blockchain на сети. Также, необходимо учитывать, что рост числа узлов blockchain будет влиять на характеристики сети. Поэтому, возникает необходимость оценивания – насколько узел blockchain загружает сеть, и есть способ снизить эту нагрузку, для обеспечения качественной работы сети.

Список используемых источников

1. Ethereum [Электронный ресурс] // Wikipedia. URL: https://ru.wikipedia.org/wiki/Ethereum (дата обращения: 17.03.2020).

2. Medium. How to create a Blockchain in JavaScript. 2019 [Электронный ресурс] // URL: https://medium.com/javascript-in-plain-english/byob-build-your-own-blockchain-93ecfdc388ad

3. Елагин В. С., Белозерцев И. А., Онуфриенко А. В. Влияние технологии Blockchain на вероятностно-временные характеристики сети // Актуальные проблемы инфотелекоммуникаций в науке и образовании. VIII Международная научно-техническая

и научно-методическая конференция: сб. науч. ст. в 4 т. СПб. : СПбГУТ, 2019. С. 127–132.

УДК 004.056.53
ГРНТИ 49.33.29

ИССЛЕДОВАНИЕ ПОДХОДОВ ДЛЯ АВТОРИЗАЦИИ ПОЛЬЗОВАТЕЛЕЙ БЕСПРОВОДНОЙ СЕТИ С ПРИМЕНЕНИЕМ РАЗЛИЧНЫХ LDAP РЕШЕНИЙ

К. А. Ахрамеева, А. Д. Докшин, А. А Киселева

Санкт-Петербургский государственный университет телекоммуникаций им. проф. М. А. Бонч-Бруевича

В статье подробно описан механизм аутентификации пользователей IEEE 802.1x при подключении к беспроводной сети с использованием RADIUS сервера. Приведено подробное сравнение решений, которые поддерживают протокол RADIUS. Также представлены различные LDAP базы данных для организации аутентификации и авторизации пользователей беспроводной корпоративной сети, а именно Windows Active Directory, FreeIPA и OpenLDAP.

IEEE 802.11, безопасность беспроводных сетей, RADIUS, FreeRADIUS, Windows Active Directory, FreeIPA, OpenLDAP.

На данный момент, беспроводная сеть является объектом постоянного внимания. Системные администраторы и ИТ-директора признают, что небезопасные сети Wi-Fi являются одним из общих векторов атаки.

Многие Wi-Fi сети защищены с помощью одного общего SSID и парольной фразы. Данный режим получил название PSK или режим предустановленного ключа аутентификации. Однако такой подход является небезопасным и неэффективным, если речь заходит о предоставлении доступа к беспроводной сети вашей организации. Если общий SSID или парольная фраза состоят из большого количества символов, то велика вероятность того, что они попадут в открытые источники. Любой желающий может увидеть эту информацию. В некоторых случаях сигнал Wi-Fi достигает соседнего здания, парковки или тротуара. Таким образом, помимо угроз безопасности, защита сетей Wi-Fi с помощью SSID или парольных фраз также малоэффективны [1]. Когда люди увольняются из организации, администраторам приходится менять пароли, из-за чего могут возникнуть дополнительные сложности.

Решение данной проблемы заключается в уникальной аутентификации пользователя при доступе к сети. Такой подход устраняет общую парольную фразу и гарантирует, что администратору не придется менять пароль каждый раз, когда сотрудник покидает организацию. В этом случае каждый пользователь имеет свои учетные данные для аутентификации. Такой режим получил название Enterprise или WPA2/WPA3 Enterprise.

На рис. 1 представлена схема аутентификации пользователей в соответствии с IEEE 802.1x. Централизованная аутентификация в этом случае организовывается с использованием беспроводной точки доступа (ТД) и требует развертывания AAA сервера на сети, а также организации взаимодействия пользователей с ТД и с этим сервером [2]. Данная задача реализуется с помощью протоколов EAP и RADIUS. Существует несколько решений, поддерживающих приведенные протоколы.

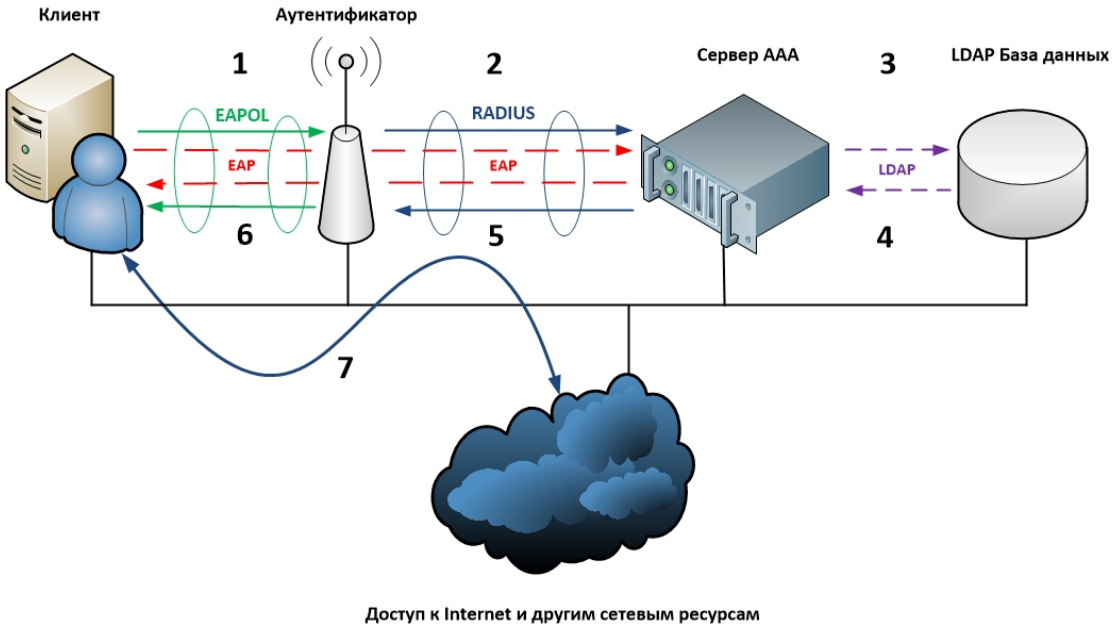


Рис. 1. Схема аутентификации

RADIUS (*Remote Authentication in Dial-In User Service*) – протокол для реализации аутентификации, авторизации и сбора данных об использованных ресурсах, разработанный для передачи сведений между аутентификатором и сервером AAA. Описывается в RFC2138, RFC2868, RFC5080, RFC6929, RFC8044 [3].

В операционной системе Windows к настройкам RADIUS можно перейти сразу после установки сервера. Настройка производится в графическом интерфейсе, что значительно снижает вероятность искажения конфигурационных файлов.

FreeRADIUS является одной из самых популярных реализаций RADIUS – сервера, так как программное обеспечение находится в свободном доступе. Для настройки FreeRADIUS пользователю придется работать

с конфигурационными файлами, что не всегда бывает удобно. Однако для работы сервера авторизации требуется централизованная база данных пользователей, а также протокол взаимодействия с этой базой. В качестве такого протокола может выступать LDAP. В таблице приведено сравнение RADIUS, который изначально предустановлен в операционной системе Windows Server и FreeRADIUS, который можно установить отдельно.

ТАБЛИЦА. Сравнение решений с поддержкой протокола RADIUS

ПО для аутентификации	Исходный код	Поддержка LDAP	Интерфейс управления
MS Windows Server RADIUS	закрыт	да	графический
FreeRADIUS	открыт	да	конфигурационные файлы

Active Directory (AD) – LDAP база данных, разработанная для операционной системы Microsoft Server, в которой хранятся данные в виде объектов. Объект – это отдельный элемент, например, пользователь, группа, приложение, устройство или принтер. Объекты обычно определяются как ресурсы, такие как принтеры или компьютеры, или как субъекты безопасности – такие как пользователи или группы [4].

Active Directory благодаря удобному графическому интерфейсу пользуется популярностью у системных администраторов. Основной службой в Active Directory являются доменные службы, которые хранят информацию о каталоге и обрабатывают взаимодействие пользователя с доменом. AD проверяет доступ, когда пользователь входит в устройство или пытается подключиться к серверу по сети. AD контролирует, какие пользователи имеют доступ к каждому ресурсу. При этом аутентификация пользователей проводится с использованием протокола LDAP. Базы данных, поддерживающие этот протокол, часто применяют для централизованного хранения пользовательских идентификаторов. Примером LDAP базы данных является Active Directory [5].

Основные конкуренты Active Directory, которые предоставляют аналогичные функции AD – это Red Hat Directory Server, Apache Directory, FreeIPA и OpenLDAP [6].

Программное обеспечение FreeIPA включает в себя LDAP базу данных. Загрузка программного обеспечения осуществляется бесплатно. Преимуществом является то, что помимо взаимодействия в консоли, FreeIPA имеет удобный графический интерфейс - это позволяет комфортно взаимодействовать с базой данных. Так же интерфейс и функционал аналогичен Active Directory. Помимо схожего интерфейса, FreeIPA возможно использовать совместно с Active Directory [7].

OpenLDAP – одна из популярных реализаций LDAP с открытым исходным кодом. Как решение с открытым исходным кодом, загрузка программного обеспечения бесплатна, но настройки на физическом оборудовании – нет. OpenLDAP чрезвычайно гибок и может использоваться для аутентификации множества различных типов ресурсов, но в конечном итоге все они используют протокол LDAP [8].

Исследование показало, что для организации аутентификации пользователей семейства стандартов IEEE802.11 могут использоваться различные решения реализации RADIUS и LDAP протокола. Однако, если говорить про реализации программы импортозамещения возникает задача проверки совместимости существующих решений с операционными системами отечественного производителя.

Таким образом, еще одной актуальной задачей является тестирование совместимости FreeRADIUS с OpenLDAP и FreeIPA на базе операционной системы Astra Linux.

Список используемых источников

1. Александрова Е. С., Иванов Г. Н., Ковцур М. М. Анализ механизмов защиты Wi-Fi сетей // Актуальные проблемы инфотелекоммуникаций в науке и образовании. VII Международная научно-техническая и научно-методическая конференция: сб. науч. ст. в 4-х т. СПб. : СПбГУТ, 2018. С. 47–51.

2. Ковцур М. М., Козьмян А. В. Исследование RADIUS-авторизации пользователей для сервиса IP-ТВ // Цифровой регион: опыт, компетенции, проекты. Труды II Международной научно-практической конференции. 2019. С. 351–354.

3. Красов А. В., Штеренберг С. И., Голузина Д. Р. Методика визуализации больших данных в системах защиты информации для формирования отчетов уязвимостей // Электросвязь. 2019. № 11. С. 39–47.

4. Ковцур М. М., Симанов М. С. Анализ особенностей организации авторизации пользователей в сетях коллективного доступа стандарта IEEE 802.11 // Актуальные проблемы инфотелекоммуникаций в науке и образовании. Международная научно-техническая и научно-методическая конференция: сб. науч. ст. в 4 т. СПб. : СПбГУТ, 2019. С. 537–541.

5. Виткова Л. А., Дудникова М. Н., Петрова А. Н. Вопросы управления информационной безопасностью // Актуальные проблемы инфотелекоммуникаций в науке и образовании. VII Международная научно-техническая и научно-методическая конференция: сб. науч. ст. в 4-х т. СПб. СПбГУТ, 2018. С. 143–146.

6. Волостных В. А., Штеренберг С. И., Гвоздев Ю. В. Проблемы обеспечения безопасности персональных данных в высших учебных заведениях // Информационные технологии и телекоммуникации. 2014. Т. 2. № 4. С. 134–141.

7. Десницкий В. А., Сахаров Д. В., Чечулин А. А., Ушаков И. А., Захарова Т. Е. Защита информации в центрах обработки данных : учебное пособие. Федеральное агентство связи. Санкт-Петербургский государственный университет телекоммуникаций им. М. А. Бонч-Бруевича. – СПб. : СПбГУТ, 2019. 91 с. : ил.

8. Сахаров Д. В., Ковцур М. М., Бахтин Д. В. Модель защиты от эксплойтов и руткитов с последующим анализом и оценкой инцидентов // Наукоемкие технологии в космических исследованиях Земли. 2019. Т. 11. № 5. С. 22–31.

УДК004.056
ГРНТИ 81.93.29

ОБЕСПЕЧЕНИЕ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ БАЗ ДАННЫХ WEB-ПРИЛОЖЕНИЙ

К. А. Ахрамеева, М. М. Ковцур, А. В. Михайлова

Санкт-Петербургский государственный университет телекоммуникаций им. проф. М.А. Бонч-Бруевича

В данной статье рассматриваются механизмы обеспечения информационной безопасности баз данных web-приложений. Представлен результат анализа современных баз данных, выявлены наиболее актуальные базы данных при создании web-проекта. Исследованы основные угрозы, направленные на базы данных, а также способы и решения для их защиты.

информационная безопасность, база данных, web-приложение, угрозы.

В настоящее время web-приложения достаточно популярны среди пользователей сети Интернет. Они достаточно универсальны и практичны для пользователей, а также облегчают организацию хранения данных и их выдачу. Любое web-приложения состоят из 3 компонентов:

– клиентская часть – графический интерфейс пользователя;

– серверная часть – программа на сервере, которая обрабатывает запросы;

– база данных – хранение и выдача данных при обращении серверной части.

Все 3 компонента взаимодействуют между собой. Пользователь пишет HTTP-запрос в строку браузера. Браузер через Интернет отсылает HTTP-запросы web-серверу. Веб-сервер вызывает PHP-скрипт, который непосредственно обращается к базе данных. Она выдает нужные данные и PHP-скрипт возвращает клиенту web-страницу, которую и отображает браузер. База данных представляет собой единое, большое хранилище, совокупность специальным образом организованных данных, которое однократно определяется, а затем используется одновременно многими пользователями. Основная ее цель: накопление, хранение, обработка и предоставление информации. Любая современная организация не может обойтись без использования баз данных: банки, магазины, разработчики приложений, компьютерных игр и т. д. Простой пример: база данных успеваемости учащихся в школе недостаточна масштабируема для хранения и обработки информации в крупной корпорации. Основные проблемы, при использовании баз

данных является неверное применение их свойств для определенных областей использования. Так же глобальной проблемой в современном мире является увеличение угроз безопасности, утечка данных и многочисленные атаки с целью их получения (рис.).

Рис. Критерии выбора баз данных

База данных должна для web-приложения обладать определенными свойствами [1]:

1. Восстанавливаемость-возможность восстановления данных после сбоя системы.

2. Безопасность-защита данных от различных угроз и атак, несанкционированного доступа.

3. Целостность-данные должны отображаться корректно, без каких-либо изменений.

4. Эффективность-минимальное время задержки на запрос пользователя.

Важной задачей является выбор базы данных при разработке web-приложения. На рис. представлена схема с основными критериями. В результате анализа были выявлены наиболее гибкие, масштабируемые и простые в использовании базы данных Oracle и MySQL для разработки web-приложения. Стоит отметить, что в базе данных Oracle потребление ресурсов достаточно высокое, а также закрытый исходный код относительно

MySQL. Исследуемые базы данных просты и стабильны в использовании, имеют различный тип: Oracle мультимодельная, а MySQL-реляционная. По данным рейтинга [2, 3], который основывается на данных поисковой системы Google, выделенные базы данных занимают лидирующие позиции на февраль 2020 года.

Угрозы безопасности баз данных [4]:

– Пользовательские привилегии и злоупотребление ими-выдача прав пользователю, который не должен иметь доступ к файлам, данным.

– SQL-инъекции-взлом баз данных. Например, злоумышленник через строку авторизации, пишет запрос, чтобы он вернул ненулевой результат. Таким образом, нужные злоумышленнику данные могут быть указаны в следствие возврата базой данных ошибки.

– Аудит данных-недостаточное тестирование, мониторинг и проверка баз данных на наличие ошибок, угроз. Своевременно обнаруженные пустот защиты баз данных, помогут избежать дальнейшего проникновения злоумышленниками в них.

– Хакерские программы-атаки на базы данных и проникновение в сеть.

– Незащищенность носителей информации-утечка данных или потеря резервных копий.

– Человеческий фактор и непрофессионализм-недостаток знаний в сфере обслуживания и безопасности баз данных.

Предлагаются следующие пути защиты баз данных [5, 6]:

– Средства обнаружения и оценки угроз. Своевременный мониторинг и блокирование вредоносных web-запросов помогут предотвратить внешние угрозы, предотвратить и обезопасить базу данных.

– Управление правами доступа и привилегиями. Существуют 3 модели разграничения прав доступа: ролевая, дискреционная и мандатная. В первой управление осуществляется на основе правил, которые задаются определенному пользователю. В дискреционной модели пользователям предоставляются лишь отдельные привилегии на то или иное действие над базой данных. И в мандатной управление осуществляется по форме допуска уровня секретности при помощи специальных меток, прикреплённых к объекту базы данных.

– Аудит. Существует ряд программ-помощников по отслеживанию изменений в базах данных за какое-либо время. Их ключевыми функциями являются: фиксирование изменений, вносимых в базу данных, схемы и т. д., выявление неавторизированных пользователей и изменений, которые могут привести к падению сервера, отображение всей информации в отчетах с пометками о том, кто, когда и где совершил изменения в базе данных [7, 8].

– Резервное копирование данных. Backup бывает двух видов: логический – в нем отмечается большое количество ошибок при копировании фай-

лов, и физический – создается мгновенный снимок содержимого базы и сохранятся в виде файла с SQL-командами, при помощи которого можно воссоздать базу данных на другом сервере. Данный процесс занимает много времени

– Защита данных, архивирование, шифрование. Данные методы достаточно полезны, ведь если база данных будет взломана, то атакующий не сможет прочесть данные без ключей шифрования [9, 10].

Информационная безопасность баз данных является одной из главных составляющих функционирования всего web-приложения. Важной задачей является эшелонированное распределение многоуровневой защиты с последующим мониторингом каждого уровня, создания резервных копий, распределение прав доступа и своевременного аудита данных.

Список используемых источников

1. Смирнов С. Н. Безопасность систем баз данных. М. : Гелиос АРВ, 2007. 352 с.

2. DB-Engines Рейтинг [Электронный ресурс]. URL: https://db-engines.com/en/ranking (дата обращения: 15.02.2020).

3. Информационные технологии баз данных Рейтинг [Электронный ресурс]. URL: https://studwood.ru/1832529/informatika/informatsionnye _tehnologii_dann yh (дата обращения: 10.02.2020).

4. Десятка крупнейших угроз безопасности баз данных и борьба с ними Рейтинг [Электронный ресурс]. URL: https://www.dataarmor.ru (дата обращения: 22.01.2020).

5. Информационная безопасность баз данных [Электронный ресурс]. URL: https://slmaxim.wordpress.com (дата обращения: 22.01.2020).

6. Сахаров Д. В., Мельников С. Е., Штеренберг С. И. Инфраструктура связи на крайнем севере как база для формирования единой инфосреды // Электросвязь. 2016. № 5. С. 18–20.

7. Сахаров Д. В., Красов А. В., Ушаков И. А., Орлов Г. А. Защищенная модель программно-определяемой сети в среде виртуализации KVM // Электросвязь. 2020. № 3. С. 26–32.

8. Сахаров Д. В., Левин М. В., Фостач Е. С., Виткова Л. А. Исследование механизмов обеспечения защищенного доступа к данным, размещенным в облачной инфраструктуре // Наукоемкие технологии в космических исследованиях Земли. 2017. Т. 9. № 2. С. 40–46.

9. Ушаков И. А. Обнаружение инсайдеровв корпоративной компьютерной сетина основе технологий анализа больших данных // Вестник Санкт-Петербургского государственного университета технологии и дизайна. Серия 1: Естественные и технические науки. 2019. № 4. С. 38–43.

10. Альшаев И. А., Красов А. В., Ушаков И. А. Исследование принципов работы протокола openflow в программно-конфигурируемых сетях // Труды учебных заведений связи. 2017. Т. 3. № 2. С. 16–27.

УДК 004.722
ГРНТИ 49.33.29

ВОЛНООБРАЗНЫЙ ХАРАКТЕР ЗАВИСИМОСТЕЙ ПОТЕРЬ ГЕТЕРОГЕННЫХ ЗАЯВОК ОТ ВЕЛИЧИНЫ ДОСТУПНОГО КАНАЛЬНОГО РЕСУРСА

К. А. Батенков, А. В. Королев, А. Е. Миронов, А. Н. Орешин

Академия Федеральной службы охраны Российской Федерации

Полученные в работе графики зависимостей позволяют утверждать, что чем больше разница между требуемыми ресурсами для обслуживания каждой заявки разных сервисов, тем более волнообразный характер будут иметь зависимости вероятностей потерь от изменения канального ресурса звена мультисервисной сети связи.

мультисервисная сеть связи, гетерогенный трафик, аналитическая модель, метод Кауфмана–Робертса.

Исследованию вопросов моделирования процесса обслуживания гетерогенного трафика в подобных сетях достаточно большое время занимались учёные разных стран [1]. При этом фундаментальные результаты по решению этой проблемы были получены Френком Келли [2] и Кейтом Россом [3]. В России основополагающими работами в этой области являются работы С. Н. Степанова, К. Е., Самуйлова, Г. П. Башарина и их учеников [4].

Сервисы реального времени обслуживаются по идентичным закономерностям, что в сетях с коммутацией пакетов, что каналов [5, 6]. Трансформация классических методов передачи информации к пакетной форме не изменяет сущности восприятия телефонных сервисов потребителями. При этом основным требованием, по-прежнему, остается незначительная величина сквозной задержки между абонентами [7, 8]. При этом ограничение доли непринятых пакетов некоторой фиксированной нормированной величиной позволяет определять на основе доступности ресурса линий связи и качество обслуживания пользователей, т. е. путем оценки доли заявок, непоступивших в точку приема. Задача расчета требуемой пропускной способности линий в терминах анализа вероятности блокирования в мультипотоковых моделях узлов с коммутацией каналов может рассматриваться с точки зрения понятия единиц канального ресурса и эффективной скорости передачи информации [4, 9, 10].

В отмеченных работах рассмотрены различные модели систем МСС с различными стратегиями доступа к сетевым ресурсам. Но базовой моделью является модель звена МСС с полнодоступной стратегией доступа. Причины этого заключается в том, она оказывается аналогом классической модели Эрланга только в мультисервисном виде. В рассматриваемой системе анализируется процесс одновременного использования канального ресурса звена МСС с произвольным количеством пуассоновских потоков, имитирующих сервисы реального времени, разнящихся интенсивностью поступления, объемом ресурса, выделенного для обслуживания заявок, а также длительностью его занятия данными пользователя [1]. Для рассматриваемой модели обслуживания требований удалось получить все главные результаты, которые до этого были выведены для модели Эрланга и привели к её широкому распространению в инженерной сфере, затрагивающей проектирование телекоммуникационных сетей [5].

На основе алгоритма расчета вероятностей потерь сервисов реального времени и величины обслуженной нагрузки применяют метод Кауфмана–Робертса [4], который базируется на разбиении пространства состояний модели по числу занятых единиц канальной емкости [7], а также ниже приведенных исходных данных были построены зависимости потерь заявок двух потоков сервисов реального времени.

Исходные данные:

Рассматривается звено МСС (ЗМСС), в котором реализуется полнодоступная стратегия доступа.

На данное ЗМСС поступают требования двух сервисов реального времени ($k = 2$), например, цифровая телефония и видеоконференцсвязь. Для сервиса цифровой телефонии (малоресурсные заявки) требуется $b1 = 1$ единиц канального ресурса (ЕКР), для сервисов видеосвязи ЕКР (ресурсоемкие заявки) требуется $b2 = 20$ ЕКР.

Оба потока являются пуассоновскими со случайными длительностями занятия ЕКР, распределенными по экспоненциальному закону.

Интенсивности нагрузки:

– первого потока – $Z1 = 20$ Эрл,

– второго потока – $Z2 = 3$ Эрл.

При этом для обслуживания каждого требования сервиса цифровой телефонии требуется $b1 = 1$ (ЕКР), для сервисов видеосвязи (ресурсоемкие заявки) требуется $b2 = 20$ ЕКР.

Канальный ресурс звена МСС (V) изменяли в пределах от 10 до 100 (ЕКР) с шагом 10 (ЕКР).

Анализ полученных зависимостей позволяет сделать следующие выводы:

Вероятности потерь заявок являются убывающими функциями от аргумента V (ЕКР).

Графики зависимостей имеют волнообразный характер, т. е. возможны случаи, когда значения вероятностей потерь π_i могут возрастать даже при увеличении объёма канального ресурса звена МСС (рис.).

Потери малоресурсных заявок возрастают при достижении такого значения ресурса звена МСС V (ЕКР), при котором его становится достаточным для обслуживания большего числа ресурсоемких заявок, что в свою очередь ведет к снижению значения вероятности потерь π_2.

Уменьшение значений вероятности потерь π_2 наблюдаются при величине V кратной 20 ЕКР ($b2$ = 20 ЕКР).

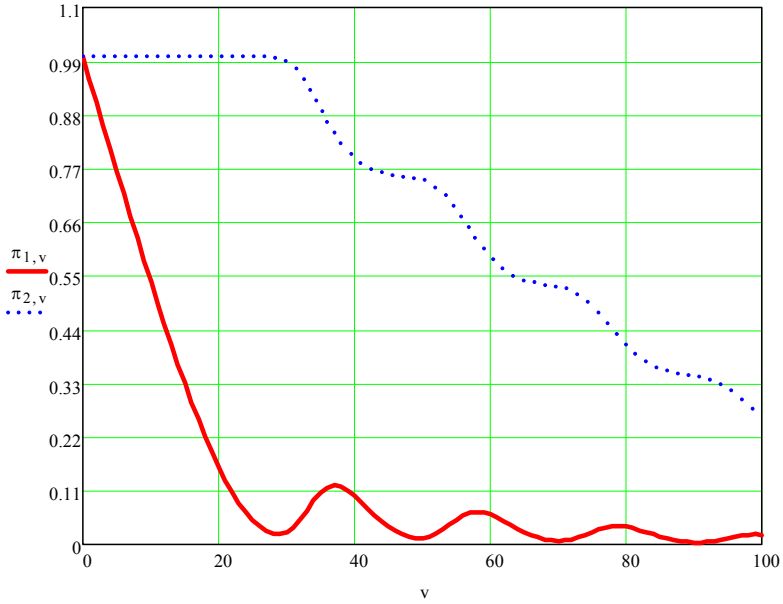


Рис. Зависимости вероятностей потерь сервисов реального времени от изменения канального ресурса звена МСС

Анализируя поведение графиков зависимостей, можно предположить, что чем больше разница между требуемыми ресурсами для обслуживания каждой заявки разных сервисов (b_i), тем более волнообразный характер будут иметь зависимости вероятностей потерь от изменения канального ресурса звена МСС [1, 4].

Список используемых источников

1. Пшеничников А. П. Теория телетрафика : учебник для вузов. М. : Горячая линия – Телеком, 2017. 212 с.

2. Kelly F. P. Mathematical models of multiservice networks. Complex Stochastic Systems and Engineering, Oxford University Press, 1995. PP. 221–235.

3. Ross K. W. Multiservice loss models for broadband telecommunication network. London : Springer, 1995. 343 p.

4. Степанов С. Н. Теория телетрафика: концепции, модели, приложения. М. : Горячая линия – Телеком, 2015. 868 с.

5. Батенков К. А. Исследование полнодоступного звена мультисервисной сети связи, реализующего равноправную стратегию доступа к канальному ресурсу линии // Актуальные проблемы инфотелекоммуникаций в науке и образовании (АПИНО 2019). VIII Международная научно-техническая и научно-методическая конференция : сб. науч. ст. в 4-х т. СПб : СПбГУТ, 2019. С. 113–116.

6. Чечик В. В., Батенков К.А. Имитационное моделирование трафика HTTP с помощью программной среды Riverbed // Труды Северо-Кавказского филиала Московского технического университета связи и информатики. 2016. № 1. С. 273–277.

7. Батенков К. А., Королев А.В., Миронов А.Е., Орешин А.Н. Анализ статистики голосового трафика сети ethernet с помощью программы Wireshark // Телекоммуникации. 2018. № 10. С. 39–48.

8. Батенков К. А. Числовые характеристики структур сетей связи // Труды СПИИРАН. 2017. № 4 (53). С. 5–28.

9. Батенков К. А., Батенков А. А. Анализ и синтез структур сетей связи по детерминированным показателям устойчивости // Труды СПИИРАН. 2018. № 3 (58). С. 128–159.

10. Батенков К. А. Точные и граничные оценки вероятностей связности сетей связи на основе метода полного перебора типовых состояний // Труды СПИИРАН. 2019. Т. 18. № 5. С. 1093–1118.

УДК 519.718:004.722
ГРНТИ 49.33.29

ФОРМИРОВАНИЕ МНОЖЕСТВА МНОГОПОЛЮСНЫХ ДЕРЕВЬЕВ В ТЕЛЕКОММУНИКАЦИОННЫХ СЕТЯХ

К. А. Батенков, А. Н. Орешин, А. Б. Фокин

Академия Федеральной службы охраны Российской Федерации

Вопросы, связанные с анализом надежности телекоммуникационных сетей остаются в центре внимания при их модернизациях или проектировании. Модель телекоммуникационной сети можно представить в виде обобщенной модели Эрдеша–Реньи, на основе которой производится процедура формирования множества многополюсных деревьев для сетей с многополюсной связностью.

сеть, граф, модель, дерево, вероятность связности, устойчивость, надежность.

Введение

Увеличение размеров и сложности существующих и перспективных сложно разветвленных систем (телекоммуникационных сетей) выносит

на первый план проблемы, связанные с анализом их надежности (устойчивости, живучести). Такие системы лучше представить в форме сети, описывающей взаимосвязи ее отдельных элементов (вершин и ребер).

Для сетей связи необходимым условием нормального функционирования является постоянная доступность заданного набора вершин и как следствие, высокая надежность сети.

Формирование множества многополюсных деревьев в телекоммуникационных сетях

Традиционно выделяют три меры связности: двухполюсная, многополюсная и всеполюсная [1, 2].

Многополюсная связность – это свойство сети, характеризуемое наличием хотя бы одного пути между заданными вершинами. Предполагается, что существует связь между любой парой вершин из заданного множества. В результате событие связности можно трактовать как существование хотя бы одного дерева (неостового), включающего все заданные вершины случайного графа.

Рассматриваемый подход к формированию множества многополюсных деревьев основывается на методе, описанном в [1, 3, 4], предполагающим последовательное преобразование всего множества остовых деревьев в многополюсные. В отличие от способа [1, 3], целесообразно воспользоваться свойством многополюсного дерева включать в качестве листьев только полюса. В результате оказывается возможным последовательно удалять из остового дерева висячие вершины и таким образом добиваться формирования требуемого подграфа. Кроме того, на каждом шаге целесообразно проверять, является ли сформированное многополюсное дерево подграфом оставшихся непроанализированных остовых деревьев, и если да, то данные деревья из дальнейшего рассмотрения убирать. Данная процедура существенно упрощает процесс формирования деревьев, т. к. исключает из анализа дубликаты многополюсных деревьев.

Формально процедуру формирования множества многополюсных деревьев целесообразно разбить на три этапа. На первом синтезируют множество остовых деревьев в форме матрицы деревьев, на втором определяют множество неполюсных вершинных сечений, а на третьем непосредственно формируют множество многополюсных деревьев путем последовательно удаления висячих неполюсных вершин и удаления избыточных остовых деревьев в матричном виде.

Процедура синтеза множества остовых деревьев в форме матрицы деревьев описывается исходя из матрицы смежностей $\mathbf{A}$ случайного графа G. Далее ее необходимо преобразовать в модифицированную матрицу смеж-

ности $\mathbf{A}' = \{a'_{i,j}\}_{i,j=1,\dots,v}$, учитывающую нумерацию ребер. Поскольку матрица неориентированного графа симметрическая, то целесообразно формировать сразу два элемента модифицированной матрицы:

$$a'_{1,j} = a'_{j,1} = \begin{cases} \sum_{r=1}^{j} a_{1,r}, a_{i,j} = 1, \\ 0, a_{i,j} = 0, \end{cases}$$

$$j = 1, \dots, v,$$

$$a'_{i,j} = a'_{j,i} = \begin{cases} \sum_{k=1}^{i-1} \sum_{r=k}^{v} a_{k,r} + \sum_{r=k}^{j} a_{i,r}, a_{i,j} = 1, \\ 0, a_{i,j} = 0, \end{cases}$$

$$i = 2, \dots, v, j = 1, \dots, v,$$

Для удобства программной реализации множества сечений целесообразно синтезировать в форме векторов сечений $\mathbf{c}_r$, $r = 1, \dots, v-1$. Для их определения производится последовательная процедура выделения по строкам ненулевых элементов матрицы смежности:

$$[\mathbf{c}_r]_1 = \{a'_{i,\min(j)} : a_{i,j} = 1, j = 1, \dots, v\}, \quad (1)$$

$$[\mathbf{c}_r]_k = \{a'_{i,\min(j)} : a_{i,j} = 1, [\mathbf{c}_i]_{k-1} < v, j = [\mathbf{c}_i]_{k-1} + 1, \dots, v\},$$
$$i \neq v_e, i = 1, \dots, v, r = \begin{cases} i, i < v_e, \\ i-1, i > v_e. \end{cases} \quad (2)$$

В результате формируется $v-1$ векторов сечений, над которыми осуществляется последовательная процедура декартового умножения с контролем уникальности, входящих в каждое произведение ребер. Исходной матрицей декартовых произведений $\mathbf{W}_1$ является транспонированный вектор сечений первой или второй ($v_e = 1$) вершины $\mathbf{W}_1 = \mathbf{c}_1^{\mathrm{T}}$, где $^{\mathrm{T}}$ – оператор транспонирования.

Результаты декартовых произведений формируются в виде матриц $\mathbf{W}_r$, k-й столбец каждой из которых образуется только в случае отсутствия повторяющихся ребер, а последовательный перебор выполняется сначала по столбцам матрицы декартовых произведений $\mathbf{W}_{r-1}$, а затем по элементам векторов сечений $\mathbf{c}_r$**:**

$$\mathbf{W}_r^{\langle k \rangle} = \left\{ \begin{bmatrix} \mathbf{W}_{r-1}^{\langle i \rangle} \\ [\mathbf{c}_r]_j \end{bmatrix} : [\mathbf{c}_r]_j \notin \mathbf{W}_{r-1}^{\langle i \rangle}, i = 1, \dots, \mathrm{cols}(\mathbf{W}_{r-1}), j = 1, \dots, \mathrm{rows}(\mathbf{c}_r) \right\},$$

$$r = 2, \dots, v-2.$$

Последнее $v-2$ декартово произведение дополнительно проверяется на связность с целью выявить подграфы, содержащие петли:

$$\mathbf{W}_{v-1}^{\langle k\rangle} = \left\{ \begin{bmatrix} \mathbf{W}_{v-2}^{\langle i\rangle} \\ [\mathbf{c}_{v-1}]_j \end{bmatrix} : [\mathbf{c}_{v-1}]_j \notin \mathbf{W}_{v-2}^{\langle i\rangle}, \mathrm{S}\left(\begin{bmatrix} \mathbf{W}_{v-2}^{\langle i\rangle} \\ [\mathbf{c}_{v-1}]_j \end{bmatrix} \right) = 1, \right.$$

$$\left. i = 1, \dots, \mathrm{cols}(\mathbf{W}_{v-2}), j = 1, \dots, \mathrm{rows}(\mathbf{c}_{v-1}) \right\},$$

где $\mathrm{S}(\mathbf{W})$ – оператор проверки связности, результат выполнения которого равен единице, если граф, состоящий из ребер **W,** связный и нуль, если нет.

Стандартным подходом для реализации этого оператора служит один из двух поисков в ширину или глубину [4].

Сформированная матрица $\mathbf{W}_{v-1}$ содержит описание всех деревьев исследуемого графа. Для удобства расчета преобразуем матрицу $\mathbf{W}_{v-1}$ в матрицу деревьев $\mathbf{W} = \{w_{i,j}\}_{\substack{i=1,\dots,l \\ j=1,\dots,s}}$, где s – общее число деревьев, каждый элемент которой определяется выражением:

$$w_{i,j} = \begin{cases} 1, i \in L'_j, \\ 0, i \notin L'_j, \end{cases}$$

где $L'_j \in L'$ – j-е дерево.

Таким образом, процедура формирования матрицы деревьев $\mathbf{W}$ на основе матрицы $\mathbf{W}_{v-1}$ оказывается очевидным, поскольку все деревья содержат одинаковое количество ребер, и используется последовательный перебор всех столбцов ранее определенной матрицы $\mathbf{W}_{v-1}$**:**

$$w_{i,j} = \begin{cases} 1, i \in \mathbf{W}_{v-1}^{\langle j\rangle}, \\ 0, i \notin \mathbf{W}_{v-1}^{\langle j\rangle}, \end{cases}$$

$$i = 1, \dots, l, j = 1, \dots, s.$$

В результате выполнения этих процедур образуется матрица $\mathbf{W}$ остовых деревьев.

Процесс формирования множества неполюсных вершинных сечений основан на выражениях (1)–(2), с учетом удаления неполюсных вершин и формирования матрицы неполюсных вершинных сечений $\mathbf{C}$. Целесообразно первоначально образовать вектор, содержащий номера вершин, не являющихся полюсами. Так, если номера вершин–полюсов v_i образуют вектор $\mathbf{k} = \{k_i\}_{i=1,\dots,v\prime}$, то вектор $\mathbf{k}' = \{k'_i\}_{i=1,\dots,v-v\prime}$:

$$\mathbf{k}' = \{\{i\}: i \notin \mathbf{k}, i = 1, \dots, v\}$$

включает номера только неполюсных вершин.

Следовательно матрица неполюсных вершинных сечений имеет вид $\mathbf{C} = \{c_{i,j}\}_{\substack{i=1,\dots,l \\ j=1,\dots,v-v'}}$, где каждый элемент определяется выражением:

$$c_{i,j} = \begin{cases} 1, i \in L'_j, \\ 0, i \notin L'_j, \end{cases}$$

где $L'_j \in L' - j$-е вершинное сечение.

Данная матрица формируются путем последовательной процедуры сравнения элементов модифицированной матрицы $\mathbf{A}'$ смежностей с индексами образуемой матрицы $\mathbf{C}$ сечений:

$$c_{i,j} = \{a_{k,j} : a'_{k,j} = i, k = 1, \dots, v\}, i = 1, \dots, l, j = 1, \dots, v - v'.$$

Синтез матрицы многополюсных деревьев разбивается на ряд этапов, на каждом из которых рассматривается одно из остовых деревьев на предмет исключения листьев, не являющихся полюсами, а затем в рамках того же этапа удаляются те остовые деревья, которые включают в себя полученное многополюсное дерево.

Удаление из осотовых деревьев листьев представляется в виде последовательной процедуры сравнения текущего вектора остового дерева $\mathbf{W}^{\langle k \rangle}$ со всеми столбцами матрицы неполюсных сечений $\mathbf{C}$. Причем подобное сравнение каждого с каждым необходимо проводить до тех пор, пока не наступит ситуация отсутствия неполюсных листьев, поскольку удаление листа может привести к возникновению новой неполюсной висячей вершины. Таким образом, образуется вектор $\mathbf{w}_r$, содержащий номера ребер подграфа по следующему закону:

$$\mathbf{w}_1 = \left\{ \mathbf{W}^{\langle k \rangle} - \mathbf{q} : \mathbf{q} = \left\lfloor \frac{\mathbf{W}^{\langle k \rangle} + \mathbf{C}^{\langle i \rangle}}{2} \right\rfloor, \mathbf{q}^{\mathrm{T}} \mathbf{1}_l = 1, i = 1, \dots, v - v' \right\},$$

$$\mathbf{w}_2 = \left\{ \mathbf{w}_1 - \mathbf{q} : \mathbf{w}_1 \neq \mathbf{W}^{\langle k \rangle}, \mathbf{q} = \left\lfloor \frac{\mathbf{w}_1 + \mathbf{C}^{\langle i \rangle}}{2} \right\rfloor, \mathbf{q}^{\mathrm{T}} \mathbf{1}_l = 1, i = 1, \dots, v - v' \right\},$$

$$\mathbf{w}_r = \left\{ \mathbf{w}_{r-1} - \mathbf{q} : \mathbf{w}_{r-1} \neq \mathbf{w}_{r-2}, \mathbf{q} = \left\lfloor \frac{\mathbf{w}_{r-1} + \mathbf{C}^{\langle i \rangle}}{2} \right\rfloor, \right.$$

$$\left. \mathbf{q}^{\mathrm{T}} \mathbf{1}_l = 1, i = 1, \dots, v - v' \right\}, r = 1, \dots$$

В конечном счете, когда вектор подграфа $\mathbf{w}_r$ не изменяется ($\mathbf{w}_{r-1} \neq \mathbf{w}_{r-2}$), то он превращается в многополюсное дерево, формализуемое как столбец матрицы $\mathbf{W}' = \{w'_{i,j}\}_{\substack{i=1,\dots,l \\ j=1,\dots,s}}$ многополюсных деревьев, где s – общее число многополюсных деревьев, каждый элемент которой определяется выражением:

$$w'_{i,j} = \begin{cases} 1, i \in L'_j, \\ 0, i \notin L'_j, \end{cases}$$

где $L'_j \in L'$ – j-е многополюсное дерево.

Следовательно:

$$\mathbf{W}'^{\langle k \rangle} = \mathbf{w}_r.$$

Удаление избыточных остовых деревьев также производится путем сравнения, но уже текущего многополюсного дерева $\mathbf{w}_r$ и всех нерассмотренных остовых деревьев $\mathbf{W}^{\langle k \rangle}$:

$$\mathbf{W}^{\langle r \rangle} = \left\{ \mathbf{W}^{\langle j \rangle} : \mathbf{w}_r \subset \mathbf{W}^{\langle j \rangle}, j = k+1, \dots, \mathrm{cols}(\mathbf{W}) \right\}.$$

Таким образом, после просмотра всех остовых деревьев формируется матрица $\mathbf{W}'$ многополюсных деревьев. Отметим, что вследствие усечения матрицы $\mathbf{W}$ количество этапов процедуры может быть существенно меньше общего числа остовых деревьев.

Заключение

Следует отметить, что многополюсные деревья являются наиболее общим понятием относительно простых цепей и остовых деревьев. Первые из них представляют собой многополюсные деревья всего с двумя полюсами, а последние – случай, когда все вершины и есть полюсы. В практических приложениях целесообразно рассматривать именно частные случаи простых цепей и остовов вследствие их меньшей вычислительного сложности. Как следствие можно предположить, что вполне логичным окажется и поиск более эффективных алгоритмов формирования множеств многополюсных деревьев с фиксированным числом полюсов, либо с количеством полюсов, зависящим от общего количества вершин в графе.

Список используемых источников

1. Chaturvedi S. K. Network Reliability Measures and Evaluation. Scrivener Publishing LLC. 2016. 237 p.

2. Paredes R., Duenas–Osorio L., Meel K. S., Vardi M. Y. Network Reliability Estimation in Theory and Practice // Preprint submitted to Reliability Engineering & System Safety. 2018. 26 p.

3. Rath D., Soman K. P. A Simple Method for Generating k-Trees of a Network // Microelectronics and Reliability. 1993. Vol. 33 (9). PP. 1241–1244.

4. Белоусов А. И., Ткачев С. Б. Дискретная математика : учебник для вузов / Под ред. В. С. Зарубина, А. П . Крищенко. 3-е изд., стереотип. М. : Изд-во МГТУ им. Н. Э. Баумана, 2004. 744 с.

УДК 004.51
ГРНТИ 81.93.29

МЕТОДИКА ЭКСПЕРИМЕНТАЛЬНОЙ ОЦЕНКИ ЭФФЕКТИВНОСТИ ЧЕЛОВЕКО-КОМПЬЮТЕРНОГО ВЗАИМОДЕЙСТВИЯ В ВИЗУАЛЬНОЙ АНАЛИТИКЕ

Ю. Е. Бахтин[1], С. Н. Бушуев[2], Д. А. Гайфулина[1], К. Н. Жернова[1], А. Ю. Иванов[1], В. И. Комашинский[3], И. В. Котенко[1]

[1]Санкт-Петербургский институт информатики и автоматизации Российской Академии Наук
[2]ЗАО «НПП ТЕЛДА»
[3]Национальный исследовательский университет ИТМО

Для анализа инцидентов компьютерной безопасности в настоящий момент требуется обработка всё большего количества данных. При этом постоянно увеличивающийся объём обрабатываемой информации требует всё более сложных моделей визуализации. Однако с увеличением сложности визуализации возрастает потребность в разработке новых, более эффективных способов человеко-компьютерного взаимодействия для управления данными, представленными в графическом отображении. Новые модели взаимодействия с моделями визуализации в системах визуальной аналитики требуют оценки эффективности, чтобы распознать, насколько подходит данная визуализация для конкретной задачи. В данной работе предлагается возможная методика оценки взаимодействия с визуализацией.

человеко-компьютерное взаимодействие, информационная безопасность, пользовательские интерфейсы, визуализация данных, оценка эффективности, сенсорные экраны.

Введение

Поскольку системы компьютерной безопасности обрабатывают огромное количество данных, мониторинг событий безопасности при визуальной аналитике требует сложных моделей визуализации. Одной из наиболее распространённых моделей визуализации является граф компьютерной сети [1].

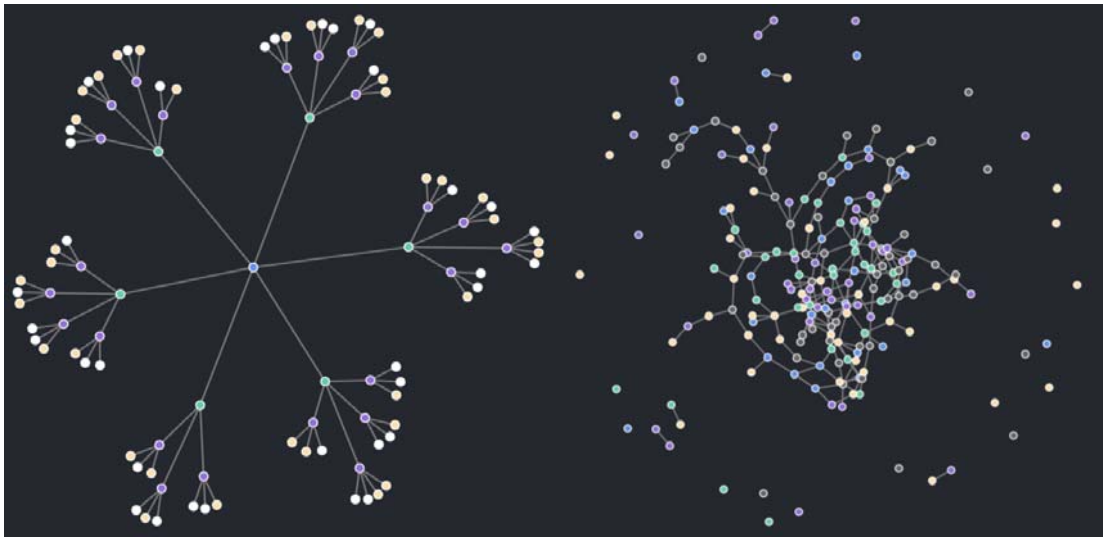
В настоящее время получили широкое распространение устройства с сенсорными экранами, поэтому также появляются программно-аппаратные средства компьютерной безопасности, поддерживающие управление жестами. Однако разработка жестов, удобных для управления сложными моделями визуализации, не является тривиальной задачей. По этой причине требуется оценить эффективность того или иного используемого жеста при работе с конкретной визуализацией.

В данной работе оценка проводилась по формальным показателям: *скорость* и *точность* выполнения заданий.

Модель взаимодействия с визуализацией

Для оценки эффективности взаимодействия пользователя с системами визуальной аналитики использовалась графовая модель визуализации с возможностью управления жестами на сенсорном экране.

На рис. 1а представлен граф централизованной сети, на рис. 1б – децентрализованной.



а) б)

Рис. 1. Графы централизованной сети устройств (а) и децентрализованной сети (б)

Для оценки эффективности взаимодействия с графовой моделью визуализации были использованы тесты на скорость прохождения заданий и проверки на точность (два теста, каждый из которых содержал 13 заданий). Скорость измеряется в секундах, потраченных на выполнение каждого задания. Точность оценивается в зависимости от количества ошибок в выполнении задания.

Оценивались следующие основные жесты на сенсорных экранах [2, 3]:

– долгое нажатие;
– сведение/разведение четырёх пальцев;
– сведение/разведение пяти пальцев;
– листание тремя пальцами вправо/влево.

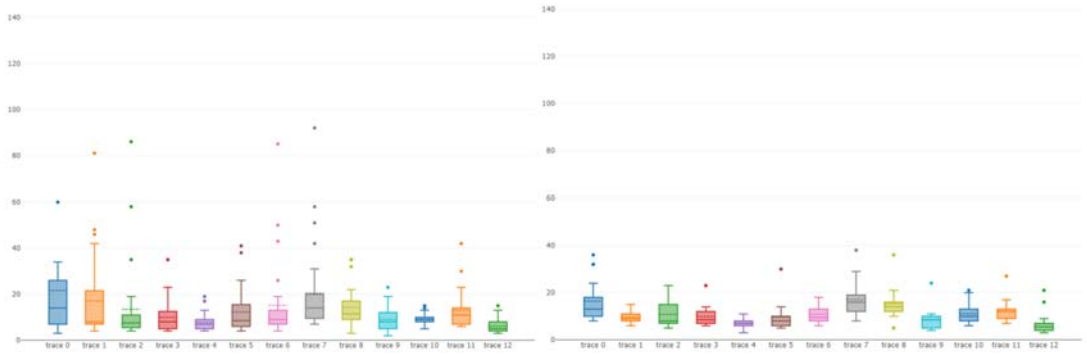
Долгое нажатие использовалось для того, чтобы притянуть к месту касания нужную вершину (на сенсорном экране сложно попасть пальцем точно по вершине графа). Сведение/разведение четырёх пальцев позволяло менять размер вершин графа для более удобного взаимодействия с ними. С помощью сведения/разведения пяти пальцев можно было менять связи

между вершинами графа. Листание тремя пальцами вправо/влево позволяло показать/скрыть дополнительную информацию на графе.

Оценка эффективности взаимодействия с визуализацией

Скорость

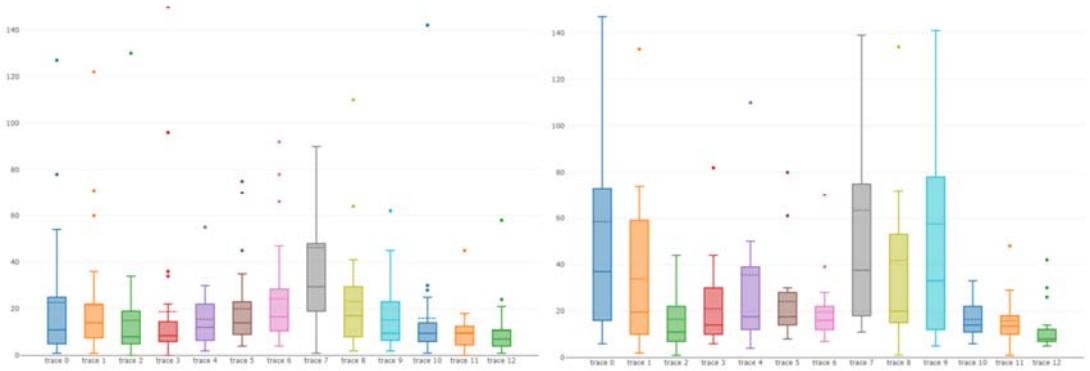
На рис. 2 представлены результаты теста на скорость выполнения заданий графа централизованной сети: задания на сенсорном экране (рис. 2а) и задания на традиционном кнопочном интерфейсе (рис. 2б).



а) б)

Рис. 2. Тест 1 на сенсорных экранах (а) и на традиционном интерфейсе (б)

На рис. 3 представлены результаты теста на скорость выполнения заданий графа децентрализованной сети: задания на сенсорном экране (рис. 3а) и задания на традиционном кнопочном интерфейсе (рис. 3б).



а) б)

Рис. 3. Тест 2 на сенсорных экранах (а) и на традиционном интерфейсе (б)

Точность

На рис. 4 представлены результаты тестов 1 и 2 для сенсорного и традиционного интерфейсов с точки зрения точности выполнения заданий.

Чем больше количество ошибок при выполнении задания – тем ниже точность. При прохождении второго теста точность повышалась по сравнению с первым как в случае с сенсорным, так и в случае с традиционным интерфейсом.

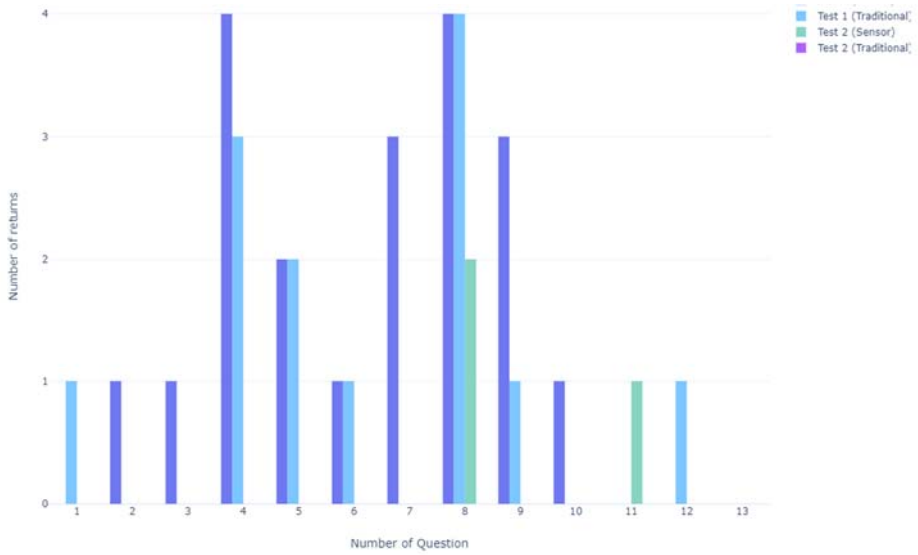


Рис. 4. Точность тестов 1 и 2 на сенсорных экранах и традиционном интерфейсе

Выводы

Для оценки эффективности человеко-компьютерного взаимодействия использовались параметры скорости и точности. При этом, несмотря на то, что точность выполнения заданий для традиционного интерфейса оказалась всё ещё выше, чем для сенсорного, для децентрализованного графа пользователи справлялись с заданиями быстрее на сенсорном экране, чем с помощью традиционного интерфейса, а для централизованного графа разница оказалась несущественной.

Работа выполнена при частичной финансовой поддержке РФФИ (проект 18-07-01488-а).

Список используемых источников

1. Kolomeec M., Chechulin A., Kotenko I. V. Methodological Primitives for Phased Construction of Data Visualization Models // J. Internet Serv. Inf. Secur. 2015. Т. 5. №. 4. С. 60–84.

2. Котенко И. В. и др. Модель человеко-машинного взаимодействия на основе сенсорных экранов для мониторинга безопасности компьютерных сетей // Региональная информатика (РИ-2018). XVI Санкт-Петербургская. 2018. С. 149.

3. Котенко И. В. и др. Методы человеко-машинного взаимодействия на основе сенсорных экранов в ситуационных центрах безопасности // Информационные технологии в управлении (ИТУ-2018). 2018. С. 554–558.

УДК 004.728.3.057.4
ГРНТИ 49.31.31

СОВРЕМЕННОЕ СОСТОЯНИЕ ТРАНСПОРТНЫХ СЕТЕЙ СИНХРОННЫХ И ПЛЕЗИОХРОННЫХ ЦИФРОВЫХ ИЕРАРХИЙ

М. Ю. Безуглов[1], А. А. Олимпиев[2]

[1]Санкт-Петербургский государственный университет телекоммуникаций им. проф. М. А. Бонч-Бруевича
[2]АО «Научно-исследовательский институт «Рубин»

В статье кратко рассмотрены аспекты синхронных и плезиохронных транспортных сетей, имеющие отношения к этапу ввода в эксплуатацию линий и телекоммуникационного оборудования. Приводятся сведения об используемых сигналах технического обслуживания, дана оценка достаточности и содержательности этих сигналов с точки зрения лица, осуществляющего первичную настройку телекоммуникационного оборудования.

синхронная цифровая иерархия, плезиохронная цифровая иерархия, сигналы технического обслуживания.

Для описания процессов функционирования всех современных сетей связи научное сообщество использует достаточно удобную модель, в соответствии с которой используемые в сетях связи технологии условно подразделяют на технологии первичных (или, что тоже самое, транспортных) сетей связи, предназначенных для единообразного переноса абонентского трафика; и вторичных сетей связи, которые определяют многообразие потребителей, потребляемых услуг связи и переносимого трафика.

Такое деление на первичные и вторичные сети связи удобно ввиду достаточно существенных отличий в применяемых технологиях, моделях трафика и назначении. Если для транспортных сетей связи больше внимания уделяется обеспечению качества предоставления услуги переноса абонентского трафика, вопросам распределения приоритетов, надежности сетей связи, то при исследовании вторичных сетей в большей степени рассматривается информационная безопасность и синтез конкретного набора прикладных услуг связи. Если вопросы синтеза первичных сетей связи в большей степени ориентированы на эффективное распределение имеющихся ресурсов, то синтез вторичных сетей связи – на экономное их использование.

Транспортные сети связи занимают большую часть всех имеющихся в мире телекоммуникаций и включают как спутниковые и радиорелейные,

так и оптоволоконные системы связи, а также системы связи на базе коаксиальных и витых пар. От качества их совместной работы зависит не только доступные каждому связь по сети Интернет и сотовая связь, но и телекоммуникации между производственным оборудованием, работа систем охранной сигнализации, систем телемеханики, диспетчеризации и многое другое.

Среди всего многообразия сетевых технологий, которые применяются для формирования транспортных сетей связи, одно из центральных мест занимают технологии синхронной (СЦИ) и плезиохронной (ПЦИ) цифровых иерархии. И, если первая из этих технологий продолжает активно развиваться в виде NG SDH, то во второй технологии продолжает сохранять популярность лишь канал E1, который оказался эффективным и практически незаменимым, если необходимо объединить в одной линии большое количество разнородных низкоскоростных каналов управления технологическими процессами.

Как правило, эти две технологии используются совместно по причине их научно-технического «родства» и простоты переноса кадров E1 внутри виртуальных контейнеров VC12, которая достигается за счет одинаковой тактовой частоты работы этих сетей. Ниже приведена таблица 1, полученная в результате анализа ряда источников, среди которых [1, 2].

В таблице приведены абсолютные значения показателей без учета допустимых стандартами отклонений битовой скорости. Также в таблице в качестве базовых информационных каналов взяты E1 и STM-1, вместо E0 и STM-0 соответственно, что обусловлено тем фактом, что каналы E0 и STM-0 являются скорее теоретическими элементами иерархий скоростей, которые используются при анализе и синтезе аппаратуры оборудования, и практически не встречаются при эксплуатации.

Как видно из таблицы, каждая из перечисленных технологий имеет свои достоинства и недостатки, например, для переноса абонентского канала по транспортной сети СЦИ, необходимо либо использовать поток E1 для уплотнения, что имеет смысл, когда есть другие низкоскоростные каналы, либо, использовать контейнер VC12, в котором большая часть ресурса будет не задействована.

В то же время при переносе 60 каналов E1, в СЦИ требуется всего лишь 1 STM поток и мультиплексор первого уровня иерархии со скоростью передачи информации 155,52 Мбит/с, в то время как для технологии ПЦИ потребуется канал E4, скорость которого составляет 139264 Кбит/с, построенный с помощью мультиплексоров второго, третьего и четвертого уровней.

Однако, при пристальном рассмотрении этих технологий, несмотря на достаточно длинную их совместную историю, которая начинается в 80-х годах прошлого века, обнаруживается достаточно много проблем, причина

которых лежит, в основном, в существенном отставании развития стандартов ПЦИ от СЦИ в части применения современных методов управления – как минимум лет на 10.

ТАБЛИЦА. Показатели качества мультиплексирования ПЦИ и СЦИ

Показатель	Значение показателя в ПЦИ	Значение показателя в СЦИ
Тактовая частота	8 КГц	8 КГц
Базовая скорость передачи информации	2048 Кбит/с	155,52 Мбит/с
Вводимая скорость	64 Кбит/с	2 Мбит/с
Размер кадра	32 байта (кадр E1)	2430 байт (63 кадра E1 + заголовок)
Возможность переноса низкоскоростного канала	Внутри таймслота	Внутри VC12
Особенности ввода или вывода абонентского канала из потока верхнего уровня	Требуется выравнивание скоростей и дополнительное оборудование, выполняющее полный разбор потока	Требуется выравнивание скоростей
Максимальная скорость канала	565 Мбит/с	40 Гбит/с

В эпоху интенсивного развития распределенного автоматизированного производства сложившаяся ситуация приводит к существенному снижению эффективности управления технологическими процессами, зависящего от качества переноса управляющей информации.

В качестве примера можно привести общее количество сигналов технического обслуживания, которое в сетях СЦИ исчисляется несколькими десятками (порядка 50 типов) [1], в то время как в сетях ПЦИ для поддержки высокого качества обслуживания предусмотрено всего 14 [2].

В то же время и развитие технологии СЦИ еще далеко от совершенства. Примером могут служить значения параметров мониторинга производительности, которые трактуются разными производителями оборудования по-разному. Так, например, на сайте Cisco Systems, Inc. [3] приведена следующая информация, касающаяся анализа отклонений указателя в цикле и сверхцикле STM (JPE события): данные события являются следствием возникновения джиттера и вандера и причину следует искать в качестве системы синхронизации. Это подтверждается [1], где отмечено, что происхождение джиттера и вандера следует искать в качестве современных систем

синхронизации, которые с некоторой интенсивностью порождают кратковременные и длительные отклонения тактовой частоты, превышающие установленные нормы.

В то же время, в стандарте G.7710 [4] отмечено, что положительное и отрицательные отклонения указателя могут свидетельствовать о неправильном использовании источников синхронизации, то есть причину следует искать не только в качестве системы синхронизации, но в и ее использовании, качестве реализации переноса синхросигнала телекоммуникационным оборудованием, топологии сети и т. п. Там же отмечено, что поиск причин требует детального анализа каждой конкретной ситуации.

В стандарте [4] также сделано замечание относительно возможности мониторинга JPE событий удаленно: такой мониторинг невозможен по причине отсутствия предусмотренных для этих целей полей в заголовках фрейма. Работник, обслуживающий оборудование, получит сообщение об аварии, зафиксированной на дальнем конце линии (RDI), что может свидетельствовать о множестве возможных причин. Это особенно критично на этапе ввода линии в эксплуатацию, когда средства EMS охватывают сеть не полностью, либо, как часто бывает, требуют для своей работы работающий канал связи, которым они в дальнейшем будут управлять.

Помимо прочего, существующее многообразие сигналов технического обслуживания не учитывает реализацию и конфигурацию конкретного оборудования, где производитель волен вносить свои дополнения и механизмы. При исследовании функциональности оборудования синхронного мультиплексирования производства АО «Супертел» был проведен эксперимент по разрыву линии связи (одного из направлений) при различных настройках оборудования. Было выявлено, что в зависимости от настроек, разрыв линии может приводить либо к формированию сигнала LOS, либо RDI. Данная особенность не является ошибкой проектирования, а необходима для реализации различных топологий сети, предусмотренных международными стандартами, и подтверждает различием в специфике работы различных видов оборудования разных производителей.

Приведенные факты указывают на необходимость совершенствования существующих решений в области реализации технологий СЦИ и ПЦИ, а также совершенствования соответствующих стандартов.

Список используемых источников

1. Зингеренко Ю. А. Оптические цифровые телекоммуникационные системы и сети синхронной цифровой иерархии : учебное пособие. СПб. : НИУ ИТМО, 2013. 393 с.

2. Бакланов И. Г. Технологии измерений первичной сети. Часть 1. Системы Е1, PDH, SDH. М. : Эко-Трендз, 2000.

3. https://www.cisco.com/c/en/us/td/docs/optical/15000r4_0/15454/sdh/reference/guide/sdh40ref/e40epm.html (дата обращения 10.03.2020).

4. Международный стандарт ITU-I G.7710/Y.1701. G series: Transmission systems and media, digital systems and networks. Data over Transport – Generic aspects. Transport network control aspects. Common equipment management function requirements.

УДК 519.6 + 51-3
ГРНТИ 20.53.23

СЕТЬ ZIGBEE

С. М. Белов, Л. М. Макаров

Санкт-Петербургский государственный университет телекоммуникаций им. проф. М. А. Бонч-Бруевича

Современное развитие сетей связи стремительно захватывает платформы, решающие различные практические задачи. Сеть ZigBee формируется на основе локальных точек связи (доступа) с отдельными объектами, например, обладающими свойством передвижения. Обычно в качестве таких устройств рассматриваются устройства по очистке помещений – мобильные роботы. Такие устройства, снабженные блоком коммуникации на основе Bluetooth технологии, позволяют воспроизвести рабочие процедуры уборки заданной территории. В техническом отношении исполнительные устройства обладают самостоятельно собирать пыль, мыть поверхность или просто контролировать её частоту. Для исполнения этих задач в устройстве предусмотрен механизм независимого электропитания питания и передвижения.

ZigBee, беспроводные сети, автономное питание.

Актуальность темы связана с активным развитием беспроводных технологий, в особенности технологий персональных беспроводных сетей, для построения которых может использоваться технология ZigBee.

Область применения данной технологии достаточно обширна, что позволяет удовлетворить потребности, как для частного пользователя, так и крупного – например – автоматизировать процесс уборки улиц, где будет работать группа беспилотных уборочных машин с одной ведущей, которая будет координировать работу остальных, для повышения эффективности уборки. ZigBee также может использоваться для построения умного дома.

ZigBee представляет собой стандарт для высокоуровневых протоколов связи, использующих миниатюрные маломощные цифровые приёмопередатчики. В основе стандарта лежит IEEE 802.15.4-2006 для беспроводных персональных сетей, например, сетей беспроводные наушники – мобильный телефон [1].

Принимая во внимание технические возможности таких устройств, выпускаемых в массовом количестве, рассмотрим принцип построения сети из рабочих агрегатов. На рис. представлен типовой вид сети, созданной

на основе модели, в которой встроен модуль коммуникации по технологии Bluetooth. Каждое устройство обладает возможностью осуществлять прием и передачу служебной информации, предназначенной для других устройств, работающих под управлением некоторого общего центра – передвижного робота с функцией сервера.

В самом общем понимании взаимодействия всех элементов сети – подвижных объектов, по единой команде от робота сервера, вся сеть приходит в движение. На первых этапах развития событий в сети ставится задача построения. Все роботы стремятся выстроиться в линию, с максимальным удалением от соседей. Передача кодов управления по сети от ближайшего к серверу робота к последующему осуществляется, например, по порядковому номеру устройства, закрепленного в памяти.

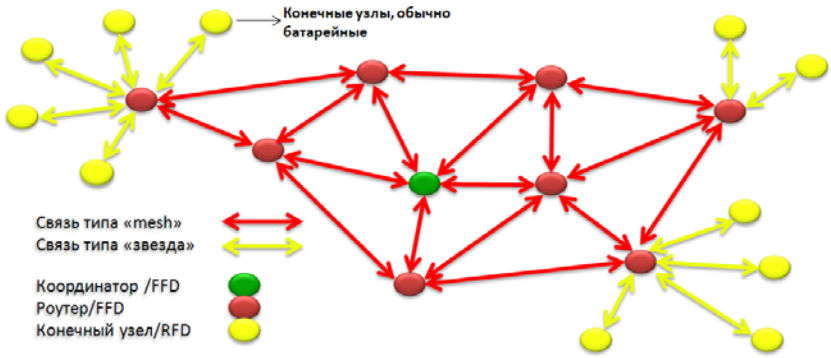


Рис. Типовая структура сети ZigBee

По завершении первого этапа, по сети связи проходит команда «приступить к исполнению рабочей функции» – уборке установленной площади. Благодаря наличию нескольких сенсорных устройств, включенных в конструкцию, каждый робот – уборщик осуществляет функцию уборки по произвольной траектории, подчас возвращаясь на уже пройденные участки площади. Однако в этих многочисленных треках передвижения есть общая цель – качественное исполнение рабочей функции, что и контролируется соответствующими сенсорами.

На данный момент существует множество инструментов, позволяющих организовать взаимодействие устройств в сети ZigBee. Можно использовать смартфон под управлением ОС Android или iOS с установленной программой для управления. Также можно управлять с помощью голосовых помощников: Apple Siri, Google Ассистент или Amazon Alexa.

Сеть ZigBee поддерживает ячеистую топологию. Сигнал передается между устройствами «по цепочке» до тех пор, пока информация не достигнет целевого узла. Все устройства сети ZigBee при необходимости могут выступать в качестве промежуточных узлов [2].

Внутри сети все устройства делятся на несколько групп:

Координаторы (ZC) – запускают сеть и задают команды для управления. Также они обеспечивают безопасность всех процессов.

Маршрутизаторы (ZR) – функционируют непрерывно и обеспечивают работу устройств, находящихся в режиме сна, а также передают данные и занимаются восстановлением узлов в случае большой загруженности или неисправности системы. Образуют соединение с координатором, другим маршрутизаторам или дочерними периферийными устройствами для передачи информации.

Оконечные устройства (ZED) – выполняют получение и отправку пакетов данных. Подключаются к координаторам или маршрутизаторам, но не могут подключать дочерние приборы. Работают с сенсорами, контроллерами и механизмами, выполняющими команды. Для экономии энергии часто работают в спящем режиме.

Список используемых источников

1. Шахнович И. В. Современные технологии беспроводной связи. М. : Техносфера, 2006. 288 с.

2. Стек протоколов ZigBee [Электронный ресурс]. URL: http://internetinside.ru/stek-ip-protokolov-zigbee/ (дата обращения 03.02.2020).

УДК 004.056.53
ГРНТИ 81.93.29

МОДЕЛЬ УГРОЗ IOT В ПРОГРАММНО-КОНФИГУРИРУЕМЫХ СЕТЯХ

Е. О. Березина[1], Л. А. Виткова[1,2]

[1]Санкт-Петербургский государственный университет телекоммуникаций им. проф. М. А. Бонч-Бруевича
[2]Санкт-Петербургский институт информатики и автоматизации Российской академии наук

Сети мобильной связи пятого поколения на базе технологий 5G активно внедряются и разворачиваются. Рост количества и многообразия мобильных устройств, сервисов, а также повышение требований, предъявляемых к полосе пропускания, обязывает большинство стран мира идти по пути скорейшего развертывания 5G. При этом для специалистов по информационной безопасности очевидны угрозы, с которыми сталкиваются такие сети связи. Сегодня нет единого международного центра, который взял бы на себя ответственность за разработку модели угроз и нарушителя в таких сетях. Авторы в данной работе рассматривают возможные угрозы и уязвимости беспроводной сети нового поколения на примере сети IoT и предлагают свой подход к систематизации угроз.

Интернет Вещей, классификация угроз, IoT, сети связи, угрозы информационной безопасности.

В последние годы наблюдается рост объемов мобильного и интернет-трафика. В частности, согласно Cisco Visual Networking Index (за 2019 г.) к 2022 году мир ожидает трехкратное увеличение потребляемого IP-трафика по сравнению с 2017 г.; мобильный трафик данных вырастет со средним показателем в 46 % в этот период, достигнув 77,5 эксабайт в месяц к 2022 году. Согласно этому же отчету, к 2022 году, среднегодовой темп прироста трафика мобильной передачи в России составит 43 %. Также к 2022 году трафик мобильной передачи данных в России достигнет 43,9 эксабайт и тем самым более чем в 6 раз превысит показатель 2017 года (7,3 эксабайт). Усредненный мобильный трафик на пользователя в России достигнет 29 Гбайт в месяц (5 Гбайт в 2017) [1].

Таким образом, современные тенденции, в частности рост числа подключенных к Интернету устройств, экспоненциальный рост объемов информации, а также развитие облачных технологий и Больших Данных, требуют пересмотра принципов построения сетей связи для обеспечения реализации требований этих новых технологий.

Ожидается [2, 3], что 5G повысит качество обслуживания конечных пользователей, предложив им новые приложения и услуги на гигабитных скоростях. Исследование 2017 года [4] показало то, что 77 % компаний признают факт того, что более широкое использование устройств IoT создает значительные проблемы с информационной безопасностью.

Существует множество работ, связанных с исследованием вопросов безопасности Интернета вещей. Отчет [5] посвящен подробному разбору вопросов, связанных с безопасностью 5G в целом, его ключевых технологий (таких как SDN и NFV). В таблице (см. ниже), обобщены основные материалы предыдущих комплексных исследований безопасности Интернета вещей.

На основании проведенного анализа рассмотрим модель угроз, представленную на рис. (см. ниже).

На основании предложенной модели угроз (рис.) можно сделать вывод, что основные угрозы безопасности IoT носят прикладной характер: использование специфических программ для кражи данных или внедрения вредоносного кода. В данном случае разумно использовать SDN для обеспечения безопасности, что также можно назвать программно-определяемой безопасностью [17]. Преимущества интеграции SDN в IoT описаны в [18]. Другие актуальные способы обеспечения безопасности IoT, такие как машинное обучение и применение нейронных сетей, описаны в [19, 20].

ТАБЛИЦА. Обзор релевантных работ в области информационной безопасности IoT

Источник	Суть исследования
Khan M.et al., [6]	Все угрозы безопасности IoT делятся на три уровня: вопросы безопасности высокого, среднего и низких уровней. Технология блокчейн как способ защиты
Maleh Y. et al., [7]	Рассматриваются вопросы безопасности с точки зрения конфиденциальности, целостности и доступности
Abdul-Ghani H. et al., [8]	Приводится сравнение удобства использования разных подходов к описанию архитектуры IoT, исследуются угрозы безопасности IoT по конфиденциальности, целостности, доступности, приватности, прозрачности, подотчетности, надежности и возможности отказа
Ahmad I. et al., [9]	Рассматриваются угрозы безопасности 5G в целом, дается краткое описание различных типов угроз и атак, отмечаются технологии (SDN), наиболее подверженные атакам или угрозам
Siddiqui S. et al., [10]	Рассматриваются угрозы безопасности трехуровневой архитектуры IoT с учетом уязвимостей протоколов, используемых на этих уровнях
Azam F. et al., [11]	Рассматриваются угрозы безопасности четырехуровневой IoT: добавляется слой промежуточного ПО. Для каждого уровня приводится перечень угроз и общие рекомендации по защите
Ahanger, T. A. et al., [12]	Рассматриваются угрозы безопасности IoT с точки зрения их применения: в умных домах, в индустрии и в медицине, а также актуальность киберугроз
Zhou W. et al., [13]	Рассматриваются угрозы безопасности IoT с точки зрения выделенных особенностей: взаимозависимость, разнообразие, множественность, отсутствие постоянного контроля, частность, мобильность, вездесущность, ограниченность
Hassija V. et al., [14]	Рассматриваются угрозы безопасности предлагаемой пятиуровневой архитектуре IoT: слой восприятия, сетевой, слой промежуточного ПО, слой приложений, а также пограничный слой
Mahmoud R. et al., [15]	Рассматриваются угрозы безопасности трехуровневой архитектуры IoT, выделяются наиболее распространенные проблемы каждого уровня, приводят способы решения, а также возможные проблемы, которые могут возникнуть при решении
Ataç C. et al., [16]	Рассматриваются вопросы IoT с точки зрения «что может помешать целям создания IoT», исходя из этого определяются требования безопасности к IoT, и уже на их основе вычленяются уязвимости и угрозы

Подводя итоги, стоит отметить, что стандартизация устройств Интернета вещей в настоящее время не завершена: каждое новое устройство, выходящее в Сеть, представляет собой еще один вектор атаки, и трудно разработать единые правила для всех. Целевая группа по инженерному обеспечению Интернета вещей (IETF) и другие органы по стандартизации работают над устранением этих пробелов.

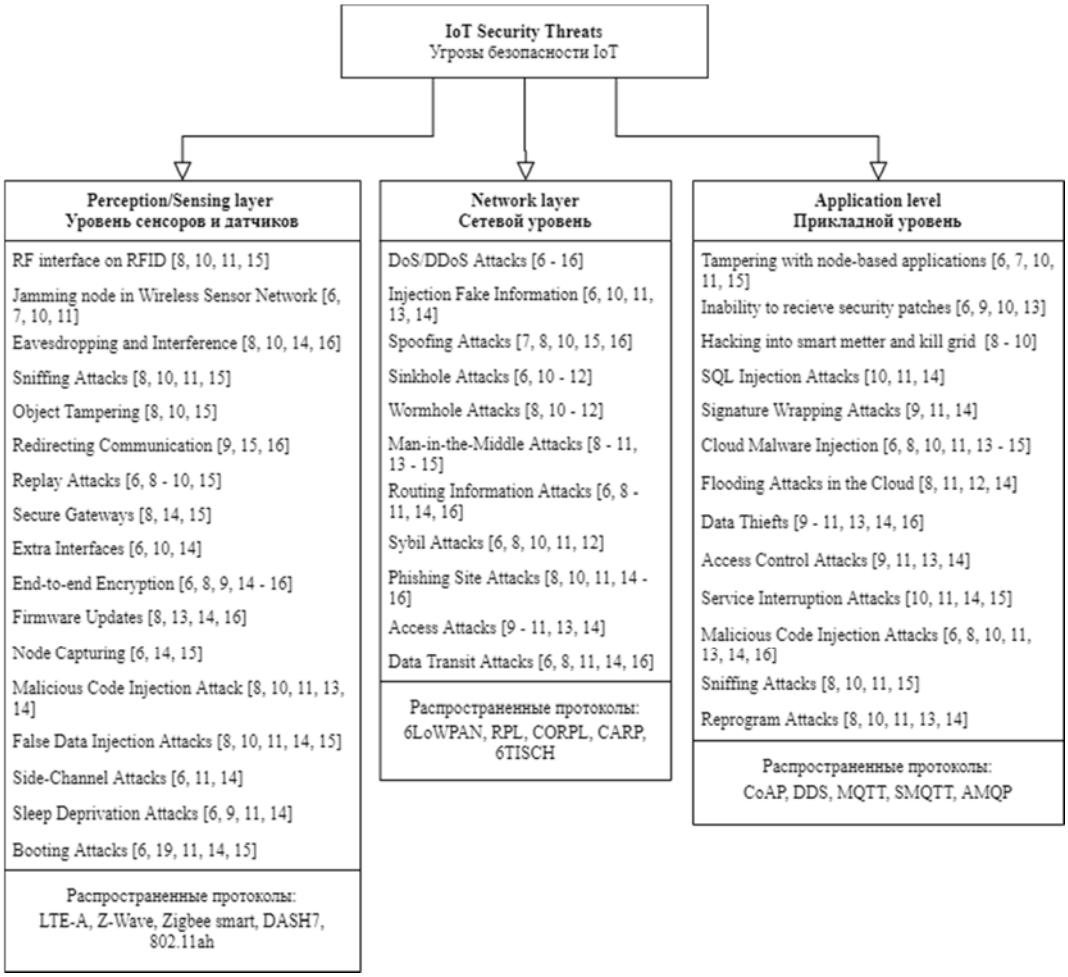


Рис. Модель угроз

5G еще предстоит развернуть; однако интеграция Интернета вещей, уже сейчас вызывает опасения в области безопасности. Необходимо искать новые решения, использующие развитие, например, искусственного интеллекта, или с использованием программируемости, обеспечиваемой SDN.

Работа выполнена при частичной финансовой поддержке бюджетной темы 0073-2019-0002 в СПИИРАН.

Список используемых источников

1. Cisco Visual Networking Index: Forecast and Trends // White Paper, 2017–2022.

2. Красов А. В., Сахаров Д. В., Ушаков И. А., Лосин Е. П. Обеспечение безопасности передачи multicast-трафика в ip-сетях // Защита информации. Инсайд. 2017. № 3 (75). С. 34–42.

3. Desnitsky, V. A., Kotenko, I. V., & Nogin, S. B. (2015). Detection of anomalies in data for monitoring of security components in the Internet of Things // 2015 XVIII International Conference on Soft Computing and Measurements (SCM). doi:10.1109/scm.2015.7190452.

4. Красов А. В., Косов Н. А., Холоденко В. Ю. Исследование методов провижининга безопасной сети на мультивендорном оборудовании с использованием средств автоматизированной конфигурации // Colloquium-journal. 2019. № 13–2 (37). С. 243–247.

5. Штеренберг С. И., Полтавцева М. А. Распределенная система обнаружения вторжений с защитой от внутреннего нарушителя // Проблемы информационной безопасности. Компьютерные системы. 2018. № 2. С. 59–68.

6. Khan, M. A., & Salah, K. (2018). IoT security: Review, blockchain solutions, and open challenges // Future Generation Computer Systems, 82, 395–411. doi:10.1016/j.future.2017.11.022.

7. Maleh, Y., Ezzati, A., & Belaissaoui, M. (2018). Security and Privacy in Smart Sensor Networks (pp. 1-441). Hershey, PA: IGI Global. doi:10.4018/978-1-5225-5736-4.

8. Abdul-Ghani H., Konstantas D. & Mahyoub M. A Comprehensive IoT Attacks Survey based on a Building-blocked Reference Model // International Journal of Advanced Computer Science and Applications (ijacsa), 9(3), 2018. URL: http://dx.doi.org/10.14569/IJACSA.2018.090349.

9. Ahmad I., Kumar T., Liyanage M., Okwuibe J., Ylianttila M., & Gurtov, A. (2018). Overview of 5G Security Challenges and Solutions. IEEE Communications Standards Magazine, 2 (1), 36–43. doi:10.1109/mcomstd.2018.1700063/

10. Siddiqui S., Alam S., Ahmad R. & Shuaib M. (2020). Security Threats, Attacks, and Possible Countermeasures in Internet of Things. 10.1007/978-981-15-0694-9_5.

11. Azam F., Munir R., Ahmed M., Ayub M., Sajid A. & Zaheer Abbasi, 2019. Internet Of Things (Iot), Security Issues And Its Solutions // Science Heritage Journal (GWS), Zibeline International Publishing, vol. 3 (2), pages 18–21, October. DOI: 10.26480/gws.02.2019.18.21.

12. Ahanger, T. A., & Aljumah, A. (2018). Internet of Things: A Comprehensive Study of Security Issues and Defense Mechanisms. IEEE Access, 1–1. doi:10.1109/access.2018.2876939.

13. Zhou, W., Jia, Y., Peng, A., Zhang, Y., & Liu, P. (2018). The Effect of IoT New Features on Security and Privacy: New Threats, Existing Solutions, and Challenges Yet to Be Solved // IEEE Internet of Things Journal, 1–1. doi:10.1109/jiot.2018.2847733.

14. Hassija, V., Chamola, V., Saxena, V., Jain, D., Goyal, P., & Sikdar, B. (2019). A Survey on IoT Security: Application Areas, Security Threats, and Solution Architectures // IEEE Access, 1–1. doi:10.1109/access.2019.2924045.

15. Mahmoud, R., Yousuf, T., Aloul, F., & Zualkernan, I. (2015). Internet of things (IoT) security: Current status, challenges and prospective measures // 2015 10th International Conference for Internet Technology and Secured Transactions (ICITST). doi:10.1109/icitst.2015.7412116.

16. Ataç, C., Akleylek, S. (2019). A Survey on Security Threats and Solutions in the Age of IoT // Avrupa Bilim ve Teknoloji Dergisi, (15), 36–42. DOI: 10.31590/ejosat.494066.

17. I. Ahmad et al. Security in Software Defined Networks: A Survey // IEEE Commun. Surveys & Tutorials, vol. 17, no. 4, 2015, pp. 2317–46.

18. Sood, K., Yu, S., & Xiang, Y. (2016). Software-Defined Wireless Networking Opportunities and Challenges for Internet-of-Things: A Review // IEEE Internet of Things Journal, 3(4), 453–463. doi:10.1109/jiot.2015.2480421.

19. I. Kotenko, I. Saenko, and A. Branitskiy. Applying Big Data Processing and Machine Learning Methods for Mobile Internet of Things Security Monitoring // Journal of Internet Services and Information Security, vol. 8, is. 3, pp. 54–63, 2018. http://www.jisis.org/vol8no3.php. DOI: 10.22667/JISIS.2018.08.31.054.

20. Branitskiy, A., & Kotenko, I. (2018). Applying Artificial Intelligence Methods to Network Attack Detection. Intelligent Systems Reference Library, 115–149. doi:10.1007/978-3-319-98842-9_5

Статья представлена доцентом кафедры ЗСС СПбГУТ, кандидатом технических наук А. А. Браницким.

УДК 621.391
ГРНТИ 49.33.29

ИМИТАЦИОННАЯ МОДЕЛЬ ФУНКЦИОНИРОВАНИЯ МУЛЬТИСЕРВИСНОЙ СЕТИ СВЯЗИ НА ПРИНЦИПАХ КОНЦЕПЦИИ NETWORK FUNCTIONS VIRTUALIZATION

К. Б. Боброва[1,2], А. К. Канаев[2], М. А. Сахарова[2,3]

[1]ОАО «Радиоавионика»
[2]Петербургский государственный университет путей сообщения Императора Александра I
[3]ЗАО «Институт телекоммуникаций»

Тенденция развития современных мультисервисных сетей связи (МСС) показала, что ближайший этап развития МСС базируется на основе концепции NFV, что должно обеспечить численное сокращение оборудования, гибкость настройки и масштабируемость ресурсов.

При этом этап планирования и проектирования МСС, как сложной технической системы, должен включать ряд комплексных процедур оценки основных показателей качества услуг и сетевой надежности NVF.

Разработана имитационная модель в среде AnyLogic на базе дискретно-событийных методов моделирования с учетом особенностей формирования, обработки и передачи трафика, внутренних процессов функционирования оборудования NVF узлов связи.

Результат моделирования позволил получить оценку вероятностно-временных характеристик процессов функционирования МСС на базе NFV, а представленная модель работоспособна и чувствительна к изменению исходных данных.

мультисервисная сеть связи (МСС), Network Function Virtualization (NFV), Quality of Service (QoS), гибкость, масштабируемость.

Рост потребностей пользователей в количестве и разнообразии телекоммуникационных услуг оказывает влияние на развитие и появление новых сетевых технологий. Увеличение спектра предоставляемых услуг ведет к пересмотру требований к современным сетям связи и качеству предоставляемых его услуг (QoS). Выполнение требований QoS одна из основных задач вендоров. В таких условиях поставщики телекоммуникационных услуг стремятся предоставить потребителям новые сервисы, построенные на основе современных информационно-коммуникационных технологиях, например: IoT, SaaS, Big Data, SDN, NFV и др.

В настоящее время мультисервисная сеть связи (МСС) строится на базе большого количества разнородного физического оборудования. В процессе эксплуатации оборудования поставщики услуг сталкиваются с проблемами, которые приводят к ухудшению требований QoS, а именно, к задержкам передачи данных и потерям пакетов. Также поставщики должны обеспечить

максимальную скорость и безопасность при передаче данных, и требования к МСС. МСС выполняет следующие функции:

1. предоставление пользователям доступа к ресурсам сети;
2. обеспечение гарантированного качества услуг;
3. обеспечение требований гибкости и масштабируемости сети для возможности дальнейшего наращивания и развития.

Сегодня крупные телекоммуникационные компании развивают технологию Network Functions Virtualization (NFV) [1]. Концепция виртуализации сетевых функций позволит пересмотреть подход к организации сети, создать гибкую архитектуру, а также делегировать сетевые функций от специализированных выделенных устройств на универсальные серверы.

Анализ материалов [2, 3, 4, 5, 6, 7, 8, 9] позволил обобщить особенности NFV, которые существенным образом могут улучшить характеристики формирования, обработки и передачи данных в МСС:

1. численное сокращение физического оборудования и трансформация инфраструктуры;
2. клиентоориентированные сетевые инфраструктуры;
3. упрощение процесса администрирования с высокими параметрами отказоустойчивости;
4. оперативность предоставления сервисов за счет использования облачных вычислений;
5. экономическая эффективность.

Несмотря на то, что технология NFV находится на стадии разработки, в последние годы она получила широкое распространение в различных областях [10, 11].

Телекоммуникационная отрасль активно внедряет в свои направления NFV. Операторы связи могут вводить новые услуги без наращивания сетевой инфраструктуры. Поставщики оборудования создают унифицированное телекоммуникационное оборудование с поддержкой NFV технологии.

Создание собственной IT-инфраструктуры в малом бизнесе, основанной на виртуальной облачной сети, охватывающий центр обработки данных, облако и периферийную инфраструктуру.

Российские компании разрабатывают средства серверной виртуализации и хранения данных для создания устойчивых продуктов на собственной платформе. Виртуализированная платформа предоставляет возможность для работы с вычислительными ресурсами, хранилищем, сетью, а также средства управления сетью и процессами.

Пусть реализован фрагмент МСС на базе NFV (далее МСС), в котором имеется n-узлов и l-каналов.

Каждый узел МСС принимает и обрабатывает трафик от m-пользователей. Каждый m-пользователь производит k-сообщений в единицу времени. Весь передаваемый объем информации перед передачей по сети

разбиваются на пакеты *p*-длиной (например, длина IP-пакета = 1500 байт), с установленным приоритетом (*R*). Каждый пакет содержит адрес абонента-получателя и передается по сети независимо от других (дейтаграммный режим). Принятое *n*-узлом сообщение хранится в буфере узла в течение заданного времени ($t_{ns} \le t_{ns\_зад}$), необходимого для отправки конечному узлу. В соответствии с заданным алгоритмом маршрутизации и при наличии свободного канала связи пакет передается до получателя.

Сообщение хранится в буферной памяти *n*-узла отправителя ограниченное время (тайм-аут) или до прихода получения квитанции о доставке ($t_{кв} \le t_{ns}$). При отсутствии квитанции в течение заданного интервала времени происходит повторная передача сообщения по выходящему каналу в направлении получателя. Для исключения бесконечного числа повторных передач одного и того же сообщения устанавливается предельное количество попыток ($A_{ns} \le A_{ns\_max}$) передать сообщение, после которого передача данного сообщения прекращается, и выбранное направление передачи (маршрут) исключается из рассмотрения и в дальнейшем не используется [12]. Для повторной передачи выбирается новое направление передачи в соответствии с таблицей маршрутизации.

Для анализа имитационного моделирования представим сеть в виде математических соотношений:

$$\begin{cases} n_s \in \{n_1, n_2 \cdots n_s\} \Rightarrow \{B_{ns}, t_{ns}, A_{ns}\}, \\ l_s \in \{l_{12}, l_{13} \cdots l_{ns}\}, \\ m_i \div n_s \in \{m_{i1}, m_{i2} \cdots m_{ij}\} \Rightarrow m_{nj} \to \{k, p\}, \end{cases};$$

при условии, если $p \le p_{зад}$; $k \equiv \infty$.

На основе всех вышеперечисленных факторов, данная модель МСС на базе NFV позволит оценить показатели качества обслуживания QoS [13], а именно $\{T_{ср}, K_{пот}\}$, где $T_{ср}$ – время задержки, $K_{пот}$ – коэффициент потерь, а также показатели надежности ($K_г$), где $K_г$ – коэффициент готовности канала электросвязи [14].

Фрагмент сети МСС представлен на рис. 1, в которую входят: отправитель, получатель, узел сети (маршрутизатор), каналы.

При моделировании введем следующие ограничения и допущения:

1. Ограниченный объем буферной памяти (B_{ns});
2. Обработка и распределение заявок выполняется согласно FIFO;
3. Рассматривается пуассоновский поток сообщений.

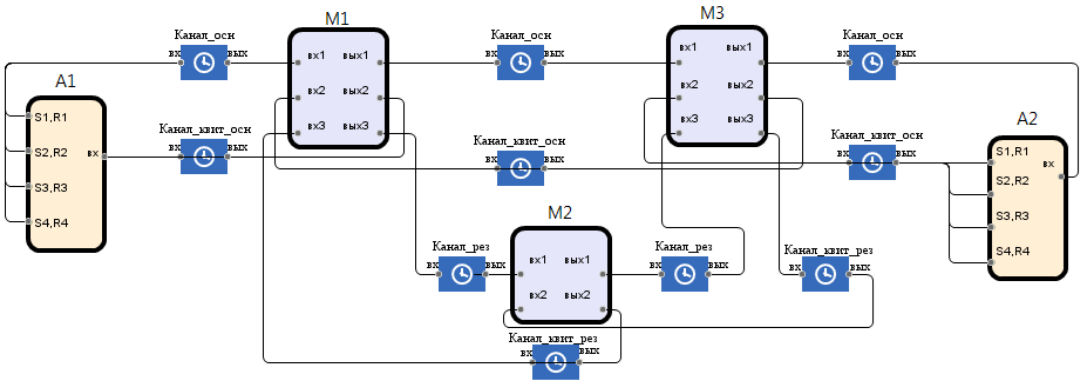


Рис. 1. Фрагмент сети верхнего уровня main программе AnyLogic

Исходные данные для моделирования представлены в таблице.

ТАБЛИЦА. Исходные данные

№	Название	Обозначение	Значение	
			МСС	NFV
1	Количество узлов	n_s	3 шт.	
2	Назначение каналов связи	l_s	2 (основной и резервный)	
3	Количество абонентов	m_i	2 (отправитель и получатель)	
4	Количество приоритетов сообщений	R_m	4	
5	Максимальный размер передаваемой информации каждой категории	p_{max_m}	{1500;3000;43500;43500} байт	
6	Максимальный размер пакета	p_{max}	1500 байт	
7	Скорость в канале связи от абонента до узла	V_1	1000000 Мбит/с	
8	Скорость в канале связи между узлами	V_2	1000000 Мбит/с	
9	Объем буфера маршрутизатора	B	56200 байт	1000000 байт
10	Максимальная величина времени задержки в каждом порту/модуле маршрутизатора	Z_{Wb}	10 мс	–
11	Модель обработки пактов в очереди в каждом узла	–	Согласно приоритету входящего сообщения (FIFO)	
12	Интенсивность формирования сообщений	L	от 25 до 5500 пак/мс	

Результаты доведения сообщений.

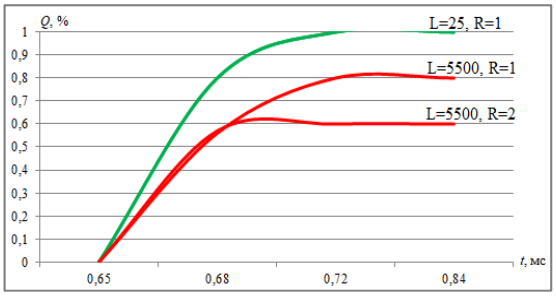
Как видно из графиков (рис 2 а, б), что:

1. по мере увеличения объема p_{max_m} передаваемого сообщения уменьшается вероятность доведения сообщения за заданное время, например,

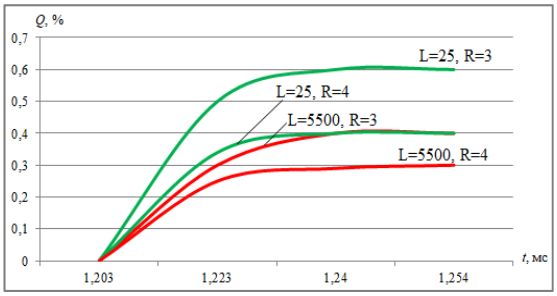
при увеличении p_{max_m1} до p_{max_m4} вероятность доведения сообщения уменьшается на 60 %, при этом время доведения для p_{max_m1} и p_{max_m4} увеличивается на 0,52 мс;

2. чем больше интенсивность L отправки сообщений, тем больше потребуется времени для доведения сообщения с заданной вероятностью;

3. вероятность доведения сообщений уменьшается при увеличении интенсивности генерации пакетов, например, при передаче сообщения первого приоритета вероятность доведения уменьшается в среднем на 20 %.



а) первый и второй приоритет сообщений



б) третий и четвертый приоритет сообщений

Рис. 2. Вероятность доведения сообщений в зависимости от размера и приоритета обработки в МСС

На рис. 3 показана зависимость вероятности доведения сообщений от времени передачи пакета. В частности, при малой интенсивности (25 пак/мс) наблюдается выигрыш МСС в сравнении с NFV при заданном времени доведения сообщения до 1,223 мс. Однако, вероятность доведения сообщения составляет не более 40 %, в то время как при использовании МСС на базе NFV вероятность доведения сообщения достигает 60 %.

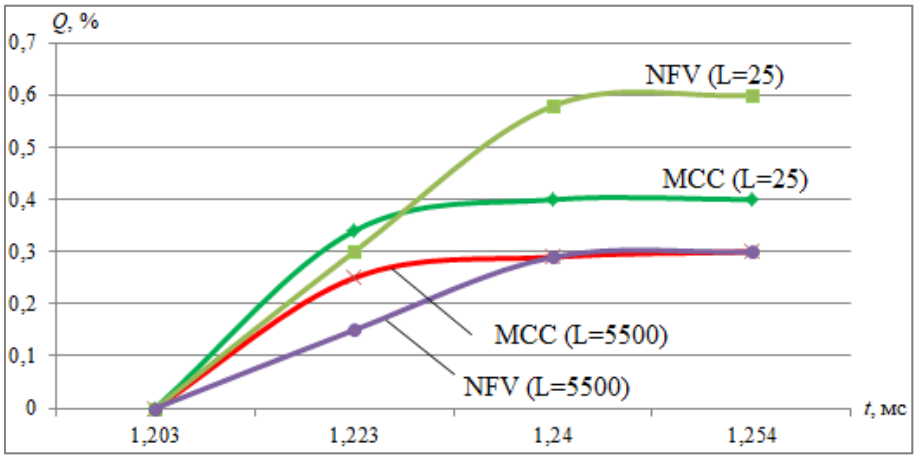


Рис. 3. Сравнение результатов доведения сообщений четвертого приоритета (43500 байт) для МСС и МСС на базе NFV

Подход, предлагаемый в данной работе, позволяет повысить качество обслуживания пользователей сети за счет применения технологии виртуализации сетевых функций.

Реализация МСС на базе NFV способна обеспечить оптимизацию инфраструктуры для работы в новых условиях. Возможность использовать относительно недорогие «неинтеллектуальные» коммутаторы, позволяет существенно снизить затраты операторов на модернизацию сетей для поддержки постоянно растущего трафика.

Список используемых источников

1. Новости ИТ и телекоммуникаций. Чем удивил Воентелеком «Армию-2016» [Электронный ресурс] // Воентелеком. URL: https://voentelecom.ru/news/novosti-kompanii/chem-udivil-voentelekom-armiyu-2016/ (дата обращения: 29.03.2019).

2. Портал о современных технологиях мобильной и беспроводной связи – Технологии SDN/NFV в развитии [Электронный ресурс]. URL: http://1234g.ru/novosti/tekhnologii-sdn-nfv-v-razvitii (дата обращения 17.03.2020).

3. Технологии связи – Обзор технологий SDN/NFV [Электронный ресурс]. URL: https://itechinfo.ru/content/technologies-sdnnfv (дата обращения 17.03.2020).

4. Ciena – Что такое NFV? [Электронный ресурс]. URL: https://www.ciena.ru/insights/what-is/What-is-Network-Functions-Virtualization_ru_RU.html (дата обращения 17.03.2020).

5. Стандарт ETSI (ETSI GS NFV 001 v1.1.1 2013-10).

6. Стандарт ETSI (ETSI GS NFV 004 v1.1.1 2013-10).

7. Forbes – Виртуальные сети: как телеком-операторы уводят вычисления в «облака» [Электронный ресурс]. URL: https://www.forbes.ru/tehnologii/342047-virtualnye-seti-kak-telekom-operatory-uvodyat-vychisleniya-v-oblaka (дата обращения 17.03.2020).

8. Стандарт ETSI (ETSI GS NFV-MAN 001 v1.1.1 2014-12).

9. Гениев А. VMware: NFV сокращает срок вывода новых услуг на рынок в 3–4 раза [Электронный ресурс] // TELECOMDAILY. URL: http://tdaily.ru/news/2017/07/07/artem-geniev-vmware-nfv-sokrashchaet-srok-vyvoda-novyh-uslug-na-rynok-v-3-4-raza (дата обращения 17.03.2020).

10. Новости цифровой трансформации, телекоммуникаций, вещания и ИТ «COMNEWS» – «Ростелеком» на грани SDN и NFV [Электронный ресурс]. URL: https://www.comnews.ru/content/100193/ 2016-03-23/rostelekom-na-grani-sdn-i-nfv (дата обращения 17.03.2020).

11. Новости цифровой трансформации, телекоммуникаций, вещания и ИТ «COMNEWS» – Виртуализация на марше [Электронный ресурс]. URL: https://www.comnews.ru/content/105950/2017-02-13/virtualizaciya-na-marshe (дата обращения 17.03.2020).

12. Алиев Т. И. Сети ЭВМ и телекоммуникации : учеб. пособие. СПб. : СПбГУ ИТМО, 2011. 399 с.

13. ГОСТ Р 53111-2008. Устойчивость функционирования сети связи общего пользования. Требования и методы проверки. М. : Изд-во стандартов, 2009. 15 с.

УДК 004.056.53
ГРНТИ 81.93.29

ОБЗОР МОДЕЛЕЙ И АЛГОРИТМОВ ОБНАРУЖЕНИЯ АНОМАЛЬНОЙ СИГНАЛИЗАЦИИ В IoT

Л. Н. Богданова[1], Д. А Клеверов[2], М. А. Клеверов[2]

[1]Санкт-Петербургский государственный университет телекоммуникаций им. проф. М. А. Бонч-Бруевича
[2]Санкт-Петербургский институт информатики и автоматизации Российской академии наук

Развитие сферы телекоммуникаций происходит с огромной скоростью. Одним из немаловажных этапов этого процесса является появление новой архитектуры мобильной связи и развитие Интернета вещей. В статье рассматриваются возможные угрозы, наследуемые от предыдущих поколений мобильной связи, а также представлен обзор алгоритмов машинного обучения обнаружения аномальной сигнализации в сетях IoT. Также авторами исследуются некоторые категории методов обнаружения аномалий в трафике, то есть классификация, статистические методы и кластеризация.

IoT, безопасность IoT, угрозы безопасности IoT, аномальная сигнализация, машинное обучение.

Обнаружение аномалий является важной задачей анализа данных, решение которой сводится к обнаружению отклонений в трафике. Причинами таких отклонений могут служить, как и неверно произведенные настройки, так и незаконные действия со стороны злоумышленников [1].

Алгоритмы обнаружение аномалий опираются на теорию математической статистики, вероятности и широко используются в машинном обучении [2, 3]. В качестве методов выявления аномалий в сигнальном трафике 5G возможно использовать алгоритмы, основанные на существующих подходах к обнаружению сетевых аномалий. В [4] рассматриваются методы классификации, кластеризации, а также статистического анализа, на основе которых создаются алгоритмы обнаружения сетевых аномалий. Эти алгоритмы, по большей части, реализуются с помощью машинного обучения.

Методы классификации

Алгоритмы, использующие метод классификации, создаются исходя из заранее полученных знаний о характеристиках сетевых атак. Иными словами, атака с заранее известным шаблоном может быть обнаружена сразу после ее запуска [5]. Далее приведены алгоритмы, реализованные на основе метода классификации.

1. SVM (*Support Vector Machine*).

Основной принцип машины опорных векторов (SVM) состоит в том, чтобы получить гиперплоскость, которая максимизирует разделительную границу между положительным и отрицательным классами исследуемых данных. Стандартный алгоритм SVM является контролируемой техникой машинного обучения, которая требует помеченных данных для создания правила классификации. В [6] рассматривается концепция неконтролируемого SVM для обнаружения аномальных событий. Алгоритм находит гиперплоскости, которые отделяют экземпляры данных от их источников с максимальным запасом. После этого решается задача оптимизации, в результате решения которой определяется наилучшая гиперплоскость.

2. Байесовская сеть.

Байесовская сеть является эффективным подходом для моделирования области, содержащей неопределенность. Дискретная случайная величина представляется с использованием ориентированного ациклического графа (DAG), где каждый узел отражает состояние случайной величины и содержит таблицу условных вероятностей (CPT). Задача CPT состоит в том, чтобы обеспечить вероятность того, что узел находится в определенном состоянии [7]. В байесовской сети между узлами существуют родительско-дочерние отношения, которые указывают, что переменная, представленная дочерним узлом, зависит от переменных, представленных родительскими узлами. Байесовская сеть применяется для выявления аномальных событий путем введения корневого узла, который представляет переменную с двумя состояниями. Один дочерний узел используется для захвата выходных данных модели, а второй подключен к корневому узлу. Ожидается, что выходные события будут отличаться, когда входные данные будут ненормальными или нормальными.

Предполагается, что системы обнаружения аномалий содержат ряд проблем, которые могут возникнуть при анализе различных особенностей событий. Во-первых, модели, которые обеспечивают оценку или вероятность ненормальности события, требуют, чтобы система обнаружения аномалий объединяла их различные выходные данные, которые приводят к большому количеству ложных срабатываний (ошибка 1 рода). Во-вторых, системы обнаружения аномалий не могут обрабатывать поведение, которое является необычным, но законным, например, внезапное увеличение загрузки ЦП, использование памяти и т. д.

В [4] предложен подход для решения вышеупомянутых проблем, основанный на концепции байесовской сети. Для упорядоченного потока входных событий ($S = e_1; e_2 \ldots$) система классификации событий решает, является ли событие нормальным или нет. Это решение основано на результатах ($o_i | \ i = 1; 2; \ldots; k$) из k моделей ($M = m_1; m_2; \ldots; m_k$) и возможной дополнительной информации (I). Модели анализируют особенности заданного входного

события и сравнивают их результаты с результатами ранее созданных моделей. Результат от системы классификации событий (*EC*) определяется как:

– $EC(o_1, o_2, \dots, o_k, I) = e$ – нормальное событие;
– $\sum_{i=1}^{k} o_i \leq I || e$ – аномальное событие;
– $\sum_{i=1}^{k} o_i > I$ – аномальное событие.

Статистические методы

Статистические методы обнаружения аномалий основываются на анализе накопленных данных. Предполагается, что создается профиль нормальных событий в информационной системе. Основная идея заключается в обнаружении как большого отклонения событий от нормы, так и аномалий, и вторжений [8, 9].

Основываясь на концепции, что аномалия лежит в большом количестве нормальных элементов, в [4] рассмотрена смешанная модель для обнаружения аномалий по данным шума. Как правило, в смешанных моделях каждый элемент относится к одному из следующих двух классов:

– с малой вероятностью λ, или
– большинство элементов, имеющих вероятность 1 – λ.

С точки зрения обнаружения вторжений, набор системных вызовов с вероятностью 1 – λ является легальным использованием системы, а вторжения имеют вероятность λ. С точки зрения смешанной модели, два вероятностных распределения, которые генерируют данные, называются мажоритарным (*M*) и аномальным (*A*) распределениями, причем элемент (x_i) генерируется из любого из них. Когда генеративным распределением для данных является *D*, оно может быть представлено как

$$D = (1 - \lambda)M + \lambda A.$$

Элементы данных, генерируемые из распределения *A*, считаются аномальными.

Методы кластеризации

Кластеризация относится к неконтролируемым методам обучения, которые не требуют предварительно помеченных данных для извлечения правил группировки похожих экземпляров данных. В отличие от классификации и статистики, выходные данные в кластеризации рассматриваются в двоичном виде, то есть, трафик является нормальным, либо аномальным. Методы, предоставляющие на выходе двоичные метки, являются вычислительно эффективными, поскольку каждый экземпляр данных не должен предоставлять или иметь оценку аномалии [4]. Использование метода кла-

стеризации, как правило, предусматривает 3 ключевых предположения, которые принимаются во внимание при разработке алгоритмов обнаружения аномалий:

1. Поскольку создаются кластеры только нормальных данных, любые последующие новые данные, которые не соответствуют существующим кластерам нормальных данных, считаются аномалиями [10].

2. Когда кластер содержит как нормальные, так и аномальные данные, нормальные данные лежат близко к центроиду ближайших кластеров, а аномальные находятся далеко от центроидов. При этом допущении аномальные события обнаруживаются с использованием показателя расстояния.

3. В кластере с кластерами разных размеров, меньшее и разреженное можно считать аномальным, а большие - нормальным. Экземпляры, принадлежащие кластерам с размерами и/или плотностями ниже порога, считаются аномальными.

В [10] приведен подход, использующий алгоритм кластеризации к аномальным данным. Этот алгоритм использует кластеризацию данных для генерации нормальных и аномальных кластеров.

Вывод

Существующие методы обнаружения аномалий в основном предназначены для мониторинга одной системы или одной сети путем проведения локального анализа атак. Между такими методами обнаружения аномалий не существует взаимодействия, однако можно сравнить эффективность алгоритмов, применяемых для обнаружения атак.

В дальнейшем авторы планируют проведение экспериментов, и в связи с тем, что только методы кластеризации не требуют размеченных данных, однако показывают высокий уровень точность, аккуратности, в работе будут использоваться изначально методы, предложенные в [10].

Работа выполнена при частичной финансовой поддержке РФФИ (проект 18-07-01369) и бюджетной темы 0073-2019-0002.

Список используемых источников

1. Штеренберг С. И., Виткова Л. А., Просихин В. П. Методика применения концепции адаптивной саморазвивающейся системы // Информационные технологии и телекоммуникации. 2014. Т. 2. № 4. С. 126–133.

2. Виткова Л. А. Андрианов В. И. Исследование и разработка адаптивных систем информационной безопасности на основе теории бифуркации // Актуальные проблемы инфотелекоммуникаций в науке и образовании. II Международная научно-техническая конференция: сб. науч. ст. СПб. : СПБГУТ, 2013. С. 813–815.

3. Герлинг Е. Ю., Кулишкина Е. И., Бирих Э. В., Виткова Л. А. Модели нарушителей информационной безопасности // Известия высших учебных заведений. Технология легкой промышленности. 2017. Т.3 5. № 1. С. 27–30.

4. Mohiuddin Ahmed, Abdun Naser Mahmood, Jiankin Hu. Canberra: A survey of network anomaly detection techniques, 2015. P. 4.

5. Браницкий А. А., Котенко И. В. Анализ и классификация методов обнаружения сетевых атак // Труды СПИИРАН. 2016. № 2 (45). С. 207–244.

6. Kruegel C., Mutz D., Robertson W., Valeur F. Bayesian event classification for intrusion detection // In: Proceedings of 19th annual computer security applications conference. 2003. P. 14–23.

7. Браницкий А. А. Иерархическая гибридизация бинарных классификаторов для выявления аномальных сетевых соединений // Труды СПИИРАН. 2017. № 3 (52). С. 204–233.

8. Никитин В. Н., Ковцур М. М., Юркин Д. В. Повышение защиты протоколов распределения ключей от атак вторжения в середину канала связи // Информационно-управляющие системы. 2014. № 1 (68). С. 70–75.

9. Ковцур М. М., Никитин В. Н. Оценка вероятностно-временных характеристик защищенной IP-телефонии // Защита информации. Инсайд. 2012. № 4 (46). С. 38–44.

10. Münz G., Li S., Carle G. Traffic anomaly detection using kmeans clustering // In GI / ITG Workshop MMBnet, 2007.

Статья представлена доцентом кафедры ЗСС СПбГУТ, кандидатом технических наук А. А. Браницким.

УДК 654.026
ГРНТИ 49.13.01

МОДЕЛЬ УСТРОЙСТВА СОПРЯЖЕНИЯ ИНТЕРФЕЙСОВ ТЕЛЕКОММУНИКАЦИОННОГО ОБОРУДОВАНИЯ ПОЛЕВЫХ И СТАЦИОНАРНЫХ КОМПОНЕНТОВ ТРАНСПОРТНОЙ СЕТИ СВЯЗИ СПЕЦИАЛЬНОГО НАЗНАЧЕНИЯ

А. П. Бойко, М. А. Таранов

Военная академия связи имени Маршала Советского Союза С. М. Буденного

В настоящее время транспортная сеть связи ВС РФ представлена двумя компонентами, для взаимодействия которых необходима привязка комплексных аппаратных связи к узлам связи доверенных операторов. Однако, для обеспечения отбора цифровых каналов и групповых трактов в точках приема в настоящее время не предусмотрено оборудование, обеспечивающее совместимость интерфейсов полевых и стационарных компонентов транспортной сети, и повышающее оперативность предоставления услуг.

транспортная сеть связи ВС РФ, сопряжение, физические интерфейсы, оперативность предоставления услуг.

В настоящее время транспортная сеть связи ВС РФ представлена двумя компонентами: стационарным и полевым. Физическую основу стационарной компоненты транспортной сети связи составляют волоконно-оптические линии связи (ВОЛС). Однако, строительство собственных ВОЛС является экономически сверх затратным, и в этих условиях единственным выходом является аренда телекоммуникационного ресурса у доверенных операторов связи. В свою очередь полевая часть транспортной сети связи развёртывается по мере необходимости для наращивания, усиления и резервирования стационарной части, а также для обеспечения управления войсками при отсутствии стационарной части или ее разрушении, а также в ходе операции [1, 2].

Для взаимодействия полевого и стационарного компонентов транспортной сети комплексные аппаратные связи привязываются к стационарным узлам связи доверенных операторов. Однако, при проведении отбора цифровых каналов и групповых трактов в точках приема возникают проблемы, связанные с разнородностью интерфейсов физического уровня и видами применяемых технологий.

Не редко на разработку и поиск технических решений по согласованию оборудования полевой и стационарной транспортных сетей затрачивается существенный временный ресурс. Возникающие проблемы сопряжения интерфейсов способствуют снижению оперативности предоставления услуг должностным лицам пунктов управления. Поэтому задача по созданию устройства, позволяющего согласовывать типы физических интерфейсов полевой и стационарной компонентов транспортной сети связи специального назначения, является весьма актуальной.

Решение подобной задачи нашло своё отражение в вооруженных силах стран НАТО. Применение волоконно-оптических кабельных сборок значительно сокращает временные показатели по прокладке кабельных линий между оконечными пунктами стационарных и полевых узлов связи, путем согласования используемых разнородных типов интерфейсов, а вместе с тем способствует оперативности выполнения поставленных задач по предоставлению различных видов услуг.

В современных условиях в ВС РФ не предусмотрено оборудование, обеспечивающее совместимость технических средств связи стационарных узлов связи с оборудованием, входящим в состав комплексных аппаратных связи. Так при использовании базовых узлов транспортной сети (узлов устранения цифрового неравенства, УУЦН), обеспечивающих подключение к транспортной пакетной сети и базовых узлов оптической сети (шкафов энергетиков, ШЭ),обеспечивающих подключение к магистральной ВОЛС

в процессе проведения мероприятий по отбору цифровых каналов и групповых трактов возникают проблемы подключения, вызванные отличительными особенностями интерфейсов, применяемых, приоритетно, в стационарной компоненте транспортной сети связи.

В то время как в составе комплексных аппаратных связи предусмотрено наличие лишь внутриузлового, распределительного кабеля П-269М, а также полевого одномодового оптического кабеля ОК-ВМ-4Т, линзовый соединитель которого не позволяет подключиться к оборудованию доверенного оператора.

В настоящей статье представлена модель устройства, предназначенного для решения возникающих проблем по сопряжению типов интерфейсов различных компонентов транспортной сети связи, которая наиболее полно соответствует решению данной задачи.

Основными элементами представленного устройства являются: оптическая патч-панель, оптический Ethernet-конвертер, фотонный коммутатор, а также различные типы разъёмов для подключения коннекторов, непосредственно использующихся в стационарной компоненте транспортной сети связи.

Проблемы, связанные со сложностью подключения оптического кабеля с линзовым соединителем из состава КАС в предлагаемом устройстве решаются с использованием однотипной полумуфты, применяемой на стыке телекоммуникационного оборудования транспортной сети связи доверенного оператора. При согласовании направляющих систем два оптических волокна используются для приема/передачи клиентского сигнала, в то время как два других волокна задействованы для приема/передачи управляющего Ethernet-сигнала. С помощью фотонного коммутатора осуществляется распределение клиентского сигнала на различные типы оптических и электрических интерфейсов. Для передачи оптического излучения в сторону электрических интерфейсов, клиентский сигнал дополнительно претерпевает преобразование в электрический вид. Управление работой данного устройства предусмотрено не только по Ethernet сигналу, передаваемому вместе с клиентским сигналом по одной направляющей системе, но, а также сигналом, поступающим к устройству с ПЭВМ, располагающегося в непосредственной близости. На рисунке (см. ниже) представлен вариант применения предлагаемого устройства по сопряжению физических интерфейсов телекоммуникационного оборудования при взаимодействии полевой и стационарной компонентов транспортной сети связи.

Управление распределением клиентского сигнала по различным типам физических интерфейсов, присущим оборудованию, применяемому в узлах связи доверенного оператора может осуществляться с помощью оборудования, размещенного в КАС.

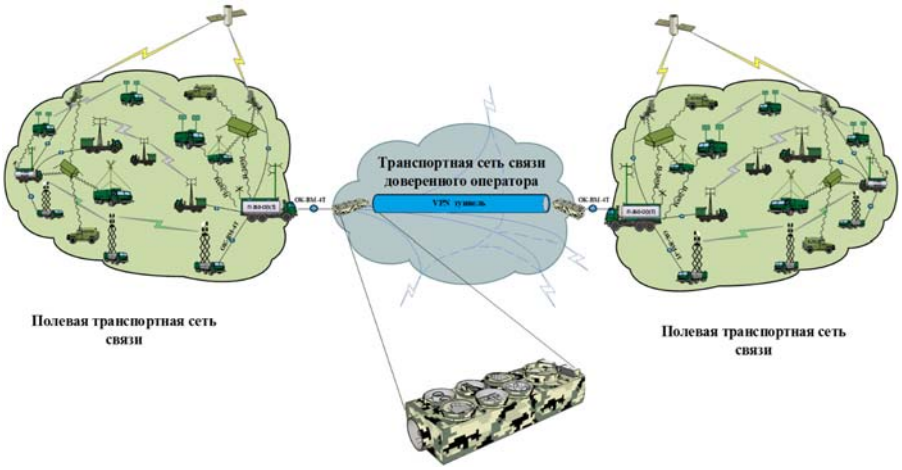


Рис. Вариант применения устройства сопряжения физических интерфейсов телекоммуникационного оборудования полевых и стационарных компонентов транспортной сети связи

Возможность использования множества различных физических интерфейсов, а также дистанционное управление работой устройства способствует повышению оперативности предоставления услуг должностным лицам.

Список используемых источников

1. Макаренко С. И. Перспективы и проблемные вопросы развития сетей связи специального назначения // Системы управления, связи и безопасности. 2017 № 2. С. 18–68.

2. Буренин А. Н., Легков К. Е. Особенности архитектур, функционирования, мониторинга и управления полевыми компонентами современных инфокоммуникационных сетей специального назначения // Наукоемкие технологии в космических исследованиях Земли. 2013. Т. 3. С. 12–17.

УДК 004.738, 621.391
ГРНТИ 49.01.81

ОПРЕДЕЛЕНИЕ КЛАССОВ КАЧЕСТВА СЕТИ ПЕРЕДАЧИ ДАННЫХ ПО ОЦЕНКАМ ВРЕМЕНИ ЗАДЕРЖКИ НА ИНТЕРФЕЙСАХ UNI-UNI

П. Е. Бородина, С. А. Владимиров

Санкт-Петербургский государственный университет телекоммуникаций им. проф. М. А. Бонч-Бруевича

Работа представляет результаты тестирования сегментов сетей передачи данных с целью оценки класса качества сети согласно рекомендациям ITU-T Y.1540, Y.1541

и Y.1543. Тестирование времени задержки сетей на передачу пакетов производится программным тестером, разработанным на кафедре Сетей связи и передачи данных СПбГУТ. Операция тестирования с протоколированием результатов производится со стороны измерительного сервера на базе интерфейсов UNI-UNI. Особенностью программного обеспечения для тестирования является отсутствие требований для синхронизации часов клиентской и серверной стороны. Основная цель работы заключена в практической отработке вариантов тестирования сетей и анализе полученных результатов.

класс качества сети передачи данных, QoS, показатели уровня обслуживания, SLA, время задержки пакетов, джиттер, потери IP-пакетов.

Рассматривая существующие в настоящее время услуги на телекоммуникационных сетях, можно сказать, что большая часть из них требует соблюдения определенных критериев по качеству с точки зрения технических параметров доставки контента. Разбиение сетей по классам качества QoS определено в руководящем документе ITU-T Y.1541 [1]. Указанная рекомендация определяет классы качества обслуживания (QoS) для сетей с требованиями к техническим параметрам показателей качества по протоколу IP. Такое разбиение по классам применяется для IP-сетей общего пользования и при этом предполагается, что рекомендации по качеству и приведенные требования реально достижимы на обычных реализациях IP-сети.

Производительность собственной сети устанавливается поставщиком услуг (SP) и отслеживается ее пользователями, что подтверждает доверие к объявленному качеству сети (показатели уровня обслуживания SLA). Особенностью такой оценки является рассмотрение сквозной производительности, то есть объединенной производительности по нескольким сегментам сети или по нескольким гетерогенным SP, включая собственные частные сети пользователей. Существующие стандарты определяют несколько метрик и методов измерения для двухточечной производительности типа UNI-UNI. Следует отметить стандарты ITU-T Y.1540 и Y.1541, а также стандарты Рабочей группы IETF по показателям производительности протокола Интернета (IPPM). При этом, многие параметры остаются неуказанными, как и сопоставление между показателями для IP-сетей и не-IP-сетей, не определены точность и порядок обработки данных. Каждый из этих вопросов должен быть указан для поддержки QoS или параметров SLA между несколькими гетерогенными SP.

Недавняя рекомендация ITU-T Y.1543 [2] направлена на разъяснение этих вопросов и определяет основные варианты измерений производительности, проводимых операторами в рамках зоны действия своей сети, которые могут быть объединены для оценки сквозной производительности сетей или междоменного QoS и обеспечение научного подтверждения результатов таких измерений с целью локализации сбойных узлов и источников

ошибок на сетях. Помимо этого, измерения UNI-UNI, проводимые пользователями позволят:

– обеспечить поставщиков услуг данными о производительности их сети в разных маршрутных направлениях;

– проводить мониторинг и своевременно устранять повреждения на своих сетях по разным маршрутным направлениям;

– производить мониторинг производительности других сетевых операторов;

– обеспечивать информацией системы и их компоненты, задачей которых является автоматизированное управление сетью.

ITU-T Y.1543 определяет точки разделения доменов, как точки разграничения (DP) между сетями доступа и сетями транзита, края поставщиков услуг (PE), края клиентских сетей (CE) и другие точки размещения оборудования для инициации измерений. Указывает, что в распределении односторонней задержки пакета в потоке пакетов опорной является минимальная задержка потока и все изменения оценивают относительно этого минимума. Задает среднее отклонение (сглаженное абсолютное значение) разности прихода данных для пакетов различной длины для пары пакетов. Обозначает следующие параметры производительности сети для характеристики междоменного QoS [2]:

– средняя задержка в одном направлении;

– минимальная задержка;

– изменение задержки в одном направлении (PDV);

– коэффициент потери пакетов (PLR);

– недоступность пути.

Рекомендация определяет период времени нарушения QoS или SLA и период недоступности [2]. При этом, измерения могут проводиться для каждого из сегментов сети и могут быть рассмотрены и объединены для формирования многосегментных, межсайтовых, сквозных измерений или измерений IP-терминал к IP-терминалу. Подмножество этих заданных метрик может и будет использоваться для отчетов поставщиков по предлагаемым услугам.

Формулы Литтла позволяют оценить доступную пропускную способность маршрута (сглаженное абсолютное значение разности прихода данных для пакетов различной длины для пары пакетов), используя данные о задержке пакетов [2]:

$$BR = \frac{(L_2 - L_1)}{(IPTD_2 - IPTD_1)}, \text{бит/с.}$$

Относительная погрешность доступной пропускной способности:

$$\eta = \frac{2 \cdot \Delta TD \cdot 100}{(IPTD_2 - IPTD_1)}, \%.$$

где L – длина пакета, бит; $IPTD$ – время задержки пакета UNI-UNI, мкс; ΔTD – точность измерения задержки, мкс.

Разработанная на кафедре ССиПД СПбГУТ программа оценки качества обслуживания сети выполняет раздельное тестирование сегментов сетей передачи данных от устройства, на котором установлен сервер тестирования до устройства, на котором установлен клиент тестирования, по протоколам TCP и UDP [3]. На хосте-сервере запускается программа-демон, которая создает и инициализирует «слушающий» сокет [4], ожидающий получение пакетов от программ-клиентов, запущенных на выбранных для тестирования других хостах сети. Пришедший от клиента пакет, информирующий о попытке установить соединение, сервер записывает в память, после чего выделяет адрес этого хоста в массив соединений для дальнейшего использования и отправляет ответный пакет, информирующий клиента о том, что соединение успешно установлено, сервер готов и работа по тестированию будет продолжена. В окне терминала сервера выводится оперативная информация обо всех хостах, записанных в массиве соединений сервера: IP-адрес, порт и время пинга [3]. Схема проведения тестирования сегментов сетей передачи данных представлена на рис. 1.

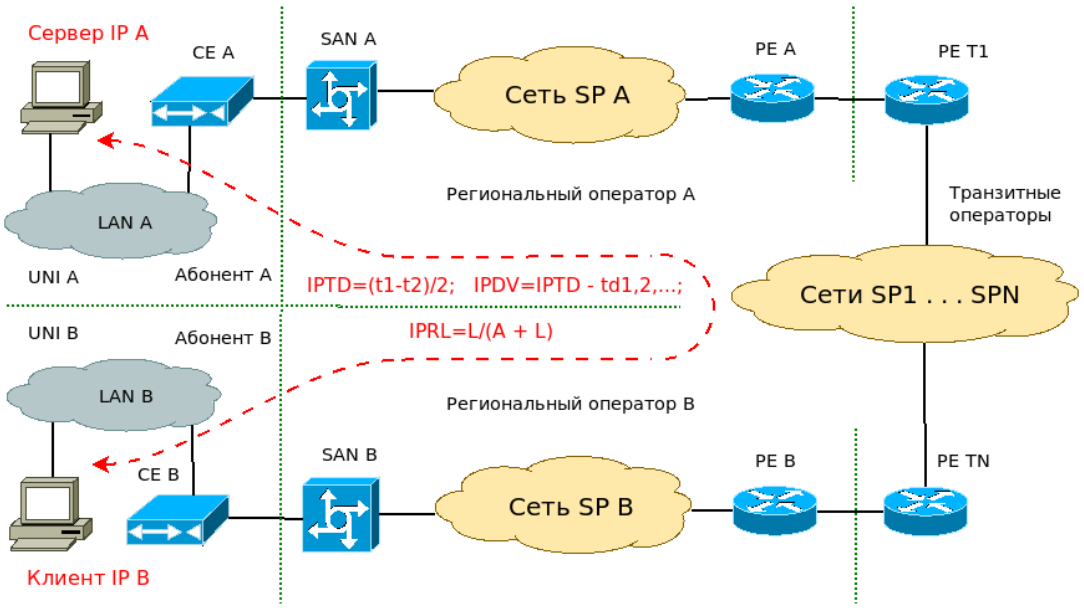


Рис. 1. Схема тестирования сегментов сети UNI-UNI

Пользователь со стороны сервера выбирает с каким клиентским хостом необходимо выполнить передачу пакетов для оценки качества соединения и инициирует процесс тестирования. Между сервером и клиентом выполняется информационный обмен пакетами с изменением их размера от 65 до 1300 байт с шагом 65 байт. В процессе обмена для каждого из пакетов оценивается время задержки передачи пакета, вариация задержки, а также

потеря пакетов. Оценка выполняется с точностью до 1 микросекунды, стабильность которой соответствует стабильности кварцевого генератора внутренней тактовой синхронизации устройства, выполняющего роль сервера. Им выступает обычный пользовательский компьютер под управлением операционной системы Linux или Windows. Роль сервера или клиента выбирается при запуске с дополнительным указанием клиенту IP-адреса хоста-сервера. Так как инициатором измерений является сервер, и он же выполняет оценку времени задержки, дополнительная синхронизация времени на хостах-партнерах по измерению не требуется.

На рис. 2 представлены измеренные характеристики соединения СПбГУТ (сервер) – Кудрово (клиент) по протоколу UDP. Провайдер Ростелеком. Технология доступа PON со скоростью 150 Мбит/с. Расчетные значения *BR* = 12682927 бит/с ± 0,26 % и *IPRL* = 0 %. Класс качества QoS = 0. На гистограмме четко отслеживаются четыре устойчивых маршрута.

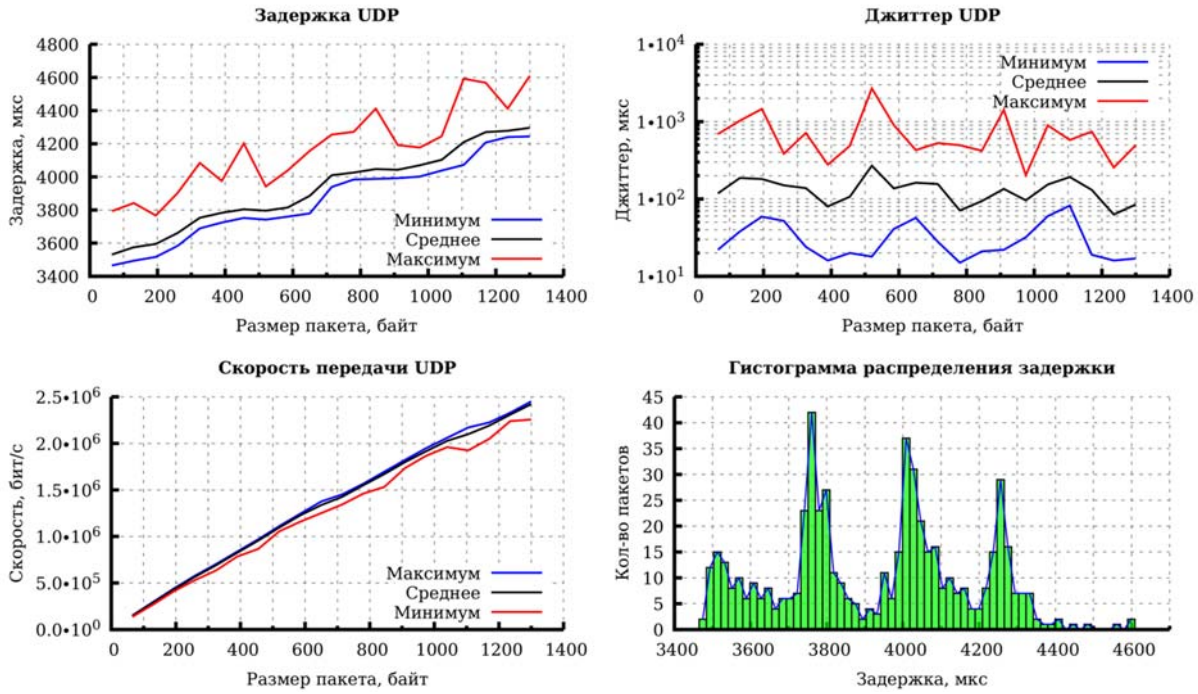


Рис. 2. Данные тестирования СпбГУТ (сервер) ‑ Кудрово (клиент). IP 92.101.237.193

На рис. 3 (см. ниже) представлены измеренные характеристики соединения СПбГУТ (сервер) – Казахстан (клиент) по протоколу TCP. Провайдер Казахтелеком. Технология доступа FTTB со скоростью 100 Мбит/с. Расчетное значение *BR* = 1371460 бит/с ± 0,03 %. Класс качества QoS = 0.

Результаты тестирования по протоколу TCP на рис. 3 показывают хорошие стабильные маршруты и приемлемое качество для такой дистанции сети передачи данных.

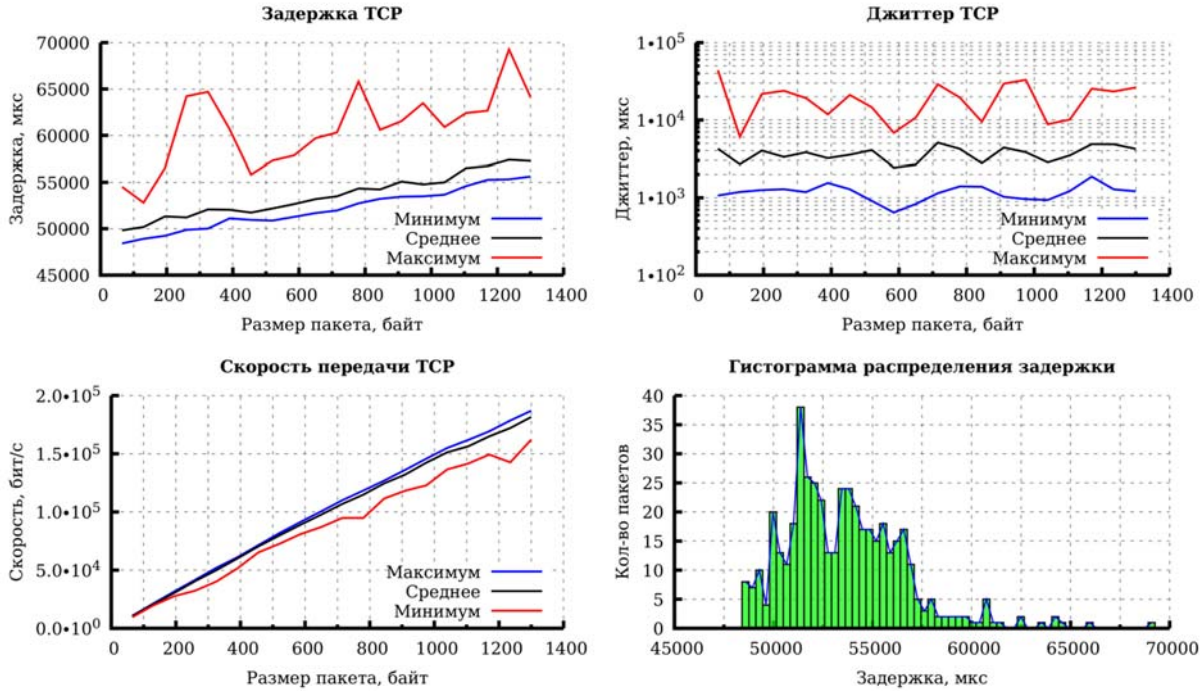


Рис. 3. Данные тестирования СпбГУТ (сервер) – Казахстан (клиент). IP 5.76.47.65

Проведенная работа доказала способность разработанных программных средств производить оценки различных сегментов операторских сетей передачи данных на соответствие классам QoS и параметрам SLA и подтвердила гипотезу об экспоненциальном характере распределения задержки пакетов в реальной сети.

Список используемых источников

1. Recommendation ITU-T Y.1541 (12/2011). Network performance objectives for IP-based services.

2. Recommendation ITU-T Y.1543 (06/2018). Measurements in Internet protocol networks for inter-domain performance assessment.

3. Владимиров С. А., Алексеев И. С., Воронов А. С. Реализация методики оценки операторских сетей на соответствие рекомендациям ITU-T Y.1540, Y.1541 // Информационные технологии и телекоммуникации. 2018. Том 6. № 3. С. 52–64.

4. Савич У. Программирование на C++ (4-ое издание) : учебное пособие. Addison-Wesley, 2004. 784 с.

Статья представлена заведующим кафедрой ССиПД СПбГУТ, доктором технических наук, профессором А. Е. Кучерявым.

УДК 004.056
ГРНТИ 81.93.29

РЕАЛИЗАЦИЯ И ОЦЕНКА МЕТОДОВ АДАПТАЦИИ И ПЕРЕОБУЧЕНИЯ СИСТЕМЫ АНАЛИЗА ИНФОРМАЦИОННЫХ ОБЪЕКТОВ В ВЕБ-КОНТЕНТЕ

А. А. Браницкий[1,2], П. А. Гладышева[2], В. А. Десницкий[1], И. В. Котенко[1]

[1]Санкт-Петербургский институт информатики и автоматизации Российской академии наук
[2]Санкт-Петербургский государственный университет телекоммуникаций им. проф. М. А. Бонч-Бруевича

Рассматриваются методы адаптации и переобучения системы анализа информационных объектов в сети Интернет. В качестве таких методов исследуются метод параллельного обучения классификаторов и методы сжатия признакового пространства (метод главных компонент, метод удаления слабо коррелирующих с меткой класса признаков). Данные методы направлены на снижение времени, затрачиваемого в процессе выполнения задач, связанных с адаптацией и переобучением классификаторов в рамках разработанной системы. При реализации системы анализа информационных объектов в веб-контенте используются язык программирования Python и библиотека машинного обучения scikit-learn.

методы адаптации и переобучения, веб-документы, информационные объекты, сеть Интернет.

Объем передаваемого по сети Интернет трафика увеличивается с каждым годом. Задача анализа веб-контента является важной, поскольку часть информации может носить вредоносный характер. Для сокращения времени адаптации и переобучения использовались следующие методы: методы сокращения размерности векторов признаков, метод параллельного обучения классификаторов. Среди методов сокращения размерности векторов признаков рассмотрим метод главных компонент [1] и метод исключения слабо коррелирующих с меткой класса признаков. Метод главных компонент позволяет понизить размерность векторов признаков с сохранением максимальной изменчивости (максимального значения дисперсии) в исходных данных. Это достигается за счет следующего преобразования над входным вектором $\boldsymbol{z}$:

$$F(\boldsymbol{z}) = (\boldsymbol{v_1}, \dots, \boldsymbol{v_{n'}})^T \cdot (\boldsymbol{z} - \overline{\boldsymbol{x}}),$$

где $\boldsymbol{v_1}, \dots, \boldsymbol{v_{n'}}$ – ортонормированные собственные векторы (отсортированные в порядке убывания соответствующих им собственных чисел) матрицы ковариации, составленной из элементов обучающей выборки, $\overline{\boldsymbol{x}}$ – математическое ожидание случайного вектора, представляющего собой обучающие

данные, $\boldsymbol{n'}$ – выбранная размерность нового пространства, $\boldsymbol{v_i^T} \cdot \boldsymbol{z}$ – i-ая главная компонента вектора $\boldsymbol{z}$.

Метод исключения слабо коррелирующих с меткой класса признаков подразумевает вычисление коэффициента корреляции для различных признаков $\boldsymbol{x}$ и метки класса $\boldsymbol{y}$ согласно следующей формуле:

$$r_{\boldsymbol{xy}} = \frac{\sum_{i=1}^{M}(x_i-\bar{x})\cdot(y_i-\bar{y})}{\sqrt{\sum_{i=1}^{M}(x_i-\bar{x})^2\cdot\sum_{i=1}^{M}(y_i-\bar{y})^2}}.$$

После вычисления таких коэффициентов из рассмотрения исключаются те признаки $\boldsymbol{x}$, для которых выполняется следующее условие $\left|r_{\boldsymbol{xy}}\right| < R$, где величина $R \leq 1$ задает порог линейной зависимости признака $\boldsymbol{x}$ и вектора $\boldsymbol{y}$, представляющего метку класса.

Для базовых классификаторов, которые представляют собой комбинацию бинарных классификаторов, построенных, к примеру, с использованием подходов один-ко-многим (*one-vs-all*) или один-к-одному (*one-vs-one*), может быть применен метод их параллельного обучения. Предположим, что базовый классификатор включает в свой состав P бинарных классификаторов `binary_classifiers[0:P-1]`. Тогда при наличии Q процессоров можно выполнить параллельное обучение P бинарных классификаторов в соответствии с ниже представленным псевдокодом:

```
parallel_for i = 0..Q-1 do
    l = i * div(P, Q) + min(i, mod(P, Q))
    r = l + div(P, Q) + (i < mod(P, Q) ? 1 : 0)
    train(binary_classifiers[l:r]) # [l, r)
od
```

При проведении экспериментальных исследований использовался набор данных, содержащий 74893 веб-документа, размеченных по 19 классам [2].

Было произведено вычисление следующих показателей классификации: точности (*precision*, PR), полноты (*recall*, RC), *f*-меры (*f-measure*, FM) и аккуратности (*accuracy*, AC) с учетом применения метода главных компонент для трех значений размерностей: $n = 300, 200, 100$. В таблице (см. ниже) приведены значения разностей показателей ΔPR, ΔRC, ΔFM, ΔAC, которые вычислялись для двух случаев: (1) при сравнении показателей коллектива классификаторов, построенного на основе метода взвешенного голосования, без применения метода главных компонент (вход – 402-мерный вектор) с показателями коллектива классификаторов с учетом применения метода главных компонент (размерность входного вектора варьировалась от 300 до 100), (2) при сравнении показателей коллектива классификаторов

с показателями наилучшего базового классификатора при идентичной размерности входного вектора.

ТАБЛИЦА. Сравнение показателей обоснованности коллектива классификаторов с показателями обоснованности наилучшего представителя среди базовых классификаторов при различных значениях размерности входного вектора на общем наборе данных

n	Случай 1				Случай 2			
	ΔPR(%)	ΔRC(%)	ΔFM(%)	ΔAC(%)	ΔPR(%)	ΔRC(%)	ΔFM(%)	ΔAC(%)
300	3,02	3,04	3,03	2,56	8,33	0,24	4,39	4,08
200	3,36	3,64	3,5	2,9	7,7	−0,4	3,74	4,8
100	5,41	5,6	5,51	4,6	4,68	−1,08	1,82	6,3

Из этой таблицы видно, что с уменьшением размерности качество классификации по всем показателям уменьшается (случай 1). Анализируя данные из правой части таблицы, можно сказать, что метод взвешенного голосования дает прирост показателей классификации по сравнению с применением отдельных базовых классификаторов, за исключением размерностей $n = 200$ и $n = 100$, когда наблюдается спад только показателя RC.

Уменьшение размерности векторов признаков при помощи второго метода осуществлялось посредством исключения тех компонент, которые доставляли наименьшую абсолютную величину корреляции с меткой класса (рис. 1).

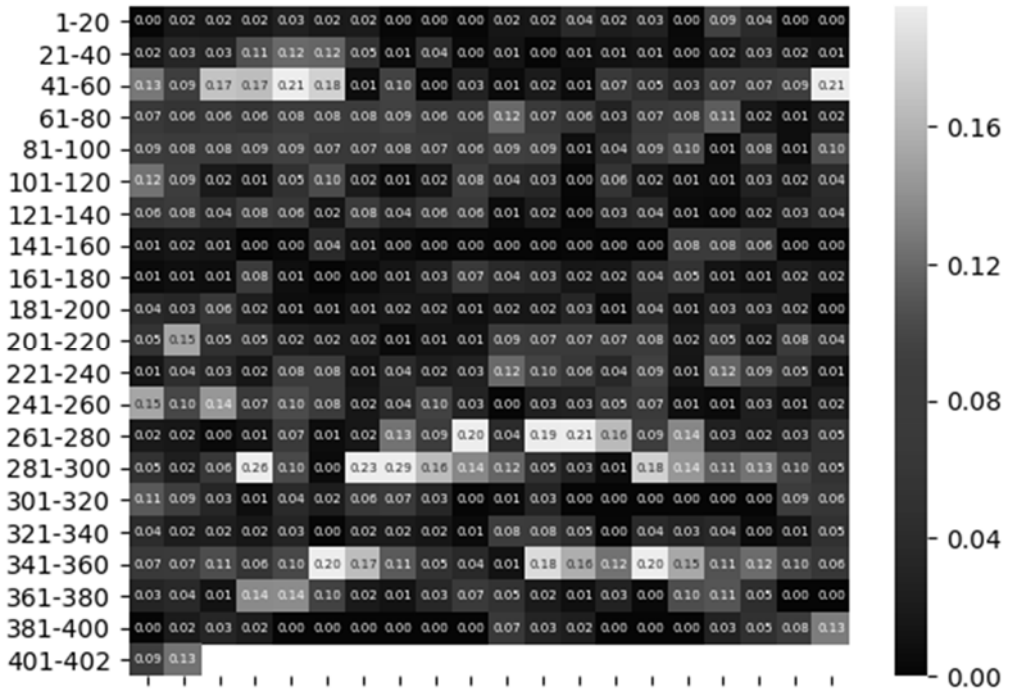


Рис. 1. Корреляция признаков с меткой класса

Из данного рисунка видно, что коэффициент корреляции отдельных компонентов вектора признаков с меткой класса является малым (не превосходит 0,29). Тем самым переход к чрезмерно низкоразмерному пространству признаков является нецелесообразным и может приводить к существенному снижению значений показателей обоснованности, вычисляемых на тестовой выборке.

На рис. 2 изображены временные показатели, затраченные в процессе настройки методов предобработки: min-max нормализации, метода главных компонент (МГК); базовых классификаторов: машины опорных векторов (МОВ), метода *K* ближайших соседей (МБС), наивного байесовского классификатора (НБК), линейной регрессии (ЛР) и дерева решений (ДР); композиции на основе метода взвешенного голосования (МВГ).

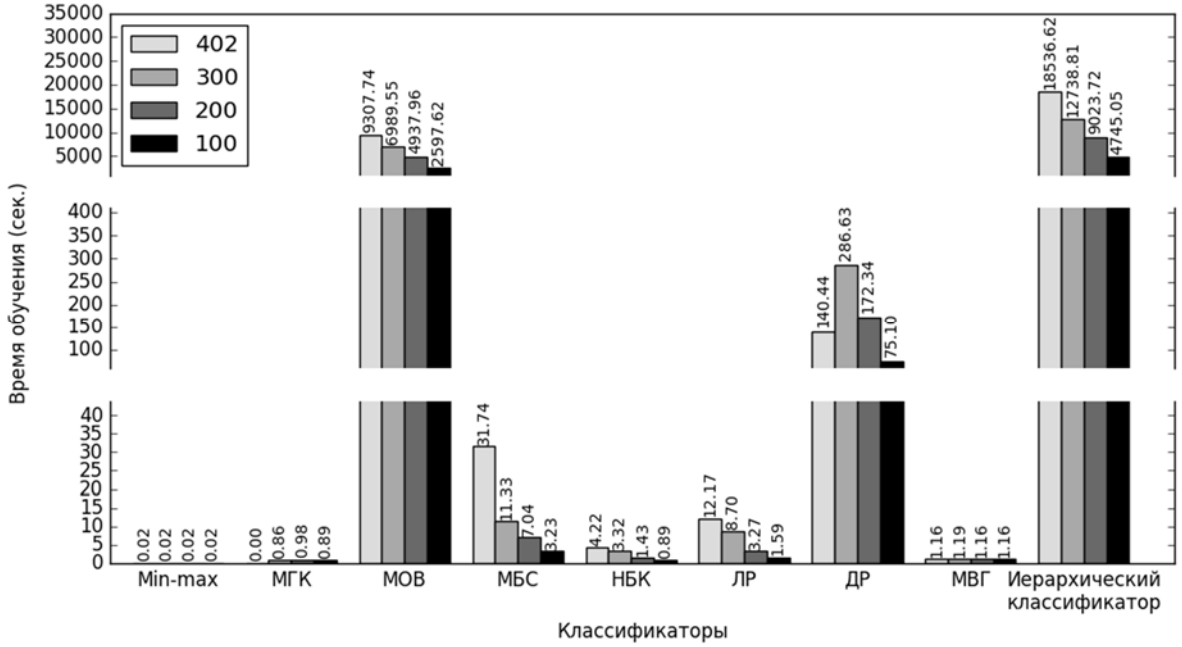


Рис. 2. Временные характеристики процесса обучения для каждого классификатора и для различных размерностей входного вектора

Наименьшие затраты по времени обучения принадлежат НБК, напротив, МОВ обладает наиболее длительным процессом настройки параметров. Отметим, что при сужении размерности пространства признаков наблюдается и уменьшение времени обучения иерархического классификатора. Снижение размерности пространства признаков с 402 до 300 компонентов позволило сократить время обучения иерархического классификатора почти в 1,5 раза, с 402 до 200 компонентов – более чем в 2 раза, а с 402 до 100 компонентов – почти в 4 раза.

Для уменьшения времени адаптации классификаторов выполнялось их параллельное обучение. Для 100-мерного вектора признаков время обу-

чения коллектива, состоящего из пяти базовых классификаторов, сократилось почти в пять раз при переходе от однопоточного режима обучения к восьмипоточному (рис. 3). Кроме того, для трех базовых классификаторов, а именно МОВ, МБС и ДР, наблюдается существенный выигрыш в скорости обучения этих классификаторов. Для оставшихся классификаторов, а именно НБК и ЛР, подобного эффекта не наблюдается.

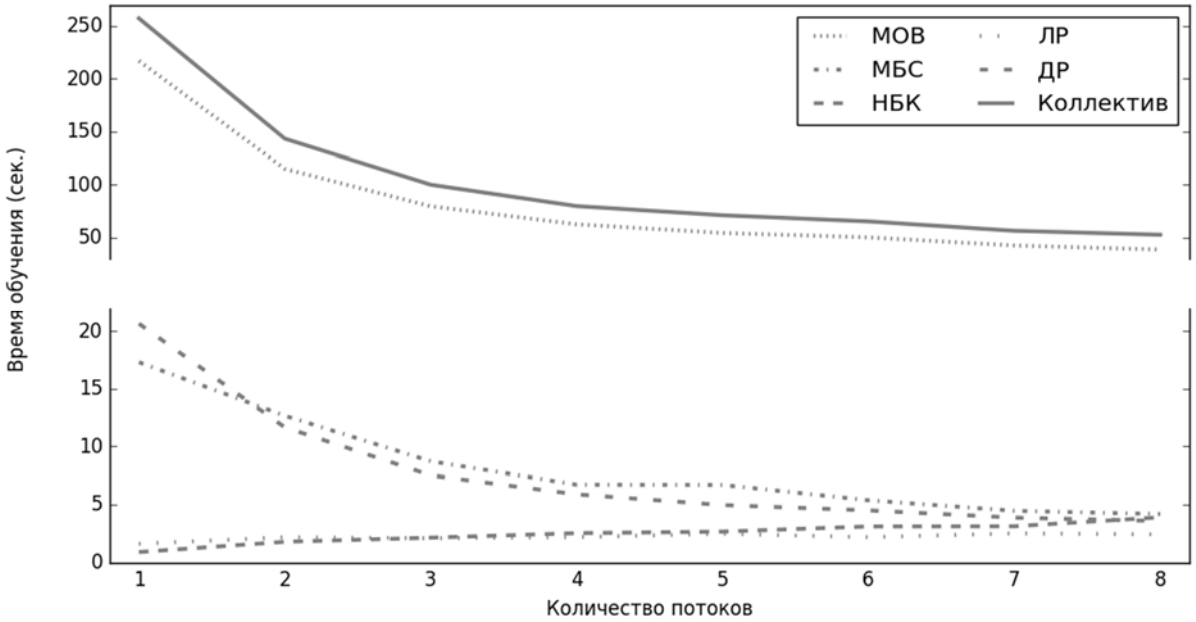


Рис. 3. Зависимость времени обучения базовых классификаторов и их коллектива от числа параллельных потоков (вход – 100-мерный вектор признаков)

В статье представлены методы адаптации и переобучения системы анализа информационных объектов в сети Интернет. Среди таких методов выделены метод главных компонент, метод исключения слабо коррелирующих с меткой класса признаков, а также метод параллельного обучения базовых классификаторов. Выполнена экспериментальная оценка этих методов.

Работа выполнена при финансовой поддержке проекта РНФ № 18-11-00302 в СПИИРАН.

Список используемых источников

1. Jolliffe I. T. Principal component analysis // Springer Series in Statistics. 1986. 271 p.
2. Браницкий А. А., Саенко И. Б. Методика многоаспектной оценки и категоризации вредоносных информационных объектов в сети Интернет // Труды учебных заведений связи. 2019. Т. 5. № 3. С. 58–65.

УДК 004.056
ГРНТИ 81.93.29

МЕТОДИКА ОПРЕДЕЛЕНИЯ ПОДВЕРЖЕННОСТИ ПОЛЬЗОВАТЕЛЕЙ СОЦИАЛЬНЫХ СЕТЕЙ ДЕСТРУКТИВНОСТИ НА ОСНОВЕ НЕЙРОННЫХ СЕТЕЙ

А. А. Браницкий[1,2], Е. В. Дойникова[1,2], И. В. Котенко[1,2]

[1]Санкт-Петербургский институт информатики и автоматизации Российской академии наук
[2]Санкт-Петербургский государственный университет телекоммуникаций им. проф. М. А. Бонч-Бруевича

В настоящее время популярным средством общения молодежи являются социальные сети. В то же время они могут использоваться для распространения информации, оказывающей деструктивное влияние на пользователей. Для выявления и предотвращения таких воздействий предлагается методика, предполагающая обнаружение признаков деструктивных воздействий в информации, предоставляемой пользователями в социальной сети. В ее основе лежит предположение, что между этой информацией и подверженностью пользователей деструктивности существует зависимость. Для выявления этой зависимости предлагается использовать аппарат искусственных нейронных сетей. В рамках исследования были проведены эксперименты, подтвердившие наличие зависимости между информацией, предоставляемой пользователями в социальных сетях, и психологическим характеристиками личности. В дальнейшем планируется определить набор признаков и провести эксперименты по выявлению деструктивных воздействий в динамике.

деструктивное воздействие, социальная сеть, тест Аммона, нейронная сеть, прогнозирование.

Социальные сети являются популярным средством обмена информацией. В то же время, они могут использоваться для распространения деструктивных, разрушительных воздействий с самыми разными целями. Для сохранения психологического здоровья общества в целом и молодежи как активных пользователей социальных сетей в частности, важно выявлять и противодействовать таким воздействиям. Ввиду того, что определение полного комплекса воздействий, оказываемых на отдельного пользователя, практически невозможно, предлагается определять наличие деструктивного воздействия на пользователя по изменениям его поведения в социальной сети. А именно, по той информации, которую пользователь размещает в социальной сети (переписка с друзьями, сведения о личных интересах, фотографии).

Для определения подверженности индивидуумов деструктивным воздействиям используются специализированные тесты. Одним из наиболее распространенных является тест Аммона. В зависимости от ответов индивидуума на 220 вопросов теста, он отображает деструктивные, дефицитарные и конструктивные проявления по шести личностным функциям (агрессия, тревога, внешнее Я-отграничение, внутреннее Я-отграничение, нарциссизм и сексуальность) и позволяет отследить эти проявления в динамике.

В рамках данного исследования предлагается методика прогнозирования результатов данного теста с помощью информации, предоставляемой пользователями в социальной сети, и автоматизации таким образом процесса выявления деструктивных воздействий в социальных сетях. Предлагаемая методика включает следующие этапы:

1) ручное тестирование пользователей социальных сетей с использованием теста Аммона для определения их подверженности деструктивным воздействиям;

2) использование информации профилей социальных сетей для автоматического прогнозирования результатов теста Аммона с использованием нейронных сетей;

3) регулярный сбор данных и прогнозирование результатов теста Аммона для пользователей с целью выявления изменений в их состоянии и обнаружения деструктивных воздействий.

В свою очередь, второй этап методики включает три шага:

1) сбор данных из профилей пользователей социальной сети;

2) анализ собранных данных и формирование вектора признаков для обучения нейронной сети;

3) прогнозирование результатов теста Аммона по собранным данным при помощи обученных нейронных сетей. Для прогнозирования были выбраны многослойные нейронные сети ввиду их способности к аппроксимации разделяющих гиперплоскостей между сложными линейно неразделимыми множествами [1, 2, 3].

Для экспериментов было проведено онлайн-тестирование 460 пользователей социальной сети по тесту Аммона. Для обучения нейронной сети были собраны и проанализированы данные профилей пользователей. В результате анализа были выделены три группы признаков для обучения нейронной сети:

1) численные параметры (в том числе, месяц рождения, количество подписчиков, друзей и фотографий и др.);

2) последовательность слов (в том числе, результат применения word2vec [4] между пятью наиболее употребительными словами, характерными для постов каждого класса, и тремя наиболее употребительными словами в постах анализируемого профиля, и др.);

3) параметры, вычисляемые на уровне бинарных потоков данных (например, результат классификации изображения при помощи нейронной сети imagenet [5]).

Для проведения экспериментов исходный набор признаковых данных был разбит на 10 частей, 9 из которых использовалось для обучения, и 1 – в качестве тестовой (для вычисления точности результатов прогнозирования), половина элементов которой формировала валидационное множество (для вычисления среднеквадратичной ошибки). Эксперименты проводились только для деструктивных проявлений. Для экспериментов были выбраны следующие нейросетевые классификаторы: многослойная нейронная сеть (МНС) с тремя скрытыми слоями нейронов, машина опорных векторов с радиально-базисным ядром, линейная регрессия, и сверточная нейронная сеть (СНС). Для обучения первых трех классификаторов использовались вышеперечисленные признаки, для обучения СНС использовались посты на стенах профилей пользователей в социальной сети. Наибольшее значение точности прогнозирования (61,34 %), полученное посредством усреднения по шести психологическим шкалам деструктивности, показала МНС, обученная с применением 101-мерного вектора признаков (включал три вышеперечисленные группы признаков и дополнительный признак, представляющий собой выходное значение СНС, предварительно обученной на постах).

Результаты экспериментов для тестовой группы указывают на наличие связи между результатами теста Аммона и информацией, выкладываемой пользователями в социальных сетях, что в свою очередь указывает на возможность применения предложенной методики для выявления деструктивных воздействий. При этом необходимо отметить, что целью исследования не является автоматическое определение психологических характеристик личности, а именно выявление деструктивных воздействий. Дальнейшая работа будет посвящена как определению третьего этапа предложенной методики, связанного с выявлением изменений в социальных сетях, указывающих на наличие деструктивных воздействий, так и анализу выявленных изменений для улучшения алгоритмов, используемых при прогнозировании результатов теста на втором этапе работы методики.

Работа выполнена при финансовой поддержке РФФИ (проект 18-29-22034 мк).

Список используемых источников

1. Cybenko G. Approximation by superpositions of a sigmoidal function // Mathematics of Control, Signals, and Systems (MCSS). 1989. Vol. 2, N 4. P. 303–314.

2. Funahashi K. I. On the approximate realization of continuous mappings by neural networks // Neural networks. 1989. Vol. 2, N 3. P. 183–192.

3. Hornik K., Stinchcombe M. White H. Multilayer feedforward networks are universal approximators // Neural networks. 1989. Vol. 2, N 5. P. 359–366.

4. Mikolov T. et al. Efficient estimation of word representations in vector space // arXiv preprint arXiv:1301.3781. 2013.

5. Krizhevsky A., Sutskever I., Hinton G.E. Imagenet classification with deep convolutional neural networks // Advances in neural information processing systems. 2012. P. 1097–1105.

УДК 004.056
ГРНТИ 81.93.29

ИССЛЕДОВАНИЕ МЕТОДА ОБНАРУЖЕНИЯ УЯЗВИМОСТЕЙ В ПРИЛОЖЕНИЯХ, ИСПОЛЬЗУЮЩИХ КОДЕК JBIG2

А. А. Браницкий[1,2], Н. Н. Ле[2]

[1]Санкт-Петербургский институт информатики и автоматизации Российской академии наук
[2]Санкт-Петербургский государственный университет телекоммуникаций им. проф. М. А. Бонч-Бруевича

Кодек JBIG2 используется в приложениях чтения электронных PDF-документов. Широкая распространенность и популярность документов в таком формате ставит вопрос обеспечения безопасности соответствующих приложений особо острым. В процессе исследования применяется метод инспектирования кода для анализа уязвимостей. Таким образом, посредством анализа графа потока управления программы и наличия взаимосвязи между объектами становится возможным выявлять ошибки и эксплуатировать их.

кодек JBIG2, обнаружение уязвимостей, PDF-документы, инспектирование кода.

JBIG2 – это международный стандарт ISO/IEC для сжатия двухуровневых изображений с потерями и без потерь [1]. Типичный кодер JBIG2 разбивает входное двухуровневое изображение на несколько областей и кодирует каждую из областей в отдельности, используя другой метод кодирования. [2]. Декодер JBIG2 предоставляет возможность указать, как перекрывающиеся области рекомбинируются для формирования конечного изображения страницы. На рис. 1 (см. ниже) показаны основные компоненты декодера и соответствующие буферы [3]. На этом рисунке процедуры декодирования выделены жирными линиями, а компоненты памяти выделены нежирными линиями. Также жирные стрелки указывают, что одна процедура декодирования вызывает другую процедуру декодирования; например, процедура декодирования словаря символов вызывает

процедуру декодирования общей области для декодирования битовых карт для символов, которые она определяет. Жирные стрелки указывают поток данных: процедура декодирования текстовой области считывает символы из памяти символов и выводит их в буфер страниц или вспомогательный буфер. Хотя это не показано на рис. 1, поток кодированных данных переходит к процедурам декодирования, а блок, помеченный как «Страничные и вспомогательные буферы», создает окончательные декодированные изображения страницы [3].

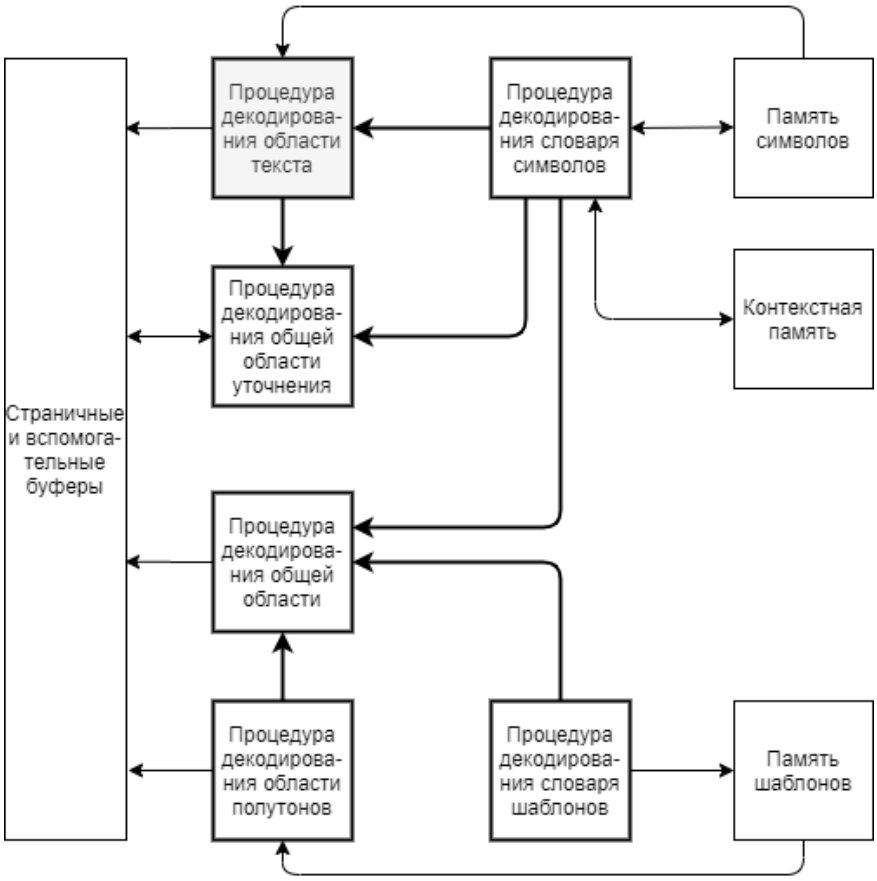


Рис. 1. Структурная схема основных компонентов декодера

По диаграмме на рис. 1, когда проводится поиск ошибки в основных компонентах декодера (процедурах декодирования), нужно определить в этих компонентах объекты, функции, и протоколы, которые взаимодействуют между компонентами. При рассмотрении компонентов очень важно знать типы ошибок, которые часто возникают в определенных компонентах. Кодер JBIG2 используется в одном приложении; обычно возможны следующие ошибки:

– Целочисленное переполнение. JBIG2 использует много типов алгоритмов арифметического декодирования и выполняет много операций с целыми числами. Поэтому стоит сосредоточиться на компонентах, которые имеют вышеуказанные характеристики, чтобы обнаружить эти ошибки.

– Уязвимости в куче (*heap*). Временные данные, такие как словарь символов и словарь шаблонов, хранятся в динамической памяти. Следует сосредоточиться на объектах, которые хранят временные данные, проанализировать отношения между объектами и жизненным циклом объектов, если ставится цель обнаружения этих ошибок.

Анализ уязвимости CVE-2018-16076

В коде синтаксического анализатора JBIG2 в Google Chrome присутствует уязвимость, позволяющая использовать данные за пределами допустимой области динамической памяти (*out-of-bound read*). Специально созданный PDF-документ (*PortableDocumentFormat*) может вызвать чтение за пределами допустимого диапазона, что может привести к утечке информации, которая может быть использована в качестве эксплойта. Злоумышленник должен заставить пользователя посетить вредоносный сайт, чтобы вызвать уязвимость.

Переполнение буфера динамической памяти присутствует в коде, ответственном за декодирование потока изображения JBIG2. Буфер, на который указывает lineSrc, косвенно зависит от значений *sw* (ширина битовой карты сегмента региона) и *sh* (высота битовой карты сегмента региона), поэтому он находится под контролем атакующего. Ошибка чтения из-за пределов памяти заключается в том, что можно пропустить проверку в [*] и увеличить указатель lineSrc в [**] за пределы выделенного буфера, таким образом предоставляя доступ к смежной памяти. Переменная rtSrc.top также увеличивается на единицу при каждом вызове ComposeToOpt2WithRect, поэтому, если проверка в [*] выполнилась, lineSrc может указывать за пределы области памяти.

```
bool CJBig2_Image::ComposeToOpt2WithRect(CJBig2_Image* pDst,
                                         int32_t x,
                                         int32_t y,
                                         JBig2ComposeOp op,
const FX_RECT&rtSrc) {
  ...
  int32_t sw = rtSrc.Width();
  int32_t sh = rtSrc.Height();
  int32_t ys0 = y <0 ? -y : 0;
  int32_t ys1 = y + sh>pDst->m_nHeight ? pDst->m_nHeight - y : sh;
  int32_t xs0 = x <0 ? -x : 0;
  int32_t xs1 = x + sw>pDst->m_nWidth ? pDst->m_nWidth - x : sw;
if ((ys0 >= ys1) || (xs0 >= xs1)) {   [*]
   return 0; }
  uint8_t* lineSrc = data() + (rtSrc.top + ys0) * m_nStride + (((xs0 + rtSrc.left) >> 5) <<
2);   [**]
```

Эта ошибка приводит к сбою в строке 747, когда осуществляется доступ к памяти за пределами области памяти:

```
for (int32_t yy = yd0; yy < yd1; yy++) {
  uint32_t tmp1 = JBIG2_GETDWORD(lineSrc) >> shift;
  uint32_t tmp2 = JBIG2_GETDWORD(lineDst);
...
```

Эксплуатация

Для реализации уязвимости требуется объект PDF, описывающий детали изображения JBIG2 с конкретными деталями:

```
5 0 obj
<<
/Width 1
/ColorSpace /DeviceGray
/Height 2
/Filter /JBIG2Decode
/Subtype /Image
/Length 17
/Type /XObject
>>
stream
...
endstream
endobj
```

В вышеуказанном объекте представленные ширина и высота имеют значение. Ниже показано минимальное содержимое потока, необходимое для запуска этой уязвимости:

```
00 00 00 00 # номер региона
30          # тип региона
00
00
00 00 00 00 #длина данных региона
00 00 00 00 # номер региона
26          # тип региона (38 – непосредственный общий регион)
00
00
00 00 00 00 # длина данных (фиктивная, игнорируется)
00 00 00 01 # ширина растрового изображения сегмента региона
00 00 00 01 # высота растрового изображения сегмента региона
00 00 00 00 # сегмент региона x местоположение
00 00 00 00 # регион сегмент y местоположение
00          # оператор внешней комбинации (ИЛИ в этом случае)
```

```
02        # общие флаги сегмента региона (задает GBTEMPLATE для арифметического кодирования на основе шаблонов, в этом случае GBTEMPLATE равен 1)
00        # GBATX
00        # GBATY
00 00 00 00 00 00 00 00 00 00 00 00 # требуется заполнение
00 00 00 00 00 00 00 00 00 00 00 00
00 00 00 00 00 00 00 00 00 00 00 00
```

С помощью инструмента AddressSanitizer был выполнен анализ нарушений кода эксплойта, и получена информация об ошибке.

```
SUMMARY: AddressSanitizer: heap-buffer-overflowJBig2_Image.cpp:747 inCJBig2_Image::ComposeToOpt2WithRect(CJBig2_Image*, int, int, JBig2ComposeOp, FX_RECTconst&)
Shadowbytesaroundthebuggyaddress:
  0x1c04000002e0: fafafdfafafafdfdfafafdfafafafdfd
  0x1c04000002f0: fafafdfafafa 00 fafafafdfdfafafdfd
  0x1c0400000300: fafa 00 00 fafa 00 00 fafa 00 00 fafafdfa
  0x1c0400000310: fafafdfdfafa 04 fafafa 04 fafafa 00 00
  0x1c0400000320: fafa 00 00 fafafdfdfafa 00 00 fafa 04 fa
=>0x1c0400000330: fafa 00 fafafa 00 fafafa 00[fa]fafafafa
  0x1c0400000340: fafafafafafafafafafafafafafafafa
  0x1c0400000350: fafafafafafafafafafafafafafafafa
  0x1c0400000360: fafafafafafafafafafafafafafafafa
  0x1c0400000370: fafafafafafafafafafafafafafafafa
  0x1c0400000380: fafafafafafafafafafafafafafafafa
```

Выполнено исследование метода обнаружения уязвимостей в приложениях, использующих алгоритм декодирования JBIG2. Проведён анализ уязвимостей в Google Chrome, и продемонстрирована возможность получения информации об ошибке с помощью инструмента AddressSanitizer.

Работа выполнена при финансовой поддержке Гранта РФФИ № 18-29-22034 мк.

Список используемых источников

1. Howard P. G. et al. The emerging JBIG2 standard //IEEE Transactions on Circuits and Systems for Video Technology. 1998. T. 8. N. 7. PP. 838–848.

2. Ono F. et al. JBIG2-the ultimate bi-level image coding standard // Proceedings 2000 International Conference on Image Processing (Cat. No. 00CH37101). IEEE, 2000. T. 1. PP. 140–143.

3. JBIG2 Final Draft Int. Std., 14492:2019. ISO/IEC.

УДК 004.051
ГРНТИ 49.46.29

LI-FI. БЕСПРОВОДНАЯ ОПТИЧЕСКАЯ ТЕХНОЛОГИЯ ПЕРЕДАЧИ ДАННЫХ НА БАЗЕ СВЕТОДИОДОВ

А. В. Брыдченко, М. Д. Гевель, М. А. Михайлова, Н. А. Тельнов

Санкт-Петербургский государственный университет телекоммуникаций им. проф. М. А. Бонч-Бруевича

Технология Li-Fi является инновационной и пока только набирает популярность. Требуется раскрытие её потенциалов в различных сферах применения для всемирного использования. Преимущества Li-Fi представляют возможность разгрузки, наиболее применяемой на данный момент, технологии Wi-Fi. Изучение принципа действия, технических характеристик и способов применения, а также оценка мирового рынка на 2020 год, поможет оценить актуальность системы передачи данных на основе светодиодов.

технология Li-Fi, передача данных, светодиодное освещение, беспроводные сети передачи данных, передача данных в видимом спектре, светодиоды, светодиодные лампы, фотоприемник.

В 2011 году профессор Харальд Хаас, заведующий кафедрой мобильной связи в Эдинбургском университете, представил свой доклад «Беспроводные данные с каждой лампочки» на конференции TED Global [1] о новой технологии, которая показала огромный потенциал в решении многих проблем, связанных с Wi-Fi. Эта технология беспроводной оптической передачи данных имеет два названия – VLC технология (*Visible Light Communication* – коммуникационная линия в видимом свете) и Li-Fi (*Light Fidelity* – свет и точность). Последнее огласил сам Харальд Хаас. Благодаря описанию технологии словами «беспроводная» «оптическая» становится понятно, что происходит излучение света бесконтактным путем. Также перевод аббревиатуры VLC указывает на процесс соединения элементов системы определенным образом за счет видимого света. Действительно, основной принцип работы заключается в том, что светодиод (передатчик), расположенный на определенном расстоянии излучает луч света в видимой области (рис., см. ниже).

Данные, необходимые для передачи, кодируются изменением яркости. Яркость света меняется за счёт включения и выключения светодиода с огромной скоростью. Происходит сложение потока импульсов в массив бинарных данных. Причём человек видит сплошной поток света, так как глаз не воспринимает более 100 мерцаний в секунду [2]. Для приёма зако-

дированной информации необходим фотоприемник. Ярким примером, о котором Хаас заявил в 2015 году на TED Global, является солнечная батарея. Она поглощает свет и преобразует его в электрический сигнал. Однако в случае Li-Fi приходит массив импульсов света, а не постоянный поток. Следовательно, на приёме мы уже имеем энергию, соответствующую передаче данных.

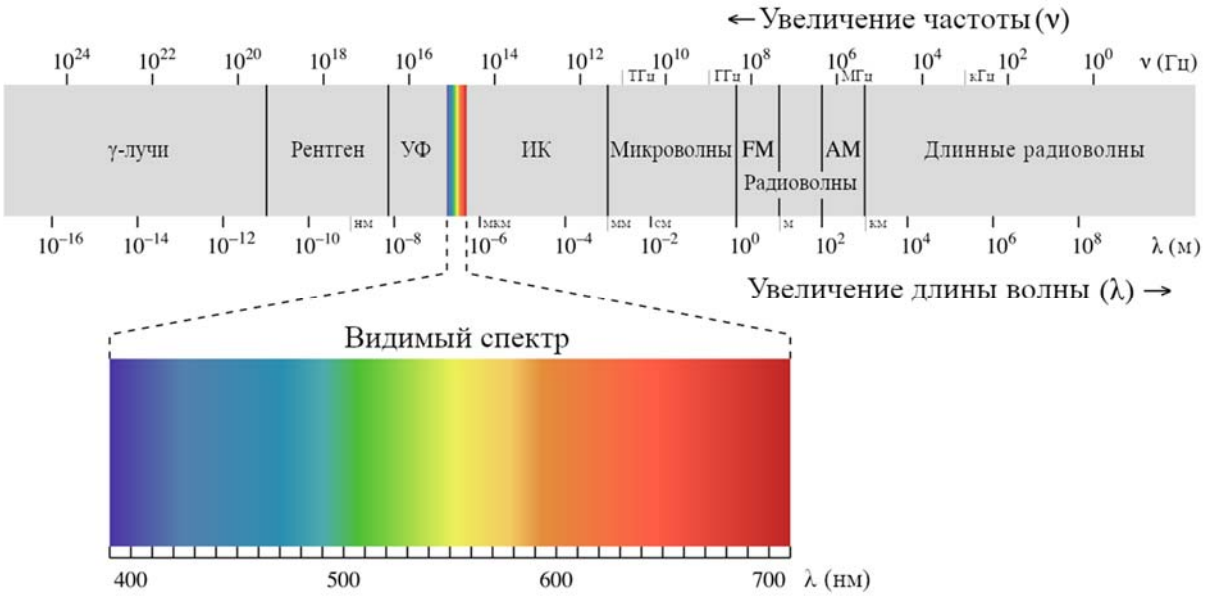


Рис. Спектр электромагнитных волн

Li-Fi использует свободное пространство как и другие действующие беспроводные технологии, но важным преимуществом является способ передачи Wi-Fi, основанный на преобразовании электромагнитных волн (ЭМВ), на данный момент, испытывает трудности с использованием частот без наложения друг на друга. При всемирном использовании спектр радиоволн настолько заполнен, что постоянно учёные ищут способы разгрузки для эффективного использования [3].

Li-Fi – прорыв в решении ранее упомянутой проблемы. Видимый спектр никак не влияет на радиоволны и расположен в другом диапазоне (400–800 ТГц) (рис.). Согласно теореме Котельникова, максимальная передача данных возможна на частоте Найквиста, равной половине частоты дискретизации. Частота света около 500 ТГц, когда частота радиоволн составляет порядка 5 ГГц, что примерно в 10000 раз дает преимущество технологии Li-Fi.

ЭМВ также открыты к внешним воздействиям и перехвату сигналов. Li-Fi гарантирует безопасность и конфиденциальность, поскольку свет не проходит через стены. Причём разведывательные лица или группы не могут получить информацию без непосредственного присутствия в помещении распространения сигнала.

Однако есть характерные особенности технологии. Во-первых, из-за того, что свет не распространяется через толстые перекрытия (стены, окна, двери), существуют ограничения по площади помещения. Li-Fi требует внедрять сложную систему для взаимодействия помещений, например, отделений офиса. Зона приёма может быть, как в прямой видимости, так и в зоне отраженного сигнала. Во-вторых, помехи, создаваемые другими способами освещения, могут влиять в худшую сторону на передачу данных. Солнечный свет является дестабилизирующим фактором, отсюда следует невозможность реализации на улице.

Особенности Li-Fi позволяют осуществить передачу данных во многих местах, где реализация с помощью радиоволн невозможна или нежелательна. Такими примерами могут послужить: салоны самолетов, вертолетов, беспилотных летательных аппаратов, космических летательных аппаратов, вагоны поездов, подводные лодки, помещения скрытого разведывательного управления, склады боеприпасов, помещения в учреждениях здравоохранения, атомные электростанции и заводы, требуемые отсутствие электромагнитных помех. В местах массового скопления людей (вокзалы, аэропорты) скорость передачи данных падает в зависимости от количества пользователей. Li-Fi в свою очередь на это не будет реагировать. Применение Li-Fi в системе IoT (*Internet of things* – интернет вещей) сделает функциональные возможности наиболее стабильными и бесперебойными.

В 2012 году Харальд Хаас вместе с доктором Мостафой Афгани основали компанию PureLiFi, которая реализует до сих пор новаторские исследования в области коммуникаций Li-Fi профессоров Эдинбургского университета и других ученых. За это время компания представила ряд мировых новинок для Li-Fi: в сентябре 2013 года первый коммерческий продукт Li-Fi (*Li-1st*), в декабре 2014 года первый мобильный продукт Li-Fi (*Li-Flame*), в марте 2016 года первая система из компактного модуля и передатчика Li-Fi (*LiFi-X*), в октябре 2017 года система LiFi-XC. На MWC (*Mobile World Congress* – Всемирный мобильный конгресс) 2014 года в Барселоне была представлена Li-1st. Причем недавно, в декабре 2019 года, они представили скорость на MWC с помощью Gigabit Li-Fi, и тем самым снова подтвердили актуальность.

В сентябре 2016 года французская компания Lucibel, новатор в области светодиодных технологий, выпустила на рынок первое Li-Fi-устройство. Скорость, которую они гарантируют на настоящий момент времени, составляет 54 Мбит/с. Причем площадь покрытия составляет 16 метров квадратных при высоте установки лампы на высоте 2,5 метра. Услугой «LIFI BY LUCIBEL» уже пользуются более 100 клиентов.

Компания Oledcomm в 2013 году проводила эксперименты в применении Li-Fi в поездах TGV, французской сети скоростных электропоездов,

управляемых железнодорожным оператором SNCF. А также в офисах международной промышленной группы Thales Group, выпускающей информационные системы для авиакосмического, военного и морского применения. Осуществила первый совместный проект «Smartcity» (умный город) с EDF (*Electricite de France* – крупнейшая государственная энергогенерирующая компания Франции). Впервые выпустила Li-Fi на самолете AirFrance. Сейчас линейка продуктов LiFiMAX Discovery Kit включает в себя все необходимые устройства для технологии Li-Fi.

На 35-й ежегодной международной конференции IEEE общества инженеров в области медицины и биологии (EMBC), проходившей 3–7 июля 2013 года в Японии, было заявлено успешное применение технологии Li-Fi в области медицины и биологии [4].

Интерес компаний на мировом рынке в коммерческой реализации увеличивается постепенно. Количество потребителей на данный момент не соответствует предполагаемой статистике по причине неосведомленности. Однако, чем выше частота применения светодиодных светильников, тем больше появляется возможностей для распространения технологии Li-Fi. Исследования Grand View Research прогнозируют рост рынка технологии к 2024 году до 100 миллиардов долларов.

Список используемых источников

1. Хаас Х. Беспроводная информация из каждой лампочки [Электронный ресурс] // Беспроводная информация из каждой лампочки : материалы науч. конф., Эдинбург, Шотландия 11-15 июля 2011 г. URL: http://www.ted.com/talks/harald_haas_wireless_data_from_every_light_bulb.htm (дата обращения 03.03.2020).

2. Гузенкова Е. А., Петрусь И. П. Аспекты практического использования беспроводной оптической технологии передачи данных [Электронный ресурс] // Связь компьютеров. Сети ЭВМ. Вычислительные сети : электрон. научн. журн. «Науковедение». 2014. № 2. URL: https://naukovedenie.ru/PDF/85TVN214.pdf (дата обращения 07.03.2020).

3. IEEE 802.11. Стандарт беспроводной локальной сети. [Электронный ресурс]. URL: http://standards.ieee.org/about/get/802/802.11.html (дата обращения: 08.03.2020).

4. Йи Йонг Тан, Санг-Джун Юнг, Ван-Юнг Чунг. Передача биометрического сигнала в режиме реального времени смешанного сигнала ЭКГ и информации о пациенте с использованием связи в видимом свете [Электронный ресурс] // Материалы науч. конф., Осака, Япония 3–7 июля 2013 г. URL: https://ieeexplore.ieee.org/document/6610619?arnumber=6610619 (дата обращения 04.03.2020).

УДК 004.042
ГРНТИ 49.37.29

РАСЧЕТ ЗАДЕРЖКИ ДЛЯ СЕТИ ТУМАНА И ОБЛАКА В СЕТЯХ IoT

Н. В. Будылдина, Е. В. Юрченко

Уральский технический институт связи и информатики

Туманные вычисления становятся перспективной парадигмой для выполнения распределенных вычислений с малой задержкой путем использования вычислительных ресурсов устройств конечных пользователей и облачных серверов. Тем не менее, динамическое и распределенное формирование локальных сетей тумана является очень сложной задачей из-за периодического появления соседних узлов тумана. Следовательно, узел тумана должен правильно выбрать набор соседних узлов и разумно перенести свои вычислительные задачи, чтобы добиться передачи и вычисления с малой задержкой.

туманные вычисления, пограничные вычисления, задержка.

В настоящее время для удовлетворения требований скорости вычисления задач при работе устройств IoT, обычные решения, применяемые в удаленных облачных вычислениях, могут не подойти из-за высокой сквозной задержки передачи в облаке [1]. Следовательно, чтобы уменьшить задержку передачи, локальная близость устройств IoT может быть использована для распределенной выгрузки вычислительных задач. Такая локальная вычислительная нагрузка приводит к появлению парадигмы туманных вычислений [2]. Туманные вычисления, также известные как граничные вычисления, которые позволяют преодолеть ограничения централизованных облачных вычислений, распределением вычислений с малой задержкой на границе сети для поддержки различных приложений беспроводной связи и IoT [3]. Кроме того, чтобы эффективно использовать объединение вычислительных ресурсов туманной сети, необходимы схемы управления ресурсами для архитектуры гибридной туманно-облачной сети [3].

Рассмотрим сеть тумана, состоящую из сенсорного слоя, туманного слоя и облачного слоя, как показано на рис. (см. ниже).

В этой системе сенсорный слой включает интеллектуальные и IoT-датчики небольшого размера с ограниченными вычислительными возможностями. Следовательно, когда датчики генерируют вычислительные задачи, они передаются на уровни тумана для удаленных распределенных вычислений. Точно так же облачные задачи могут быть выгружены в слой тумана. Слой тумана относится к набору IoT-устройств (также называемых узлами

тумана), которые могут выполнять задачи по туманным вычислениям, такие как хранение данных и вычислительные задачи.

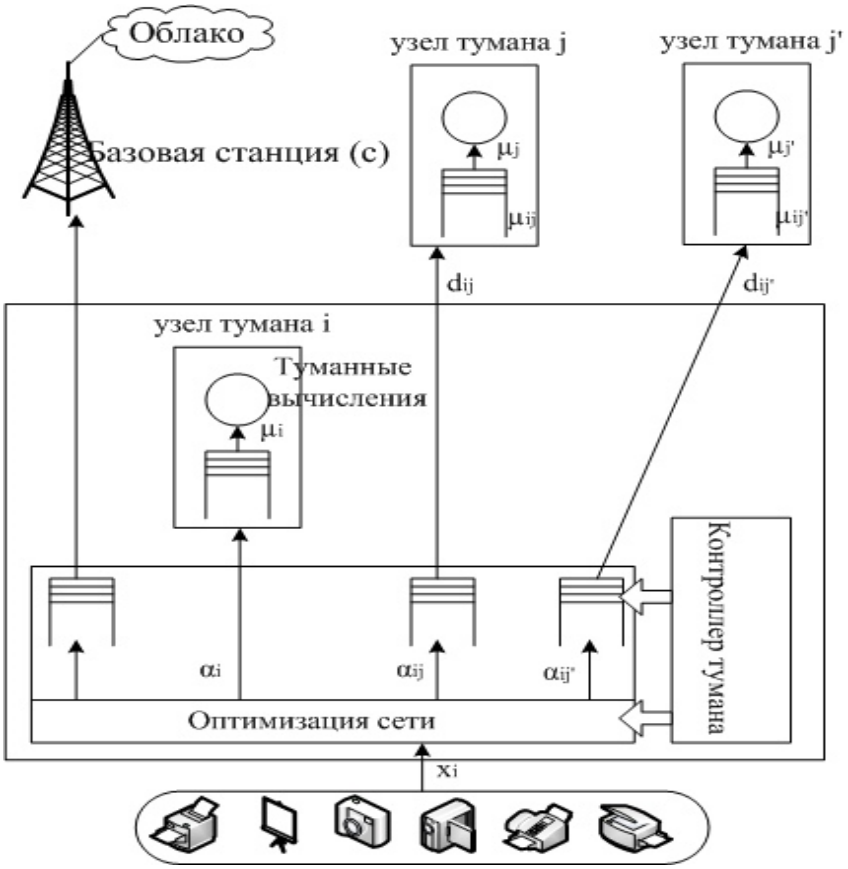


Рис. Системная модель сетевой архитектуры тумана и облака

Датчики различного типа отправляют свои данные с учетом выполняемых задач по туманным вычислениям в определенный узел i тумана, и скорость поступления данных в этот узел составляет x_i пакетов в секунду, где пакет задач по туманным вычислениям имеет размер K битов. Туманный узел i выполняет функции сбора, хранения, управления и обработки, данных выполняемых задач по туманным вычислениям с сенсорного уровня [1]. В рассматриваемой архитектуре для эффективных вычислений узел тумана i должен взаимодействовать с другими соседними узлами тумана и облачным центром обработки данных. Сеть имеет множество N из N узлов тумана, отличных от узла тумана i. Для узла тумана i рассматривается случай туманных вычислений, в котором узел тумана i строит сеть с подмножеством $J \subset N$ из J соседних узлов тумана. Поскольку облако обычно находится в удаленном месте, узел тумана i получает доступ к облаку через беспроводные линии связи, используя сотовую базовую станцию c.

Как только начальный узел тумана i получает задачи по туманным вычислениям, которые поступают со скоростью x_i пакетов в секунду, он назна-

чает долю x_i пакетов в секунду другим узлам. Затем каждый узел в рассматриваемой сети облаков тумана будет локально вычислять назначенную долю x_i пакетов в секунду. Доля задач по туманным вычислениям, локально вычисленных узлом тумана i, равна $\lambda_i\ (\alpha_i) = \alpha_i x_i$. Тогда скорость поступления задач по туманным вычислениям, выгруженных из узла тумана i в узел тумана $j \in J$, равна $\lambda_{ij}\ (\alpha_{ij}) = \alpha_{ij} x_i$. Следовательно, скорость поступления задач по туманным вычислениям, обработанных в слое тумана, равна $(\alpha_i + \sum_{j \in J} \alpha_{ij})\, x_i$. Оставшиеся задачи по туманным вычислениям $\lambda_c\ (\alpha_c) = \alpha_c x_i$ будут выгружены в облако. Когда туманный узел i принимает решение о распределении всех входных задач по туманным вычислениям x_i пакетов в секунду, переменные распределения задач по туманным вычислениям представляются в виде вектора $\alpha = [\alpha_i, \alpha_c, \alpha_{i1}, \dots, \alpha_{ij}, \dots, \alpha_{iJ}]$ с $\sum_{j \in J} \alpha_{ij} + \alpha_i + \alpha_c = 1$. Общая частота поступления задач по туманным вычислениям, которые поступают в узел тумана i, будет равна сумме скоростей поступления, назначенных всем вычислительным узлам в слоях тумана. Чтобы смоделировать случайное поступление задач по туманным вычислениям от датчиков к узлу тумана i, общая скорость поступающих к узлу тумана i задач по туманным вычислениям, может быть смоделирована с помощью процесса Пуассона. Задачи по туманным вычислениям, выгруженные в узлы тумана и облако, также следуют процессу Пуассона, если задачи по туманным вычислениям случайным образом планируются в циклическом режиме [4]. Начальный узел тумана может определять порядок передачи пакетов задач по туманным вычислениям, выгруженных с уровня датчика.

Когда задачи по туманным вычислениям поступают от датчиков к узлу тумана i, они сначала хранятся в узле тумана i, что приводит к задержке ожидания. Эта дополнительная задержка относится к передаче от узла тумана i к c или j и может быть смоделирована с использованием очереди передачи. Кроме того, когда задачи по туманным вычислениям поступают в пункт назначения, задержка, необходимая для выполнения фактических вычислений, будет зафиксирована в очереди вычислений. На рис. показаны примеры обоих типов очередей. Например, для очередей передачи узел тумана i должен поддерживать очереди передачи для каждого узла тумана j и облака c. Каждый узел тумана имеет очередь вычислений. Для моделирования очереди передачи задач по туманным вычислениям, они передаются в узел тумана j по беспроводному каналу. Тогда скорость обслуживания (в пакетах в секунду) может быть задана как:

$$\mu_{ij} = \frac{W_l}{K} \log_2 \left(1 + \frac{g_{ij} h P_{tx,i}}{W_l N_0}\right), \qquad (1)$$

где g_{ij} – усиление канала между узлами тумана i и j, d_{ij} – расстояние между ними, а h – среднее усиление замирания узла тумана i. Когда узлы тумана

расположены поблизости в аналогичной среде, предположим, что они будут иметь идентичные средние коэффициенты усиления замирания. Если $d_{ij} \leq 1$м, $g_{ij} \triangleq \beta_1$ и, если $d_{ij} > 1$м, $g_{ij} \triangleq \beta_1 g_{ij}^{-\beta_2}$, где β_1 и β_2 – постоянная потери на трассе и показатель потерь на трассе. Кроме того, $P_{tx,i}$ – мощность передачи узла тумана i, а N_0 – спектральная плотность мощности шума. Пропускная способность на узле определяется как W_l, где $l = 1$ и 2 определяет два типа схем распределения полосы пропускания: равное распределение и распределение, ориентированное на облако. Для равного распределения полосы пропускания всем узлам в сети будет назначена одинаковая полоса пропускания, т. е. $W_1 = \frac{B}{J+1}$, где общая полоса пропускания B в равной степени совместно используется узлами $J + 1$, которые включают в себя J соседних узлов тумана и соединение с облаком через базовую станцию. Чтобы выделить полосу пропускания, ориентированную на облако, возьмем ее значение в два раза больше ширины полосы пропускания узла тумана, которая будет равна $\frac{2B}{J+2}$, в этом случае полоса пропускания узла тумана будет равна $\frac{B}{J+2}$.

Поскольку задачи поступают в соответствии с пуассоновским процессом, а время передачи в (1) является детерминированным, задержка очереди передачи может быть смоделирована как система массового обслуживания типа M/D/1 (M – система имеет входной пуассоновский поток заявок; D – время обслуживание имеет фиксированное значение, т. е. детерминировано; 1 – система имеет один прибор (устройство) обслуживания) [4]:

$$T_j\left(\lambda_{ij}(\alpha_{ij}), \mu_{ij}\right) = \frac{\lambda_{ij}(\alpha_{ij})}{2\mu_{ij}\left(\mu_{ij} - \lambda_{ij}(\alpha_{ij})\right)} + \frac{1}{\mu_{ij}},$$

где первое слагаемое – время ожидания в очереди узла тумана i, а второе слагаемое – задержка передачи между узлами тумана i и j. Аналогично, когда задачи по туманным вычислениям выгружаются в облако, задержка очереди передачи будет:

$$T_c(\lambda_c(\alpha_c), \mu_c) = \frac{\lambda_c(\alpha_c)}{2\mu_c(\mu_c - \lambda_c(\alpha_c))} + \frac{1}{\mu_c},$$

где скорость обслуживания μ_c между узлом тумана i и облаком c определяется как (1), а узел тумана j заменяется облаком c.

Когда узлу тумана необходимо вычислить задачи по туманным вычислениям, они будут ожидать время в очереди вычислений этого узла тумана из-за предыдущих задач по туманным вычислениям, которые в настоящее время обрабатывается. Так как узел тумана j получает задачи по туманным вычислениям не только от узла тумана i, но также от других узлов тумана

и датчиков, процесс прибытия задач по туманным вычислениям может быть аппроксимирован пуассоновским процессом с применением приближения Клейнрока [4]. Следовательно, очередь вычислений может быть смоделирована как очередь M/D/1 и задержка вычисления узла j тумана будет равна:

$$S_j\left(\lambda_{ij}(\alpha_{ij})\right) = \frac{\lambda_{ij}(\alpha_{ij})}{2\mu_j\left(\mu_j - \lambda_{ij}(\alpha_{ij})\right)} + \frac{1}{\mu_j} + \omega_j\lambda_{ij}(\alpha_{ij}), \quad (2)$$

где первое слагаемое – задержка ожидания в очереди вычислений, второе слагаемое – задержка для извлечения надлежащего приложения, необходимого для вычисления задачи по туманным вычислениям, а третье слагаемое – функция задержки процессора. Задержка этой процедуры выборки зависит от производительности оборудования узла, которая является детерминированной константой, определяющей время обслуживания очереди вычислений. В первом и втором слагаемом (2) μ_j является параметром, относящимся к общей аппаратной производительности узла тумана j. В третьем слагаемом $\omega_j\lambda_{ij}\,(\alpha_{ij})$ – это фактическое время вычисления задачи по туманным вычислениям, а ω_j – постоянное время, необходимое для вычисления задачи по туманным вычислениям.

Рассмотренная структура позволяет любому заданному узлу тумана динамически создавать сеть тумана, выбирая наиболее подходящий набор соседних узлов тумана при наличии неопределенности в порядке поступления соседних узлов тумана, а узел тумана в свою очередь может совместно использовать свою сеть тумана и удаленный облачный сервер для выполнения задач по туманным вычислениям.

Список используемых источников

1. Чан, Мунг и Тао Чжан. Туман и Интернет вещей: обзор возможностей исследования // IEEE Internet of Things Journal 3. 2016. С. 854–864.

2. Технический документ Cisco. Туманные вычисления и Интернет вещей: расширяйте облако, где бы они ни находились, 2015 [Электронный ресурс]. URL: https://www.cisco.com/c/dam/en_us/solutions/trends/iot/docs/computing-overview.pdf (дата обращения 29.01.2020).

3. Бономи, Флавио, Родольфо А. Милито, Цзян Чжу и Сатиш Аддепалли. Туманные вычисления и их роль в интернете вещей [Электронный ресурс] // 1-й MCC семинар по мобильным облачным вычислениям. Хельсинки, Финляндия: ACM, август 2012. С. 13–16. URL: https://conferences.sigcomm.org/sigcomm/2012/paper/mcc/p13.pdf (дата обращения 29.01.2020).

4. R. Deng, R. Lu, C. Lai и T. H. Luan, На пути к компромиссу между энергопотреблением и распределением рабочей нагрузки при вычислениях в облаке и тумане // In Proc. IEEE Int. Conf. on Commun. (ICC), London, UK, July 2015. PP. 3909–3914.

УДК 621.396.4
ГРНТИ 49.43.29

ПОЗИЦИОНИРОВАНИЕ В Wi-Fi-ТЕХНОЛОГИИ ЛОКАЛЬНОЙ БЕСПРОВОДНОЙ СЕТИ

Н. В. Будылдина, Ю. О. Гусева

Уральский технический институт связи и информатики

Выбор метода позиционирования влияет на точность оценки местоположения в сетях Wi-Fi. Проведенный анализ показывает, что позиционирование с помощью RSSI измерений и метода двумерной угловой латерации предполагает метровую точность и высокую плотность размещения точек доступа.

позиционирование, Wi-Fi, двумерная угловая латерация, RSSI, траектория перемещения абонентского устройства.

Технология Wi-Fi,для оборудования беспроводных локальных сетей WLAN, основана на стандартах 802.11. Широкое развертывание сетей Wi-Fi позволяет внедрять сервисы по определению местоположения, исходя из возможности управления пользовательскими сеансами в данной технологии. На точность оценки местоположения устройства клиента беспроводной локальной сети оказывает влияние выбор топологии и метода позиционирования. В качестве методов позиционирования в данных сетях предполагается использование триангуляции и ангуляции. Первый метод предполагает определение мощности сигнала абонентского устройства в зоне пересечения трех Wi-Fi точек доступа. Это позволяет после сопоставления и анализа накопленных полученных данных определить местоположение абонента с точностью до нескольких метров. Ангуляция подразумевает использование данных об измерении угла входящего сигнала. В дополнении к измерениям метода триангуляции это позволяет обеспечить позиционирование с точностью до метра. Однако, двумерной угловой латерации для определения местоположения абонента достаточно знать лишь координаты двух точек доступа беспроводной сети и данные об измерении двух углов между точками доступа и абонентским устройством [1]. При выполнении позиционирования методом двумерной угловой латерации, координаты устройства определяются по формулам:

$$x = \frac{d \times \tan(\varphi_1)}{\tan(\varphi_1) - \tan(\varphi_2)},$$

$$y = \frac{\tan(\varphi_1) \times d \times \tan(\varphi_2)}{\tan(\varphi_1) - \tan(\varphi_2)},$$

где d – расстояние между точками доступа, м; φ_1, φ_2 – измеренные углы между точками доступа и абонентским устройством, градусы.

Местоположения устройства во время перемещения, определенные с помощью двумерной угловой латерации, представлены на рис. 1. Данные расчеты были проведены в условиях перемещения абонента в сети минимум двух базовых станций, расположенных на расстоянии в десять метров друг от друга (параметр $d = 10$).

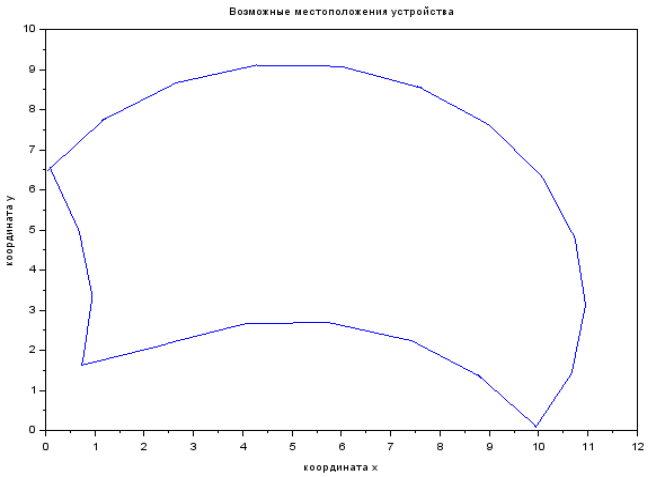


Рис. 1. Траектория перемещений абонента, определенная с помощью метода двумерной угловой латерации

На процесс позиционирования оказывают многолучевые эффекты во входящих радиосигналах до базовых станций, которые влияют на полученные измерения углов. Однако, существует метод позиционирования, основанный на данных о мощности сигнала.

Наиболее распространенным позиционированием в WLAN-сетях является оценка местоположения устройства пользователя сети на основе Received Signal Strength Indicator (RSSI) измерений. В данном случае большую роль играет выбранная модель распространения сигнала. Это обусловлено влиянием среды на сигнал, приводящий к его ослаблению. В разные моменты времени, в одной и той же области характеристики сигнала могут отличаться посредством влияния окружающей среды. Так точность алгоритма на основе RSSI измерений определяется степенью потерь при распространении сигнала от точек доступа. В зданиях и помещениях с большим количество препятствий затухание значительно выше, чем в свободной среде. На сигнал влияют преломления и отражения от препятствий, что и приводит к неточным оценкам расстояний.

Однако, данный метод имеет значительное преимущество в простоте реализации и не имеет недостатка накопления избыточности. Так как, погрешности в измерениях, в совокупности с избыточностью, снижают точность определения местоположения. Поэтому, метод на основе RSSI измерений позволяет достигать лучшего показателя позиционирования в отличие от методов, основанных на использовании уже накопленных из-

мерений, воспроизводимости ранее вычисленных моделей или использующих совокупные измерения от различных датчиков внутри абонентского устройства.

Параметр расстояния d, характеризующий расстояние от точки доступа Wi-Fi-сети до абонентского устройства и позволяющий определить местоположение устройства, определяется по формуле [2]:

$$d = 10^{\frac{P_d - 32{,}45 - 20\times\log_{10} f}{20 - 10\times n}}, \text{м}$$

где P_d – параметр RSSI, дБм, f – частота сигнала, МГц, $n = 13$ – коэффициент потери мощности сигнала при распространении в среде.

Исследуем влияние диапазонов 2,4 и 5 ГГц на точность определения местоположения устройства, исходя из диапазона значений параметра RSSI = [0; –30] дБм. Данный диапазон характеризует наилучший показатель сигнала, что свидетельствует о максимальных значениях точности позиционирования. График зависимости параметра расстояния d, характеризующего радиус действия точки доступа Wi-Fi-сети, от параметра RSSI для различных диапазонов представлен на рис. 2–3.

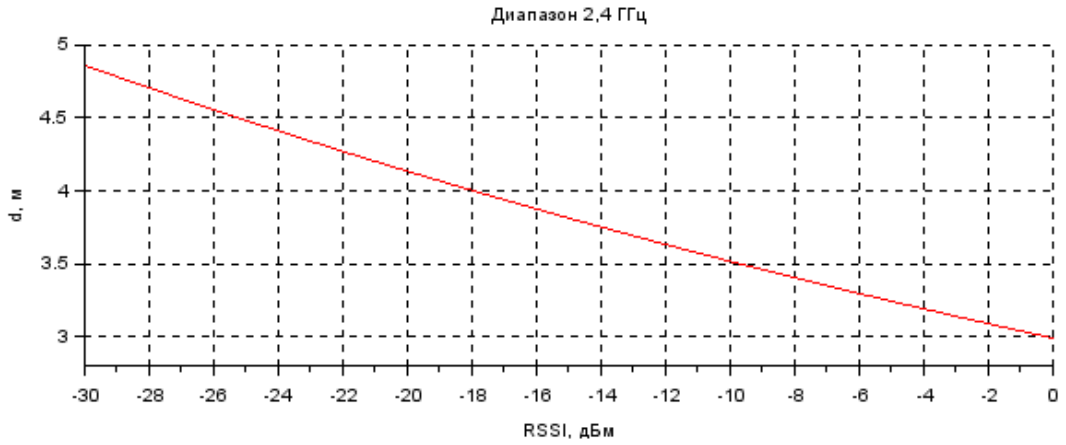


Рис. 2. Точность определения местоположения устройства для диапазона 2,4 ГГц

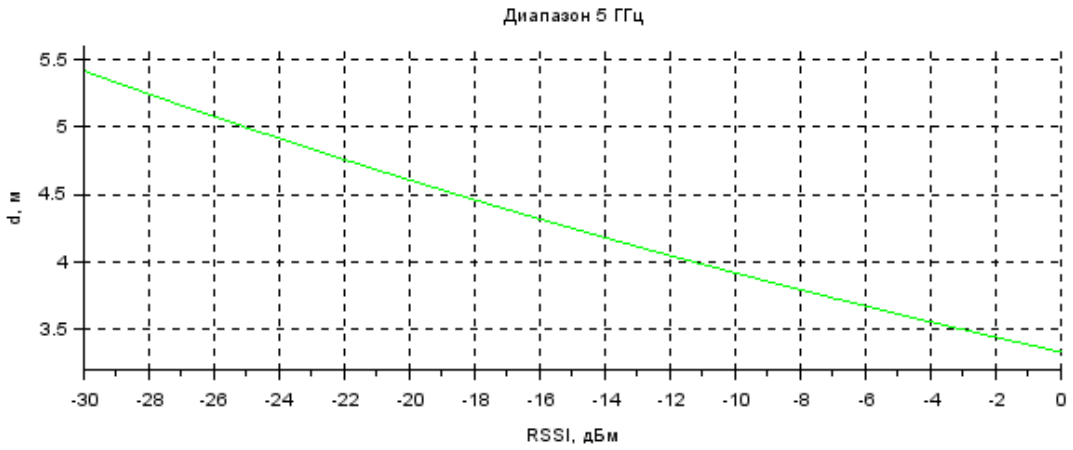


Рис.3.Точность определения местоположения устройства для диапазона 5 ГГц

Таким образом, анализируя графики, изображенные на рис. 2–3, определение местоположения абонентского устройства можно определить с точностью до 3,5 м в пяти гигагерцовом диапазоне и с точностью до 3 м в диапазоне 2,4 ГГц. Данный метод определения местоположения не может обеспечить точность сантиметрового уровня, в связи с тем, что наиболее эффективные показатели точности позиционирования достигаются при низкой мощности передаваемого сигнала в пределах зоны покрытия точки доступа.

Инфраструктура Wi-Fi-сети с функцией позиционирования требует большей плотности в размещении точек доступа для покрытия всех сегментов сети. Поэтому, появляется трудность в радиочастотном планировании таких сетей из-за подверженности диапазона 2,4 ГГц интерференции. В данном частотном диапазоне из тринадцати каналов лишь три канала являются неперекрывающимися, что накладывает ограничения на размещение точек доступа в сети. В таком случае, предполагается использование пяти гигагерцового частотного диапазона, так как все каналы этого диапазона являются неперекрывающимися. Однако оборудование стандарта IEEE 802.11a/g/n имеет некоторые ограничения в использовании, так как является устройствами для сетей малого радиуса действия. Таким образом, решением проблемы использования радиочастотного диапазона и ограничения в количестве точек доступа является использование данных позиционирования от других систем и технологий локального позиционирования. Выбор метода позиционирования определяется минимальными погрешностями в измерениях, минимальной избыточностью и наилучшей точностью. Основная проблема определения местоположения заключается в том, что предположить местоположение устройства можно основываясь на наборе измерений физических величин. Данные измерения обычно содержат значительное количество шумов или других систематических ошибок в измерении. Анализ эффективности рассмотренных в статье методов показал, что для охвата всех сегментов сети и реализации услуги позиционирования необходимо развернуть помимо Wi-Fi другие локальные технологии и системы.

Список используемых источников

1. Mohamad Yassin, Elias Rachid. A Survey of Positioning Techniques and Location Based Services in Wireless Networks // IEEE 2015 Int. Conf. Signal Processing, Informatics, Communication and Energy Systems, Kozhikode, India. 2016. PP. 4.

2. Lahteenmaki J. Indoor Propagation Models // COST Action 231. PP. 175–179.

УДК 519.872
ГРНТИ 49.03

АНАЛИЗ ДЖИТТЕРА В СМО ОБЩЕГО ВИДА

М. А. Буранова, М. И. Резяпкина, Д. Р. Эргашева

Поволжский государственный университет телекоммуникаций и информатики

Общий трафик современных сетей значительно увеличивается, а существующие ресурсы сети ограничены. Управление характеристиками сети позволяет выбрать наиболее оптимальное решение по управлению потоками. Задержка и ее джиттер являются параметрами, которые имеют наибольшее значение на передачу данных. В работе приведено сравнение аналитических результатов и результатов имитационного моделирования при оценке джиттера.

джиттер, задержка, качество обслуживания, моделирование.

Оценка производительности инфокоммуникационной сети всегда являлась одной из важнейших задач, которые решаются при исследовании телекоммуникационных сетей. При этом производительность сети тесно связана с понятием качества обслуживания (QoS – *Quality of Service*). Для обеспечения QoS в современных сетях необходимы новые методы, основанные на математических моделях реального трафика. При решении данных задач часто возникает проблема выбора адекватных моделей трафика. Проблема построения адекватной модели связанна с разнородностью обрабатываемых потоков, статистической структурой современного трафика, необходимостью учитывать конвергенцию инфокоммуникационных технологий, что может реально влиять на оценки производительности разрабатываемых сетей [1, 2, 3].

Анализ качества обслуживания связан, как правило, с оценкой таких параметров как задержка, джиттер (или вариация задержки), вероятность потери пакетов, производительность сети. Большинство исследований по данной проблеме направлено на оценку задержки. При этом для мультимедийных приложений, которые занимают значительную долю в общем объеме передаваемой информации, более важным параметром является джиттер. Его оценка для систем, обрабатывающих непуассоновские потоки представляет весьма серьезную проблему. На сегодняшний момент нет достаточно точных методов оценки джиттера при обработке трафика в системе $G/G/1$. Основные направления решения данной проблемы в основном связаны с имитационным моделированием. Это, безусловно, мощный и полезный инструмент, но и здесь возникают трудности с выбором модели трафика, описывающей реальные потоки.

В данной работе предложены подходы по анализу джиттера с использованием методов аналитического и имитационного моделирования.

В качестве примеров произвольного распределения (G) интервалов времени межу пакетами и длительностей пакетов в аналитической модели были использованы:

– экспоненциальное распределение;
– распределение Парето;
– распределение Вейбулла;
– гиперэкспоненциальное распределение – модель $H_2/H_2/1$.

Джиттер определяется либо как средняя абсолютная вариация задержки, либо как изменение задержки в потоке от некоторого минимального значения [4]. При этом согласно [5] под джиттером понимается случайная переменная:

$$J_{i+1} = |T_{i+1} - T_i|,$$

где T_i – время задержки i-го пакета в узле сети, которое определяется в виде $T_i = W_i + Q_i$, где W_i – время ожидания i-го пакета в очереди и Q_i – время его обслуживания.

Используя предположение Линдли [1], заключающееся в том, что (i + 1)-й пакет не будет ждать в очереди при условии, что интервал времени между приходом i-го и $(i+1)$-го пакета ($V_{i+1} \geq T_i$, где V_{i+1} – интервал времени между приходом $(i+1)$-го и i-го пакета) больше задержки i-го пакета, а также учитывая [2, 3, 6, 7, 8], получим:

$$W_{i+1} = \begin{cases} 0 & \text{при } V_{i+1} \geq T \\ W_i + Q_i - V_{i+1} & \text{иначе} \end{cases},$$

и поэтому

$$J_{i+1} = \begin{cases} |Q_{i+1} - T_i| & \text{при } V_{i+1} \geq T \\ |Q_{i+1} - V_{i+1}| & \text{иначе} \end{cases}.$$

Основываясь на представленных в [6] результатах, получим для среднего значения джиттера следующее выражение:

$$J = E(|T_{i+1} - T_i|) = \\ = \int_0^\infty f_V(y) \int_0^\infty f_Q(z) \left[\int_0^y |z - x| f_T(x) dx + \right. \\ \left. + |z - y| \int_y^\infty f_T(x) dx\right] dz \cdot dy, \quad (1)$$

где $f_T(x)$ – плотность вероятности случайной величины T, $f_V(y)$ – плотность вероятности случайной величины V и $f_Q(z)$ – плотность вероятности случайной величины Q.

Индексы i у плотностей вероятностей были отброшены, так как в рассматриваемом случае можно сделать предположение, что случайные величины T_i, Q_i и V_i независимы между собой и некоррелированны в структуре каждой последовательности случайной величины.

В случае экспоненциального распределения длин пакетов (1) примет вид:

$$J = \frac{(\eta^2+\mu^2)}{\eta\mu(\eta+\mu)} + \frac{2}{(\eta+\mu)}\mathcal{F}_R(\eta+\mu) - \frac{1}{\eta}\mathcal{F}_R(\eta), \quad (2)$$

где $\mathcal{F}_R(s)$ – преобразование Лапласа плотности распределения интервалов времени между пакетами; η – скорость передачи пакета, определяемая как $\eta = \mu(1-\rho)$; ρ – параметр нагрузки, определяемый как $\rho = \lambda/\mu$; μ – интенсивность обслуживания пакетов.

Преобразование Лапласа в случае экспоненциального распределения интервалов времени между пакетами имеет вид:

$$\mathcal{F}_R(s) = \frac{\lambda}{\lambda+s}.$$

И для джиттера из (2) можно получить:

$$J = \frac{1}{\mu}.$$

Для распределения Парето в [6] оценка джиттера производится с учетом того, что преобразование Лапласа имеет вид:

$$\mathcal{F}_R(s) = \alpha E_{a+1}(s,b),$$

где $E_n(x) = \int_1^\infty \frac{e^{-xt}}{t^n}dt$ – интегральная показательная функция.

Для случая распределения Вейбулла (при $a = 2$, $b = 1$), преобразование Лапласа имеет вид:

$$\mathcal{F}(s) = \frac{2}{s+2}.$$

В случае системы $H_2/H_2/1$ джиттер будет иметь вид:

$$J = \alpha_1 + \alpha_2(A+B) -$$
$$-\frac{A}{\mu_1}\left[\frac{p\gamma_1}{\mu_1+\gamma_1} + \frac{(1-p)\gamma_2}{\mu_1+\gamma_2}\right] - \frac{B}{\mu_2}\left[\frac{p\gamma_1}{\mu_2+\mu_1} + \frac{(1-p)\gamma_2}{\mu_2+\gamma_2}\right] +$$
$$+\frac{2qA}{\mu_1}\left[\frac{p\gamma_1}{2\mu_1+\gamma_1} + \frac{(1-p)\gamma_2}{2\mu_1+\gamma_2}\right] + \frac{2(1-q)B}{\mu_2}\left[\frac{p\gamma_1}{2\mu_2+\mu_1} + \frac{(1-p)\gamma_2}{2\mu_2+\gamma_2}\right] +$$
$$+2\left[\frac{A(1-q)}{\mu_2} + \frac{Bq}{\mu_1+\gamma_2}\right]\cdot\left[\frac{p\gamma_1}{\mu_1+\mu_2+\gamma_1} + \frac{(1-p)\gamma_2}{\mu_1+\mu_2+\gamma_2}\right],$$

где $A = \frac{\delta q}{|\delta-\mu_1|}$, $B = \frac{\delta(1-q)}{|\delta-\mu_2|}$, $\alpha_1 = \frac{(\mu_1-\mu_2)(Bq\mu_1-A(1-q)\mu_2)}{\mu_1\mu_2(\mu_2+\mu_1)}$, $\alpha_2 = \frac{(1-q)\mu_1+q\mu_2}{\mu_1\mu_2}$.

Значения параметров можно определить либо с использованием EM алгоритма, либо по двум моментам (среднее, дисперсия). В работе был использован второй подход.

Результаты аналитического моделирования представлены на рис. 1.

Для имитационного моделирования были использованы модели трафика на основе распределений:

– экспоненциальное распределение;
– распределение Парето;
– распределение Вейбулла;
– реальный трафик, зарегистрированный на сети провайдера.

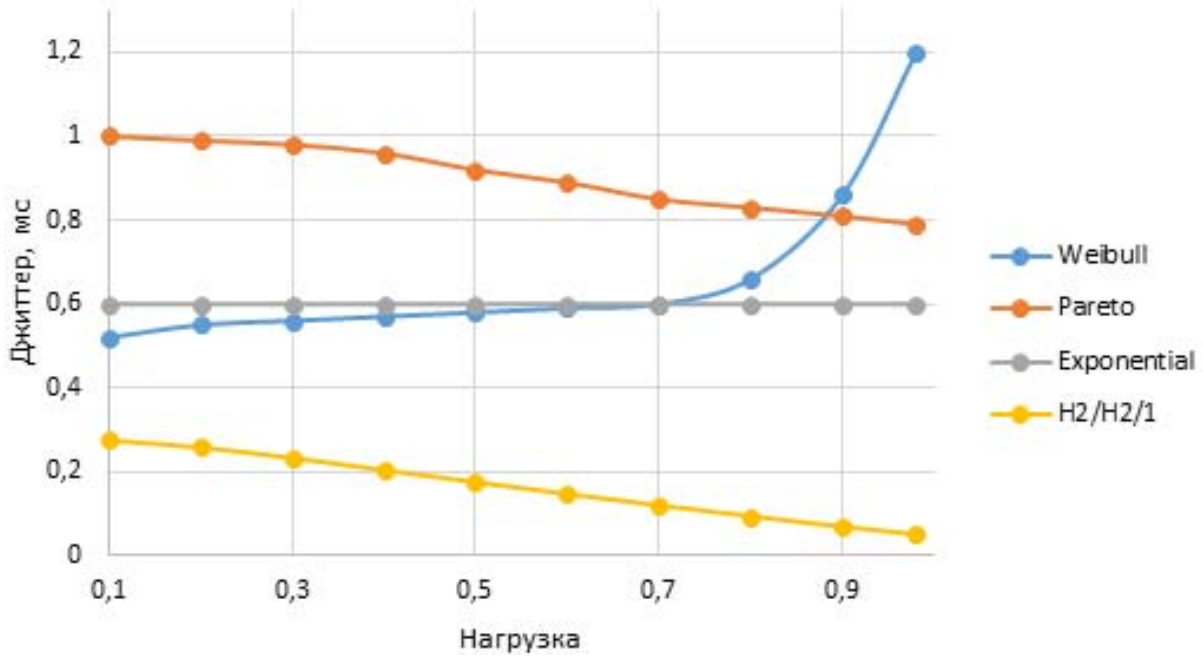


Рис. 1. Изменение джиттера задержки пакетов в зависимости от загрузки сети при аналитическом моделировании

На рис. 2 (см. ниже) представлены результаты имитационного моделирования для сравнения поведения джиттера при различных распределениях.

На основе анализа полученных результатов можно сделать вывод, что джиттер во всех рассмотренных случаях не обращается в ноль при коэффициенте загрузке равном нулю, и не становится бесконечным при загрузке близкой к единице.

В случае трафика с экспоненциальным распределением длительности пакетов и длин пакетов увеличение загрузки сети в системе не оказывает заметного влияния на значение джиттера. В случае модели трафика с распределением Парето наблюдается общее снижение джиттера при увеличении загрузки системы. В случае распределения Вейбулла джиттер увеличивается, но не обращается в бесконечность.

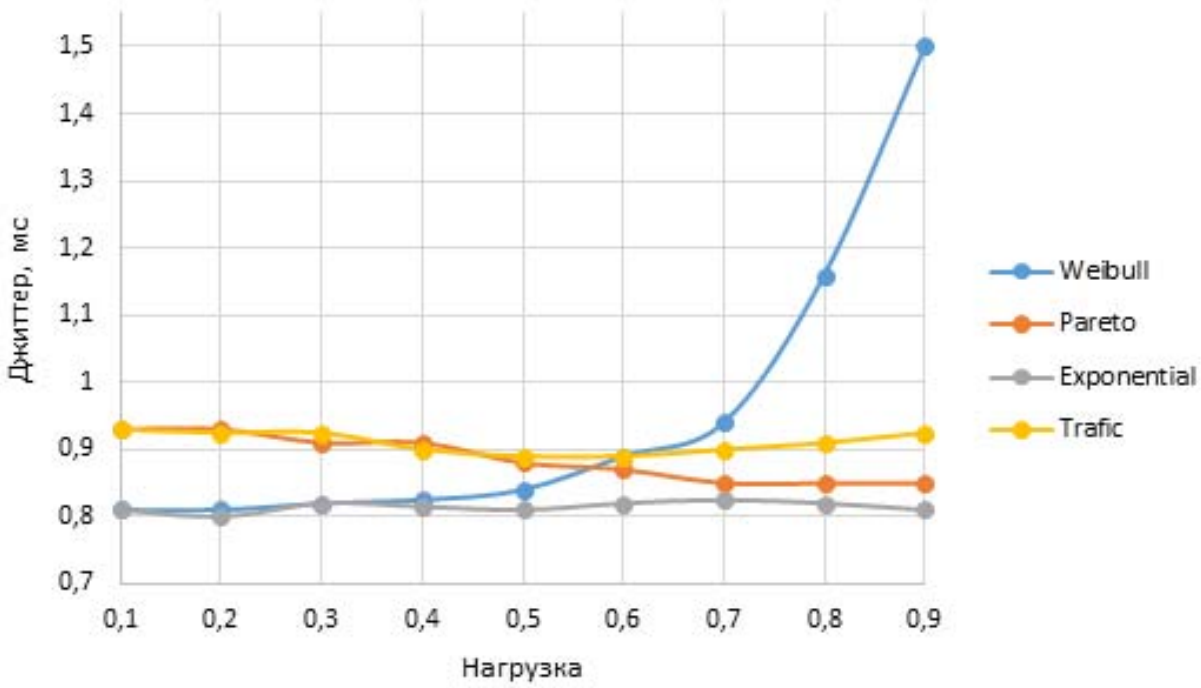


Рис. 2. Изменение джиттера пакетов в зависимости от загрузки сети при имитационном моделировании

Результаты имитационного и аналитического моделирования вполне согласуются.

Список используемых источников

1. Kleinrock L. Queueing Systems: Volume I, Theory. New York : Wiley Interscience, 1975. 417 p.

2. Kartashevskiy I., Buranova M. Calculation of Packet Jitter for Correlated Traffic. In-Internet of Things, Smart Spaces, and Next Generation Networks and Systems // NEW2AN 2019, ruSMART 2019. Lecture Notes in Computer Science, vol. 11660. Springer, Cham.

3. Карташевский В. Г., Буранова М. А. Моделирование джиттера пакетов при передаче по мультисервисной сети // Информационные технологии и телекоммуникации. 2019. Т. 17. № 1. С. 34–40.

4. Demichelis C., Chimento P. IP Packet Delay Variation Metric for IP Performance Metrics (IPPM) // Institution IETF, RFC 33934. 2000. 21 p. DOI: 10.17487/RFC3393.

5. Internet protocol data communication service IP packet transfer and availability performance parameters, ITU-T Recommendation Y.1540. 2002. 33 p.

6. Dahmouni H., Girard A., Sanso B. An analytical model for jitter in IP networks // Annals of telecommunications-annales des telecommunications, 2012. PP. 81–90.

7. Matragi W., Bisdikian C., Sohraby K. Jitter calculus in ATM networks: single node case // IEEE INFOCOM’ 94. Toronto: 1994.

8. Matragi W., Sohraby K., Bisdikian C. Jitter calculus in ATM networks: multiple node case // IEEE/ACM Trans Netw5. 1997. PP. 122–133.

УДК 004.056.5
ГРНТИ 81.93.29

ЗАДАЧИ АНАЛИЗА И СИНТЕЗА СИСТЕМ РАЗГРАНИЧЕНИЯ ДОСТУПА К ДАННЫМ В ОБЛАЧНЫХ ИНФРАСТРУКТУРАХ КРИТИЧЕСКИ ВАЖНЫХ ИНФОРМАЦИОННЫХ ОБЪЕКТОВ

С. Н. Бушуев[1], **О. И. Пантюхин**[2], **И. Б. Паращук**[3,4], **И. Б. Саенко**[3,4]

[1]АО «НПП ТЕЛДА»
[2]Санкт-Петербургский государственный университет телекоммуникаций им. проф. М. А. Бонч-Бруевича
[3]Санкт-Петербургский институт информатики и автоматизации Российской академии наук
[4]Санкт-Петербургский национальный исследовательский университет информационных технологий, механики и оптики

Рассматривается комплекс задач анализа и синтеза систем и механизмов разграничения доступа к данным в современных облачных инфраструктурах критически важных информационных объектов. Этот вид информационных инфраструктур находит все большее применение в промышленности и иных сферах деятельности личности и государства, поэтому защита данных в них является ключевой задачей. Предложенные и детально описанные сущность и содержание задач анализа и синтеза позволяют, в случае их успешного решения, добиться результатов, способных положительно повлиять на надежность и качество политик разграничения доступа, что, в свою очередь, позволит повысить защищенность элементов и контента облачных инфраструктур критически важных информационных объектов и систем.

критически важный информационный объект, система, разграничение доступа, анализ, синтез, облачная инфраструктура, данные, угроза, искусственный интеллект.

Актуальность задач разграничения доступа к данным в облачных инфраструктурах (ОИ) критически важных информационных объектов (КВИО) и систем, а также задач обнаружения и разрешения конфликтов при использовании различных политик разграничения доступа в КВИО, объективно обусловлена повышением роли и стремительным распространением ОИ, повышением ценности активов устройств, программного обеспечения и критически важных данных таких систем, а также увеличением числа атак на системы такого класса и ростом количества попыток получения несанкционированного доступа к данным, хранящимся и обрабатываемым в них. Именно поэтому возрастает роль и значимость решения задач совершенствования моделей контроля доступа, задач разработки, на основе этих моделей и технологии искусственного интеллекта, эффективных методов и алгоритмов управления политиками разграничения доступа (РД) в облачных инфраструктурах КВИО. Совершенствование моделей, методов

и алгоритмов управления политиками РД, создание новых систем РД к данным в ОИ КВИО является системной проблемой, традиционно включающей задачи анализа и синтеза [1].

К задачам анализа можно отнести детальное изучение существующих научно-исследовательских работ в предметной области РД к информации (данным) в ОИ КВИО. Причем анализ должен осуществляться с учетом специфики, присущей облачным системам хранения данных, которые являются важнейшими компонентами КВИО.

Задачи анализа должны включать детальное изучение средств и методов разработки и применения существующих и перспективных моделей контроля доступа на основе ролей Role-Based Access Control (RBAC), на основе атрибутов Attribute-Based Access Control (ABAC), моделей организационного контроля доступа Organization-Based Access Control (OrBAC), моделей доступа на основе объектов Object-Based Access Control (OBAC) и т. д., с целью выяснения возможностей и механизмов их практической реализации в облачных инфраструктурах.

К задачам анализа, безусловно, относится исследование средств и методов искусственного интеллекта (ИИ) для оптимизации, верификации и реконфигурации политик РД к данным ОИ КВИО. Итогом решения задач анализа будет формализованная постановка задачи обеспечения, требуемого РД к данным ОИ КВИО. Она должна будет включать описание исходных данных, ограничений допущений, варьируемых переменных и целевых функций для различных моделей контроля доступа.

К задачам синтеза, в первую очередь, необходимо отнести разработку системы показателей и критериев оценки качества политик РД для различных моделей управления доступом, применяемых ОИ КВИО. Показатели качества политик разграничения доступа должны показывать, насколько действующие политики отвечают предъявляемым требованиям, и позволять сформировать различные критерии синтеза (оптимизации) и реконфигурации этих политик. В настоящее время считается, что показатели качества в достаточной степени разработаны для политик, основанных на модели RBAC. Для моделей ABAC, OrBAC, OBAC этот вопрос исследован в недостаточной степени. Критерии оценки качества политик разграничения доступа увязываются с различными сценариями их формирования и позволяют сформировать различные варианты постановки задачи [2].

Важной задачей синтеза является формулировка концептуальной модели процесса разграничения доступа к данным в облачных инфраструктурах критически важных информационных систем. Эта модель призвана описать процесс разграничения доступа на самом высоком уровне. Концептуальная модель процесса РД к данным ОИ КВИО состоит из нескольких компонентов: функционального, понятийно-терминологического,

критериального и верификационного. Функциональный компонент определяет основные функции системы разграничения доступа и функциональные взаимосвязи между ее элементами. Понятийно-терминологический компонент определяет систему терминов и понятий, используемых в предметной области исследований, включая новые понятия, необходимые для использования. Критериальный компонент определяет совокупность постановок задач, описывающих процессы формирования политик РД. Верификационный компонент описывает условия, позволяющие определить и разрешить конфликты в политиках РД к данным ОИ КВИО.

Помимо этого, важной задачей синтеза является разработка моделей, методов и алгоритмов оценки качества политик РД для различных подходов к управлению доступом, применяемых в ОИ КВИО. Данные модели, методы и алгоритмы позволяют оценить качество политик разграничения доступа для различных механизмов управления доступом с учетом разработанной системы показателей качества. Возможными подходами для такой оценки являются использование гибридных нейронных сетей и применение систем нечеткого логического вывода.

Сущность и содержание задачи синтеза, нацеленной на разработку частных моделей и алгоритмов оптимизации политик РД для различных механизмов управления доступом, применяемых в ОИ КВИО, опирается на применяемый методологический аппарат – технологию ИИ. Эти модели и алгоритмы предназначены для решения оптимизационных задач формирования политик безопасности, которые по своей вычислительной сложности, как правило, являются очень трудоемкими (по аналогии с моделью RBAC). Наиболее приемлемым представляется использование для этой цели генетических алгоритмов [3].

Однако возможно также применение других типов алгоритмов, относящихся к категории биоинспирированных, например, муравьиных, роевых, методов дифференциальной эволюции и т. п. Кроме того, перечень задач синтеза не будет полным без разработки моделей и алгоритмов верификации и обеспечения непротиворечивости политик РД в ОИ КВИО на основе технологии ИИ. Разработка этих моделей и алгоритмов осуществляется на основе многоагентной нечеткой классификации.

Синтез моделей и алгоритмов выявления условий проведения и непосредственного выполнения реконфигурации политик РД в ОИ КВИО на основе технологии ИИ, является еще одной важной задачей. Данные модели и алгоритмы являются дальнейшим развитием моделей и алгоритмов оптимизации политик РД, при этом в состав исходных данных включается текущая конфигурация политики РД, а в качестве критерия синтеза выступает минимум административных издержек по приведению текущей конфигурации к новой, требуемой конфигурации.

К задачам синтеза необходимо отнести и задачу разработки обобщенной архитектуры и программного прототипа компонентов перспективной системы РД к данным в ОИ КВИО. Обобщенная архитектура описывает состав и взаимосвязь основных компонентов перспективной системы РД, а программный прототип позволяет продемонстрировать корректность выработанных решений по построению этой системы.

Заключительными этапами анализа и синтеза систем РД к данным в ОИ КВИО являются этап выработки практических рекомендаций по построению систем такого класса. Экспериментальные оценки могут быть получены на базе разработанного программного прототипа системы разграничения доступа к данным в ОИ КВИО, а рекомендации по созданию и применению системы РД для различных сценариев построения и функционирования облачных инфраструктур критически важных информационных систем носят новый, оригинальный характер – они сформулированы с учетом современных достижений в области информационной безопасности, системного анализа, моделирования, биоинспирированной оптимизации, формальной верификации, организации знаний и искусственного интеллекта, теории принятия решений, объектно-ориентированного проектирования и интеллектуального анализа данных.

Рассмотренные сущность и содержание задач синтеза и анализа составляют научно-методическую и практическую основу обеспечения безопасности информации в ходе построения и функционирования ОИ КВИО. По сравнению с другими классами информационных инфраструктур, в ОИ данная проблема не просто имеет большую актуальность, а приобретает иные, новые аспекты, особенно в области защиты от несанкционированного доступа и контроля за разграничением доступа к облачным информационным и телекоммуникационным ресурсам.

Поэтому предложенный перечень задач анализа и синтеза имеет своей общей, фундаментальной целью разработку моделей, методов и методик гарантированного, безусловного обеспечения требований по разграничению доступа к ресурсам облачных инфраструктур критически важных информационных систем на основе применения методов искусственного интеллекта. Новые виды угроз безопасности информации в ОИ, вызванные, в частности, такими факторами, как необходимость совместной обработки в них информации различных форматов представления (включая мультимедиа и геоинформацию), отличающейся различными уровнями конфиденциальности и требованиями по целостности и доступности, неполнотой и противоречивостью, а также увеличение функциональности и уровня средств злоумышленников, развитие сетевых атак и распространение злонамеренного программного обеспечения, определяют новизну, значимость и масштабность предложенного комплекса задач анализа и синтеза, от результатов решения которых зависит эффективность использования ОИ КВИО в целом.

Результаты решения комплекса задач анализа и синтеза с точки зрения противодействия угрозам в настоящий момент нацелены не столько на разработку новых механизмов РД, сколько на разработку научно-методического обеспечения по эффективному и комплексному применению этих механизмов, приводящему к корректному и обоснованному формированию политик и схем разграничения доступа и управлению ими.

Ориентация на использование технологий, средств и методов искусственного интеллекта при решении задачи разграничения доступа к ресурсам облачных инфраструктур критически важных информационных систем во многом обусловлена неполнотой и/или противоречивостью исходных данных, масштабностью вычислительных затрат, необходимых для решения этой задачи традиционными математическими методами и имеющимися результатами анализа мирового опыта разработки и успешного использования интеллектуальных средств и механизмов защиты информации в компьютерных системах и сетях.

Предполагается, что в отличие от существующих подходов, результаты решения описанных задач анализа и синтеза будут представлять собой комплекс моделей и алгоритмов, которые основываются на методах эволюционного моделирования нарушителя и средств защиты, верификации политик разграничения доступа на основании темпоральных, дескрипционных и других видов логик, совершенствования политик и схем РД на основе биоинспирированных методов оптимизации, включая генетические алгоритмы.

Кроме того, учтены результаты оценки и прогнозирования состояния ресурсов на основе моделей временных рядов и нейросетевых моделей, результаты анализа и контроля уровня обеспечения требований по РД к данным на основе интеграции методов моделирования и методов интеллектуального анализа данных.

Предложенный подход, по мнению авторов, позволит повысить надежность и качество политик разграничения доступа, что, в свою очередь, позволит повысить защищенность элементов и контента облачных инфраструктур критически важных информационных объектов и систем.

Работа выполнена при финансовой поддержке РФФИ (проект 18-07-01369) в СПИИРАН.

Список используемых источников

1. Meghanathan N. Review of Access Control Models for Cloud Computing // Proceedings of the Third International Conference on Computer Science, Engineering & Applications, ICCSEA, Chennai, India, May 24–26, 2013. PP. 77–85.

2. Паращук И. Б., Саенко И. Б., Пантюхин О. И. Анализ состояния исследований по моделированию разграничения доступа к информации в облачных инфраструктурах критически важных информационных систем // Актуальные проблемы инфотелекомму-

никаций в науке и образовании. VII Международная научно-техническая и научно-методическая конференция (АПИНО-2018); сб. науч. ст. в 4 т. СПб. : СПбГУТ, 2018. Т. 1. С. 604–609.

3. Saenko I., Kotenko I. Design and Performance Evaluation of Improved Genetic Algorithm for Role Mining Problem // In Proceedings of the 20th International Euromicro Conference on Parallel, Distributed and Network-based Processing (Garching, Germany, February 15–17, 2012). PDP'2012, IEEE, 2012. PP. 269–274.

УДК 621.315
ГРНТИ 47.61, 49.29.17, 59.29

ЗОНДИРУЮЩИЕ СИГНАЛЫ ДЛЯ РЕФЛЕКТОМЕТРИИ КАБЕЛЬНЫХ ЛИНИЙ СВЯЗИ ВО ВРЕМЕННОЙ ОБЛАСТИ

М. С. Былина

Санкт-Петербургский государственный университет телекоммуникаций им. проф. М. А. Бонч-Бруевича

Приведена классификация зондирующих сигналов, используемых для рефлектометрии во временной области. Рассмотрены требования к зондирующим сигналам и их характеристики. Проведен сравнительный анализ различных зондирующих сигналов. Показаны преимущества применения комплементарных последовательностей.

двухпроводная цепь, рефлектометрия во временной области, зондирующий сигнал, импульсный сигнал, перепад напряжения, псевдослучайная последовательность, комплементарные последовательности, комплементарные последовательности Голея.

Метод рефлектометрии во временной области (*Time Domain Reflectometry*, TDR) рекомендуется использовать для профилактических и аварийных измерений кабельных двухпроводных цепей (ДЦ) [1]. Он основан на зондировании двухпроводной цепи (ДЦ) широкополосными зондирующими сигналами с последующей регистрацией, обработкой и анализом совокупности отраженных от неоднородностей сигналов, называемой сигналом обратного потока (СОП) [1, 2, 3].

Зондирующие сигналы (ЗС), применяемые в TDR, обычно являются периодическими и имеют конечную длительность t_p, меньшую периода T_0. Поэтому рефлектограммы являются результатом многократных измерений, что позволяет уменьшить случайные погрешности и влияние электромагнитных помех на исследуемую цепь. Во временной области ЗС представляют собой зависимости электрического напряжения от времени, их можно

также характеризовать амплитудно-частотной (АЧХ) и автокорреляционной характеристиками (АКХ), так как корреляционная обработка позволяет улучшить разрешающую способность измерений [1, 3]. Длительность АКХ определяет предельную разрешающую способность ЗС.

ЗС можно разделить на простые и сложные. Примерами простых сигналов являются униполярные импульсы и перепады напряжения. Сложные сигналы могут иметь различную форму и структуру. Из сложных сигналов наиболее часто применяются псевдослучайные последовательности (ПСП) импульсов напряжения.

Подавляющее большинство современных рефлектометров используют в качестве ЗС униполярные импульсы напряжения. Импульсы, используемые для зондирования ДЦ длиной l с коэффициентом укорочения k_y, должен удовлетворять условиям:

1) длительность t_p должна быть существенно меньше удвоенного времени распространения сигнала $t_z = 2lk_y / c$,

2) период следования импульсов T_0 должен быть больше t_z. Основными параметрами униполярного импульсного ЗС, кроме t_p и T_0, являются его форма $u_1(t)$, площадь S_p и энергия W_p.

Наиболее распространенным видом униполярного импульсного ЗС является трапецеидальный импульс, имеющий конечные длительности переднего t_{f1} и заднего t_{f2} фронтов ($t_p \geq t_{f1} + t_{f2}$). Для формы $u_1(t)$, энергии W_p и спектра $\dot{U}_1(j\omega)$ трапецеидального импульса справедливо:

$$\frac{u_1(t)}{U_m} = \begin{cases} t/t_{f1}, & 0 \leq t < t_{f1} \\ 1, & t_{f1} \leq t \leq t_p - t_{f2} \\ 1-\left(t - t_p + t_{f2}\right)/t_{f2} & t_p - t_{f2} < t \leq t_p \end{cases}, \; U_m = \frac{S_p}{t_p - \left(t_{f1} + t_{f2}\right)/2}, \tag{1}$$

$$W_p = U_m^2 \left(t_p + 2\left(t_{f1} + t_{f2}\right)/3\right), \tag{2}$$

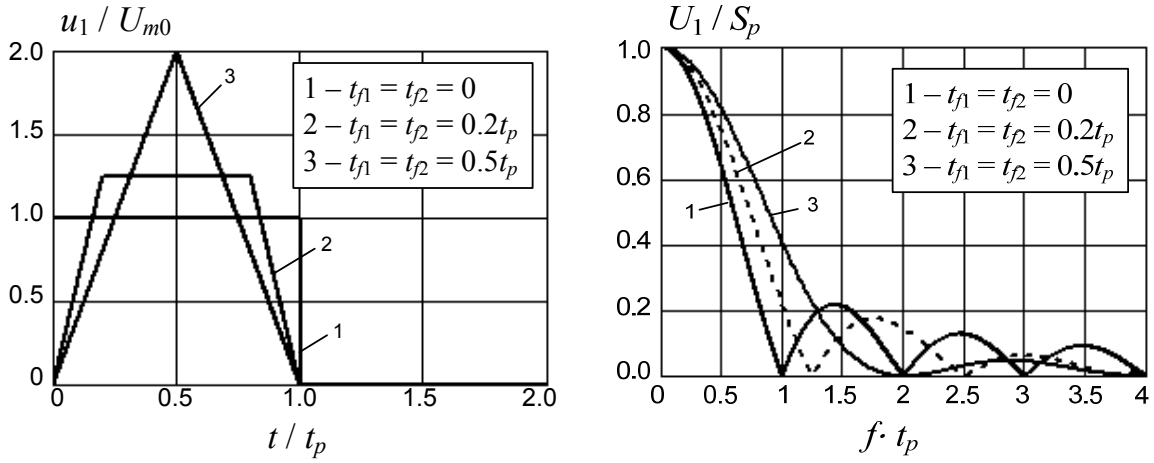
$$\dot{U}_1(j\omega) = U_m \left[t_{f2}\left(1 - e^{-j\omega t_{f1}}\right) + t_{f1} e^{-j\omega t_p}\left(1 - e^{j\omega t_{f2}}\right)\right] \Big/ \left[(j\omega)^2 t_{f1} t_{f2} \right], \tag{3}$$

На рис. 1 (см. ниже) показаны форма и амплитудный спектр трапецеидального, а также прямоугольного и треугольного импульсов той же площади, являющихся частными случаями (1) при $t_{f1} = t_{f2} = 0$ и $t_{f1} + t_{f2} = t_p$ соответственно.

Истинный перепад напряжения является одиночным сигналом с амплитудой U_m и бесконечной длительностью, для формы $u_1(t)$ и амплитудного спектра $U_1(f)$ которого справедливы соотношения:

$$u_1(t) = \begin{cases} U_m, & t \geq 0 \\ 0, & t < 0 \end{cases}, \; U_1(f) = \frac{U_m}{f} \tag{4}$$

АКХ истинного перепада представляет собой дельта-функцию, то есть перепад теоретически позволяет получить наилучшую разрешающую способность. Однако такой сигнал практически нереализуем, поэтому в реальных рефлектометрах вместо истинного перепада используют периодическую последовательность прямоугольных импульсов с длительностью $t_p > t_z$. Параметры такого ЗС определяются (1)–(3).



а) б)

Рис. 1. Форма (а) и амплитудный спектр (б) униполярных импульсов напряжения: 1 – прямоугольного, 2 – трапецеидального, 3 – треугольного

Сопоставление рефлектограмм, зарегистрированных при коротких и длинных зондирующих импульсах (перепадах) позволяет получить дополнительную информацию о неоднородностях в ДЦ.

При использовании униполярных импульсных ЗС для улучшения разрешающей способности необходимо уменьшать t_p, однако при этом уменьшается энергия СОП. Избежать уменьшения энергии позволяют ЗС, представляющие собой ПСП из N коротких импульсов напряжения, обычно положительной и отрицательной полярности. У таких сигналов общая энергия в N^2 превышает энергию одиночного импульса, а малая длительность отдельных импульсов позволяет улучшить разрешающую способность измерений.

Форма СОП $u_0(t)$ в этом случае не позволяет непосредственно анализировать ДЦ. Переход к рефлектограмме, подобной традиционной, полученной при использовании коротких униполярных ЗС, может быть реализован с помощью корреляционной обработки

$$u_c(t) = u_1(t) \times u_0(t) = u_1(t) \times u_1(t) * g(t), \qquad (5)$$

где $g(t)$ – импульсная характеристика ДЦ, × означает корреляцию, а * – свертку.

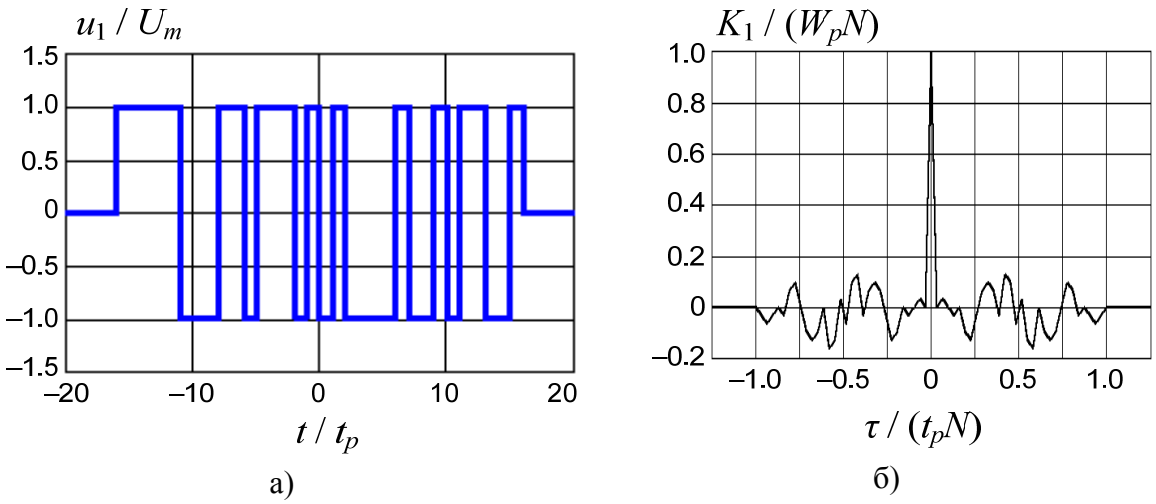
В (5) входит АКХ зондирующей последовательности $u_1(t)\times u_1(t)$, поэтому для обеспечения высокого пространственного разрешения необходимо, чтобы АКХ имела один узкий максимум без боковых лепестков. Этому требованию удовлетворяют непрерывные *M*-последовательности [4], которые формируются с помощью регистров сдвига по правилу:

$$a_0 x_i = a_1 x_{i-1} \oplus a_2 x_{i-2} \oplus \ldots \oplus a_n x_{i-n}\,, \qquad (6)$$

где x_i – символы последовательности, a_i – коэффициенты характеристического многочлена $f(x) = a_n x^n + a_{n-1}x^{n-1} + a_{n-2}x^{n-2} + \ldots + a_1 x + 1$, принимающие значения 0 или 1, n – разрядность регистра сдвига, сложение и умножение производится по модулю 2. Характеристический многочлен должен быть неприводимым и примитивным. Полученный по правилу (6) ЗС имеет период $N = 2^n - 1$, содержащий все возможные комбинации n-значных двоичных чисел, за исключением нулевой.

В рефлектометрии вместо непрерывных *M*-последовательностей, требующих выделения СОП на фоне мощного ЗС, применяются усеченные – непериодические последовательности длиной, обычно равной одному периоду N, состоящие из прямоугольных импульсов напряжения одинаковой длительности t_p, амплитуды U_m, площади S_p и энергии W_p, но разной полярности – положительные импульсы соответствуют логическим единицам, отрицательные – логическим нулям. Регистрация СОП начинается сразу после окончания ЗС, что позволяет снизить требования к устройству ввода-вывода.

На рис 2 представлены усеченная *M*-последовательность – один период последовательности, сформированной при $n = 5$ на основе характеристического многочлена $f(x) = x^5 + x^3 + 1$, и ее АКХ. В качестве начального кодового слова использована комбинация 11111.



а) б)

Рис. 2. Форма (а) и АКХ (б) одного периода усеченной *M*-последовательности

Из рис. 2 видно, что АКХ усеченной *M*-последовательности имеет боковые пики, которые приводят к искажению СОП даже после корреляционной обработки [5]. Боковые пики можно исключить в суммарной АКХ комплементарных последовательностей, например, двух последовательностей Голея [5, 6].

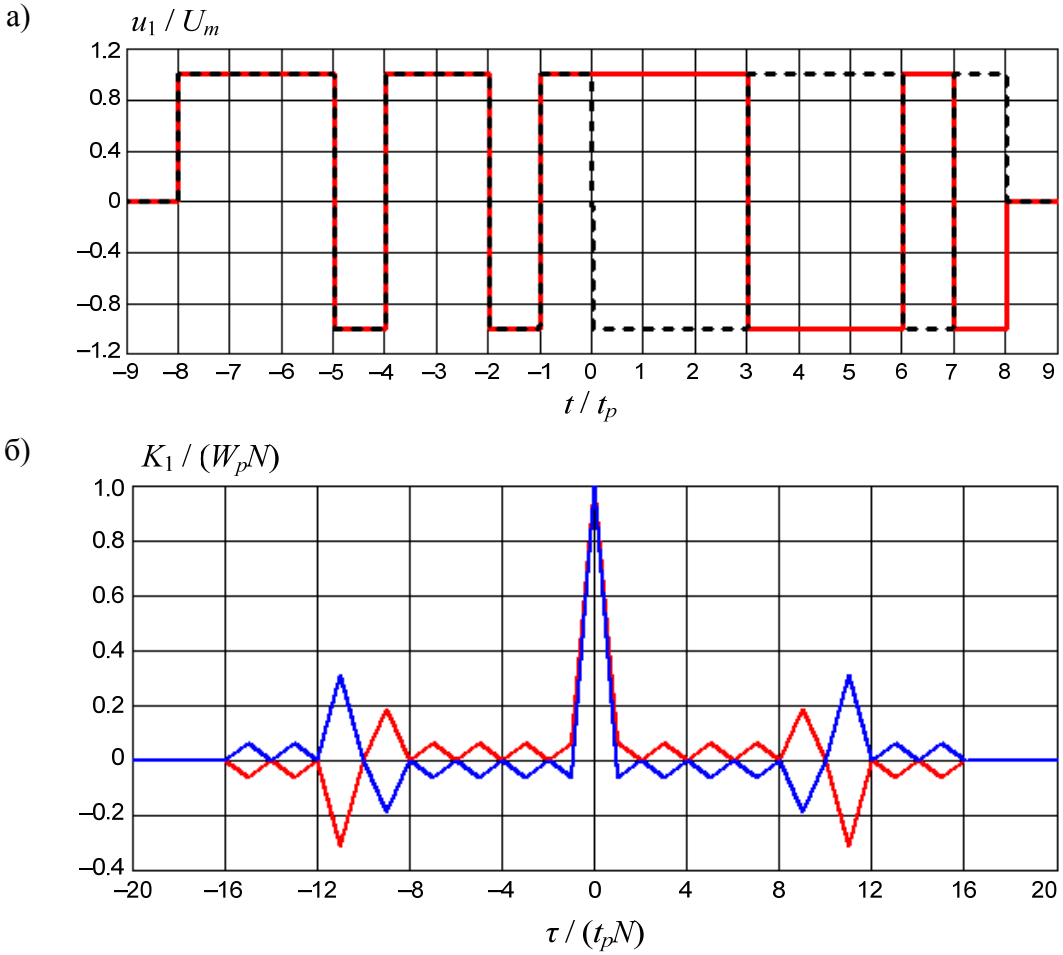


Рис. 3. Комплементарные последовательности (а) и их АКХ (б)

На рис. 3 представлены две комплементарные последовательности с $N = 16$, сформированные по правилу присоединения [7], а также их АКХ. При практической реализации рефлектометра с ЗС в виде комплементарных последовательностей Голея реализуется следующий алгоритм работы:

1. посылка первой последовательности Голея $u_{11}(t)$, прием СОП $u_{r11}(t)$ и запись его в память, вычисление взаимной корреляционной функции $K_{11} = u_{11}(t) \times u_{r11}(t)$ и запись ее в память;

2. посылка второй последовательности Голея $u_{12}(t)$, прием СОП $u_{r12}(t)$ и запись его в память, вычисление взаимной корреляционной функции $K_{12} = u_{12}(t) \times u_{r12}(t)$ и запись ее в память;

3. вычисление суммы взаимных корреляционных функций $K_1 = K_{11} + K_{12}$, запись ее в память;

4. повторение пунктов 1–3 и получение K_2, K_3, … K_M.

5. вычисление усредненной взаимной корреляционной функции $K = (1/M) \cdot \sum K_i$, которая и выводится на экран рефлектометра.

Преимуществом комплементарных последовательностей является нулевая сумма боковых пиков их АКХ. Это позволяет рекомендовать их для использования в корреляционных приборах, реализующих метод рефлектометрии во временной области.

Список используемых источников

1. Былина М. С. Обзор и сравнительный анализ рефлектометрических методов измерения параметров кабельных линий связи // Актуальные проблемы инфотелекоммуникаций в науке и образовании. VIII Международная научно-техническая и научно-методическая конференция сб. науч. Ст. в 4-х т. СПб. : СПбГУТ, 2019. Т. 1. С. 192–187.

2. Былина М. С., Глаголев С. Ф. Рефлектометрия кабелей связи : монография; СПбГУТ. – СПб., 2015. 228 с.

3. Furse C., Chung Y. C., Lo C., Pendayala P. A critical comparison of reflectometry methods for location on wiring faults // Smart Structures and Systems. 2006. Vol. 2, No. 1. PP. 25–46.

4. Варакин Л. Е. Системы связи с шумоподобными сигналами. М. : Радио и связь, 1985. 304 с.

5. Семин А. В. Разработка и исследование рефлектометрических методов контроля волоконно-оптических направляющих систем связи в процессе их строительства и эксплуатации: дисс. … канд. техн. наук : 05.12.13 / А.В. Семин; С.-Петерб. гос. ун-т телекоммуникаций им. проф. М.А. Бонч-Бруевича. СПб., 2004.

6. Golay M. J. E. Complementary Series // Proc. of IRE Trans. of Inform. Theory. 1961. Vol. IT-7, No. 2. PP. 82–87.

7. Бычков В. Е., Мрачковский О. Д., Правда В. И. Особенности применения кодов Голея в радиолокации // Радиоэлектроника. 2008. № 4. С. 49–55.

УДК 621.391.63
ГРНТИ 49.44.31

ЭКСПЕРИМЕНТАЛЬНОЕ ИССЛЕДОВАНИЕ ОПТИЧЕСКОГО ВОЛОКНА CORNING TXF

М. С. Былина, О. А. Иванов

Санкт-Петербургский государственный университет телекоммуникаций им. проф. М. А. Бонч-Бруевича

Приведены результаты экспериментального исследования инновационного оптического волокна TXF со сниженным коэффициентом затухания и увеличенной площадью модового поля, разработанного компанией Corning в соответствии с рекомендацией G.654 Международного союза электросвязи.

одномодовое оптическое волокно, коэффициент затухания, площадь модового поля, волокно Corning TXF, вынужденное комбинационное рассеяние.

Инновационное одномодовое оптическое волокно (ОВ) марки TXF было представлено компанией Corning в 2016 году [1]. Заявленные производителем параметры TXF соответствуют рекомендации Международного союза электросвязи G.654E [2] (табл. 1). Основными преимуществами TXF являются сниженный коэффициент затухания в диапазоне длин волн 1525–1625 нм, достигнутый благодаря созданию сердцевины из чистого кварцевого стекла без легирующих примесей и усовершенствованной технологии производства [3], и увеличенный диаметр модового поля, что позволяет рекомендовать его для высокоскоростных сверхпротяженных волоконно-оптических линий передачи.

ТАБЛИЦА. 1. Параметры волокна марки TXF, производства Corning [1]

Параметр	Значение
Максим. коэффициент затухания α на длине волны 1550/1625 нм, дБ/км	0,17 / 0,19
Максим. изменение коэфф. затухания* в диапазоне 1525–1575 нм, дБ/км	0,02
Максим. изменение коэфф. затухания* в диапазоне 1550–1625 нм, дБ/км	0,03
Длина волны отсечки, нм	≤ 1520
Диаметр модового поля на длине волны 1550 нм, мкм	12,4 ± 0,5
Максим. хроматич. дисперсия на длине волны 1550/1625 нм, пс / (нм·км)	23 / 29

* по сравнению с коэффициентом затухания на длине волны 1550 нм

В первой части работы было проведено экспериментальное определение зависимости коэффициента затухания TXF от длины волны. Схемы измерения представлены на рис. 1 (см. ниже). При основном измерении излучение от широкополосного источника вводилось в исследуемое ОВ TXF. Излучение из исследуемого TXF поступало на оптический анализатор спектра ANDO AQ-6315C (*Optical Spectrum Analyzer*, OSA), который регистрировал зависимость уровня мощности y от длины волны λ. При опорном измерении излучение от широкополосного источника поступало на OSA, который регистрировал опорную зависимость уровня мощности y_{ref} от длины волны λ. В качестве широкополосных источников использовались лампа накаливания и шумы усиленного спонтанного излучения (*Amplified Spontaneous Emission*, ASE) усилителя EDFA.

Поскольку TXF согласно таблице 1 может иметь длину волны отсечки до 1520 нм, для обеспечения одномодового режима его работы на всех длинах волн, на которых проводились измерения, ввод и вывод излучения осу-

ществлялся через модовые фильтры. В качестве модового фильтра использовался пигтейл, изготовленный из стандартного одномодового ОВ марки SMF-28, которое имеет длину волны отсечки, не превышающую 1260 нм. Исследуемое TXF соединялось с модовыми фильтрами посредством сварных соединений.

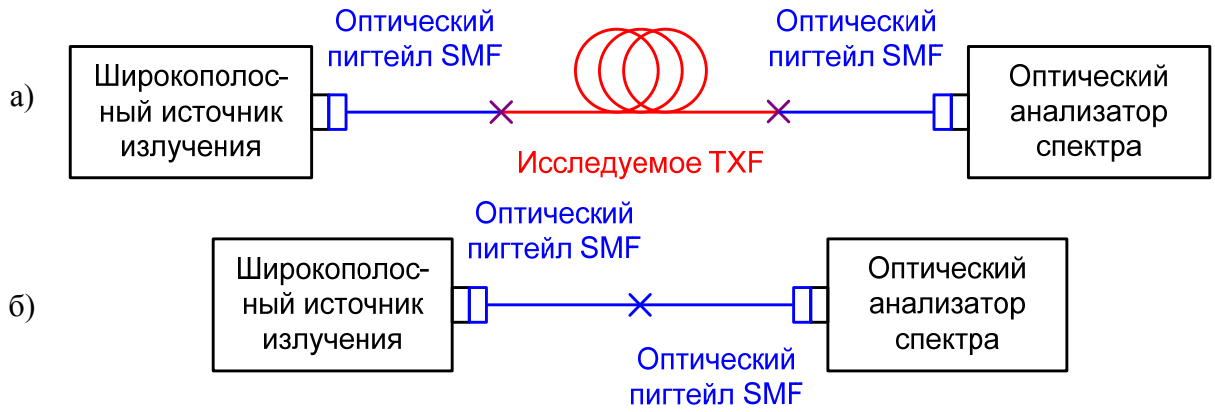


Рис. 1. Схемы измерения зависимости коэффициента затухания TXF от длины волны: а) основное, б) опорное

Коэффициент затухания α(λ) рассчитывался по результатам двух измерений следующим образом:

$$\alpha(\lambda) = \frac{y(\lambda) - y_{ref}(\lambda)}{L}, \qquad (1)$$

где L – длина исследуемого TXF.

Измерения проводились на двух образцах TXF длиной 25 и 50 км. Результаты измерений, представленные на рис. 2, подтвердили, что TXF обеспечивает сниженный коэффициент затухания. В диапазоне от 1525 до 1625 нм коэффициент затухания оказался меньше 0,2 дБ/км. Среднее затухание в *C*-диапазоне (1530–1565 нм) затухание составило около 0,172 дБ/км. Из рис. 2 (см. ниже) также видно, что TXF имеет выраженный «водяной» пик поглощения на длине волны 1383 нм.

Во второй части работы исследовалась усилительная способность TXF за счет вынужденного комбинационного рассеяния (ВКР).

Комбинационным рассеянием (КР) называют спонтанное нелинейное рассеяние фотона, происходящее при взаимодействии его с молекулой среды. В результате взаимодействия происходит спонтанное преобразование исходного фотона в комбинационно-рассеянный, энергия и частота которого с наибольшей вероятностью уменьшается, так как частично расходуется на увеличение энергии молекулы. В кварцевом ОВ частота рассеянного излучения оказывается на 13 ТГц меньше, чем исходного.

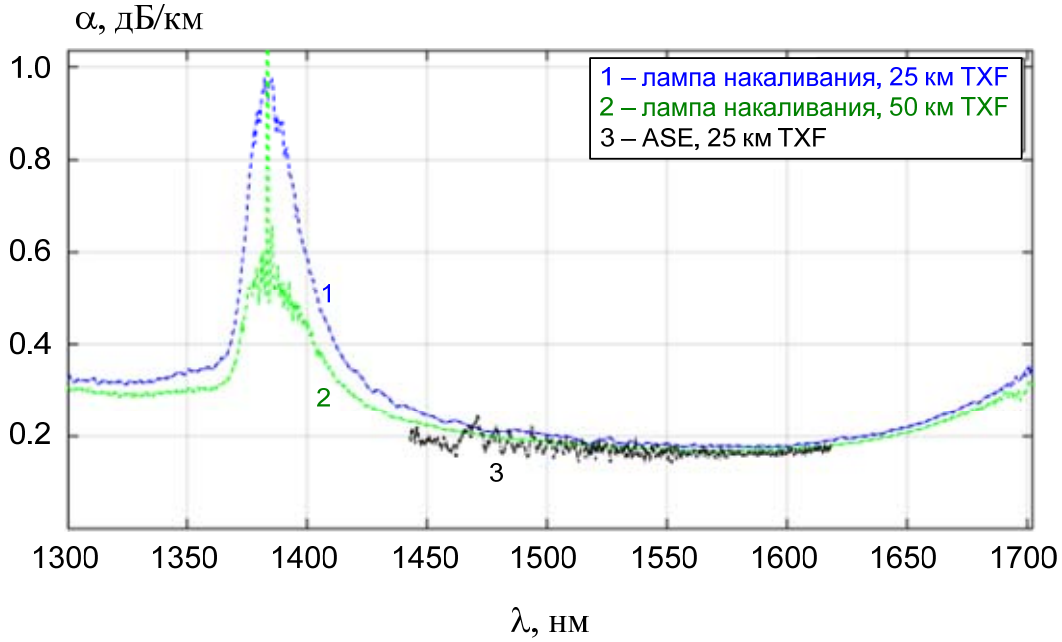


Рис. 2. Результаты измерения зависимости коэффициента затухания от длины волны

Если в ОВ одновременно распространяется мощное излучение накачки и слабое излучение сигнала, частота которого соответствует частоте рассеянного излучения накачки, то излучение сигнала будет стимулировать эффект КР. Возникнет ВКР, за счет которого произойдет усиление сигнала. На этом принципе основана работа оптического ВКР-усилителя.

Изменение мощностей сигнала P_S и попутной накачки P_P при распространении вдоль ОВ можно описать системой дифференциальных уравнений [4]:

$$\begin{cases} \mathrm{d}P_S/\mathrm{d}z = g_R P_P P_S / A_P - \alpha_S P_S \\ \mathrm{d}P_P/\mathrm{d}z = -g_R P_P \left(P_S + P_{ASE}\right)/A_S \cdot \left(\nu_P/\nu_S\right) - \alpha_P P_P \end{cases}, \quad (2)$$

где z – координата вдоль, g_R – коэффициент ВКР, ν_S и ν_P – частоты сигнала и накачки соответственно, α_S и α_P – коэффициенты затухания ОВ на частотах сигнала и накачки, A_S и A_P – площади модовых полей на частотах сигнала и накачки соответственно, P_{ASE} – мощность шумов ASE:

$$P_{ASE}(z) = \left(2h \cdot \nu_S \cdot F_n \cdot \Delta\nu + P_{ASE0}\right) \cdot G\,. \quad (3)$$

В (3) F_n – шум-фактор, h – постоянная Планка, $\Delta\nu$ – полоса оптического фильтра на выходе усилителя, G – коэффициент усиления, P_{ASE0} – мощность шумов на входе усилителя.

Если пренебречь истощением накачки, учитываемым первым членом второго уравнения (2), можно получить упрощенное аналитическое решение (2) в виде [4, 5]:

$$P_S(L) = P_{S0} \exp\left(g_R P_{P0} L_{eff}/A_P - \alpha_S L\right), \quad (4)$$

$$P_P(L) = P_{P0}\exp(-\alpha_P L),\ L_{eff} = \left(1-\exp\left(\mp\alpha_P L\right)\right)/\alpha_P\ , \quad (5)$$

$$G = P_S(L)/P_{S0} = \exp\left(g_R P_{P0} L_{eff}/A_P - \alpha_S L\right) \quad (6)$$

где $P_{S0} = P_S(0)$ и $P_{P0} = P_P(0)$ – мощности сигнала и накачки на входе ВКР-усилителя, L_{eff} – эффективная длина ОВ, на которой происходит оптическое усиление.

Если на вход ВКР-усилителя поступает только излучение накачки, то на его выходе возникнет шум ASE, который можно рассчитать по выражению [5]:

$$P_{ASE}(L) = \Gamma(1+k)\cdot\left[\Gamma_p\left(1+k, g_R P_P(L)/\alpha_P\right) - \Gamma_p\left(1+k, g_R P_P(L) e^{-\alpha_P L}/\alpha_P\right)\right]\times$$
$$\times 2h\nu_S\cdot\Delta\nu\cdot\left(1+\left(e^{h\cdot\Delta\nu/(K_B T)}\right)^{-1}\right)\cdot\left(g_R P_P(L)/\alpha_P\right)^{-k}\exp\left(g_R P_P(L)/\alpha_P\right), \quad (8)$$

где $k = \alpha_S / \alpha_P$, $\Gamma(x)$ и $\Gamma_p(x, y)$ – гамма-функция и неполная гамма-функция соответственно, K_B – постоянная Больцмана, T – абсолютная температура.

Если шум ASE на выходе ВКР-усилителя нам известен (измерен), то выражение (8) можно рассматривать как уравнение относительно g_R. Для его численного решения была разработана программа в среде Matlab.

Схема измерения представлена на рис. 3. Она включает следующее оборудование: источник накачки с длиной волны 1480 нм, широкополосный источник ASE EXFO FLS-2200, использовавшийся в качестве опорного сигнала, измерители оптической мощности Accelink PMSII-B 220-072017 и EXFO OHS-1700, мультиплексор WDM TF-1550/1480-025-1-00, два оптических разветвителя 1/99 %. Уровень мощности накачки изменялся в диапазоне от 23,6 до 31,5 дБм с шагом 1 дБ.

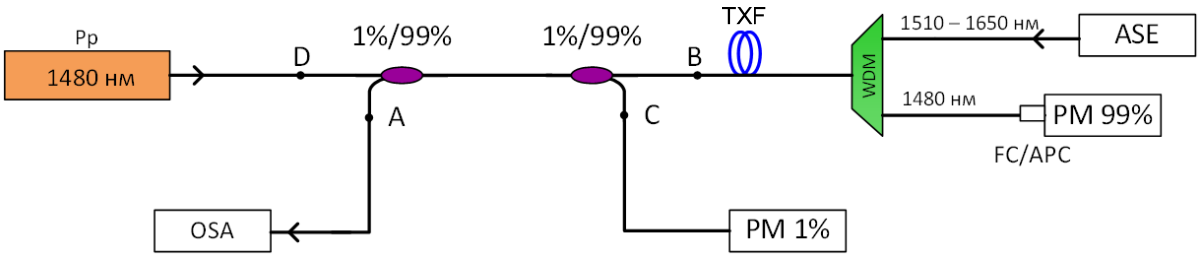


Рис. 3. Схема измерения усилительной способности TXF за счет ВКР

Для каждого значения мощности накачки определялись уровень накачки $P_P(L)$ на выходе ОВ по показаниям измерителя мощности PM 1 %, а также спектр шумов ASE с помощью OSA. Результаты измерений представлены на рис. 4. По результатам измерений с использованием разработанной программы был рассчитан коэффициент усиления ВКР (рис. 5).

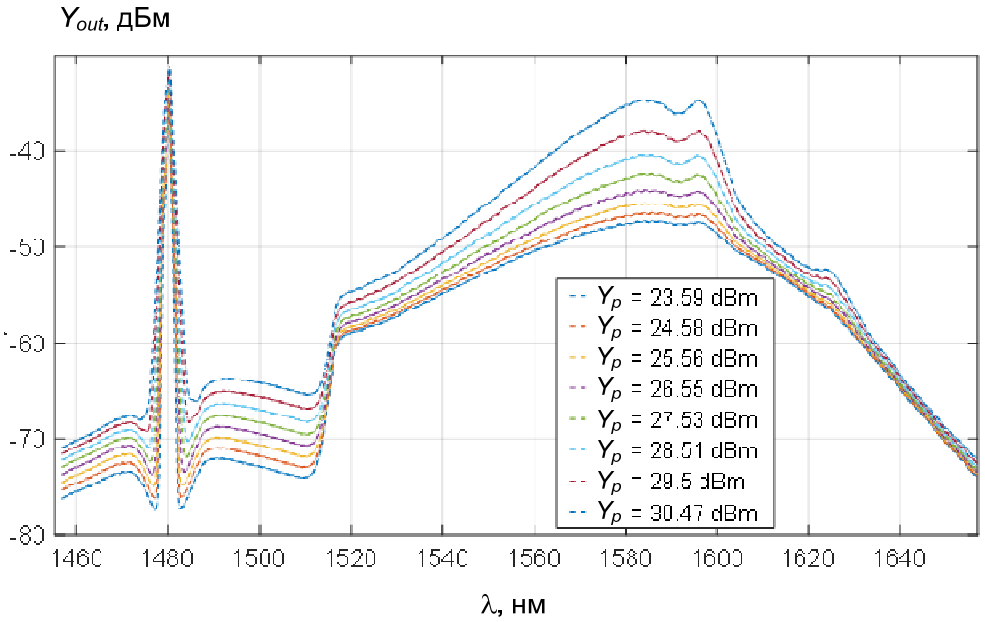


Рис. 4. Спектр излучения на выходе TXF

Из рис. 5 видно, что TXF обладает усилительной способностью и может быть использовано для создания распределенного ВКР-усилителя. Максимальный коэффициент усиления может быть получен для сигнала с частотой, на 13 ТГц меньшей частоты накачки

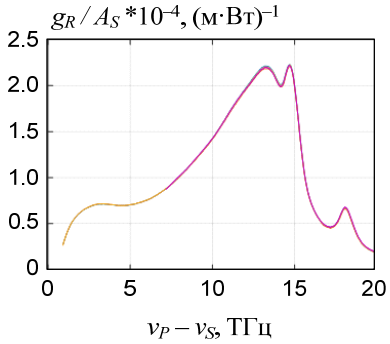


Рис. 4. Усилительная способность TXF

Список используемых источников

1. Corning® TXF™ optical fiber. Product information [Электронный ресурс] // Corning inc. 2017. 2 p. URL: https://www.corning.com/media/worldwide/coc/documents/Fiber/PI1433_10.17.pdf

2. ITU-T G.654 (11/2016) – Characteristics of a cut-off shifted single-mode optical fibre and cable. – Approved 2016. – Telecommunication Standardization Sector of ITU, 2016. 24 p.

3. Sergejs Makovejs [et al.] Towards Superior Transmission Performance in Submarine Systems: Leveraging UltraLow Attenuation and Large Effective Area // Journal of Lightwave Technology. 2016. Vol. 34, Iss. 1. PP. 114–120.

4. Bylina M., Glagolev S. Optical amplifiers for telecommunications // Proceeding of SPIE. Vol. 7026. PP. 702609-1–702609-7.

5. Андреев В. А., Дашков М. В. Рамановские усилители на волоконно-оптических линиях передачи. М. : Ириас, 2008. 219 с.

УДК 621.391.63
ГРНТИ 49.44.31

МЕТОДИКА РАСЧЕТА ШИРОКОПОЛОСНОСТИ ПОЛИМЕРНОГО МНОГОСЛОЙНОГО ВОЛОКНА

М. С. Былина, А. Н. Фомченко

Санкт-Петербургский государственный университет телекоммуникаций им. проф. М. А. Бонч-Бруевича

Многомодовые полимерные оптические волокна рекомендованы международными стандартами к использованию в локальных вычислительных сетях. Максимальная длина сегмента сети, построенной на таком волокне, оказывается ограниченной его межмодовой дисперсией. Представляет интерес применение полимерных волокон с многоступенчатым профилем показателя преломления, которые обеспечивают более высокую широкополосность по сравнению со ступенчатыми волокнами при относительно низкой стоимости.

многомодовое оптическое волокно, полимерное оптическое волокно, профиль показателя преломления, многослойное оптическое волокно, многоступенчатый профиль показателя преломления, межмодовая дисперсия, широкополосность.

Многомодовые полимерные оптические волокна (ПОВ) рекомендованы к использованию в локальных вычислительных сетях (ЛВС) со скоростями передачи до 1 Гбит/с [1]. Параметры ПОВ регламентирует стандарт IEC 60793-2-40, в котором описаны ПОВ с различными профилями показателя преломления (ППП) (табл. 1). Из табл. 1 видно, что ПОВ с многоступенчатым ППП имеют невысокую стоимость и хорошие оптические параметры, поэтому их применение в ЛВС представляет значительный интерес.

ТАБЛИЦА 1. Сравнительные характеристики ПОВ

Профиль показателя преломления	Широкополосность	Стоимость
ступенчатый	низкая	низкая
многоступенчатый	средняя	средняя
градиентный	высокая	высокая

Многоступенчатый ППП имеют ПОВ, сердцевина которых состоит из нескольких слоев полимерных материалов, которые в общем случае имеют разные толщину и показатель преломления (ПП). Известно, что наибольшей широкополосностью обладают многомодовые градиентные ПОВ с усеченным степенным ППП [2] сердцевины n_c:

$$n_c^2(r) = n_{c0}^2 \cdot \left[1 - 2\Delta \cdot \left(|r|/r_c\right)^q\right], \ |r| \le r_c, \qquad (1)$$

где r – расстояние от оптической оси ОВ, n_{c0} – ПП сердцевины на оптической оси ПОВ, r_c – радиус сердцевины ПОВ, $\Delta = \left(n_{c0}^2 - n_{cl}^2\right)/2n_{c0}^2$ – высота профиля, n_{cl} – ПП оболочки ПОВ, q – показатель профиля, обычно близкий к 2. Поэтому имеет смысл выбирать параметры слоев полимерного материала для многоступенчатого ПОВ так, чтобы при достаточно большом их количестве ППП приближался к (1). Возможны два принципа формирования ППП волокна, сердцевина которого состоит из N слоев: 1) создание слоев «равной высоты» (рис. 1а), в которых ПП двух соседних слоев отличаются на одну и ту же величину $\Delta n = \left(n_{c0} - n_{cl}\right)/N$; 2) создание слоев «равной толщины» (рис. 1б), в которых толщина каждого слоя составляет $\Delta r = r_c / N$. Для ПП n_{ci} и радиуса r_i слоя i справедливы выражения:

«равная высота» $$n_{ci} = n_{c0} - \Delta n \cdot i\,,\ r_i = r_c \cdot \left[\left(n_{c0}^2 - n_{ci}^2\right)/\left(n_{c0}^2 - n_{cl}^2\right)\right]^{1/q}. \quad (2)$$

«равная толщина» $$n_{ci} = n_{c0} \cdot \sqrt{1 - 2\Delta \cdot \left(r_i / r_c\right)^q}\,,\ r_i = \left(i+1\right) \cdot \Delta r\,. \quad (3)$$

Номер слоя i может меняться от 0 (центральный слой) до $N-1$ (слой, примыкающий к оболочке ПОВ).

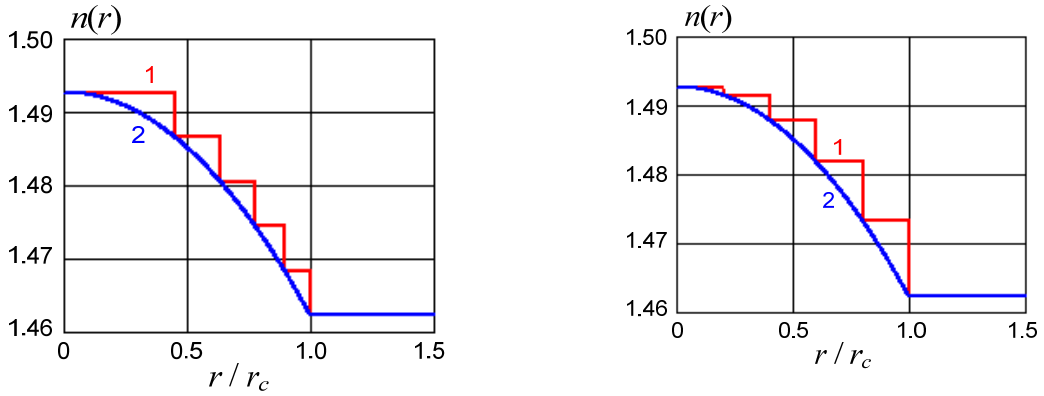


Рис. 1. Профили показателя преломления ПОВ (1 – многослойное, 2 – градиентное): а) слои «равной высоты», б) слои «равной толщины»

В [2] луч, распространяющийся в сердцевине многомодового волокна, предлагается характеризовать инвариантом β – скалярной величиной, определяющей его направление в любой точке траектории:

$$\beta = n_c \cos\theta_z\,, \quad (4)$$

Для направляемых лучей β удовлетворяет условию: $n_{cl} \le \beta \le n_{c0}$. В ступенчатом и градиентном ПОВ каждому значению инварианта β соответствует единственный луч. Удельное время распространения луча с инвариантом β на расстояние 1 км вдоль ПОВ определяется выражением [2, 3]:

$$\tau(\beta) = L_{opt}(\beta)/\left(c \cdot L_p(\beta)\right), \quad (5)$$

где c – скорость света в вакууме, $L_{opt}(\beta)$ и $L_p(\beta)$ – оптическая длина пути и полупериод траектории луча соответственно. Межмодовая дисперсия (МД) D_m и широкополосность W ПОВ определяются по выражениям [2, 3]:

$$D_m = \tau_{\max} - \tau_{\min}, \; W = 0,44/D_m, \tag{6}$$

где τ_{max} и τ_{min} – максимальное и минимальное удельные времена распространения, вычисляемые по всем направляемым лучам.

В ПОВ с многоступенчатым ППП каждому значению инварианта β в общем случае соответствует N_s направляемых лучей, где N_s – максимальное число слоев, которые может «посетить» луч (рис. 2). $N_s = 1$ только для лучей, испытывающих полное внутреннее отражение (ПВО) на границе центрального (0-го) и 1-го слоев. Для лучей, испытывающих ПВО на границе 1-го и 2-го слоев $N_s = 2$ и т. д. Для угла θ_{zi} между лучом с инвариантом β и осью ПОВ в слое i справедливо:

$$\cos\theta_{zi} = \beta/n_{ci}. \tag{7}$$

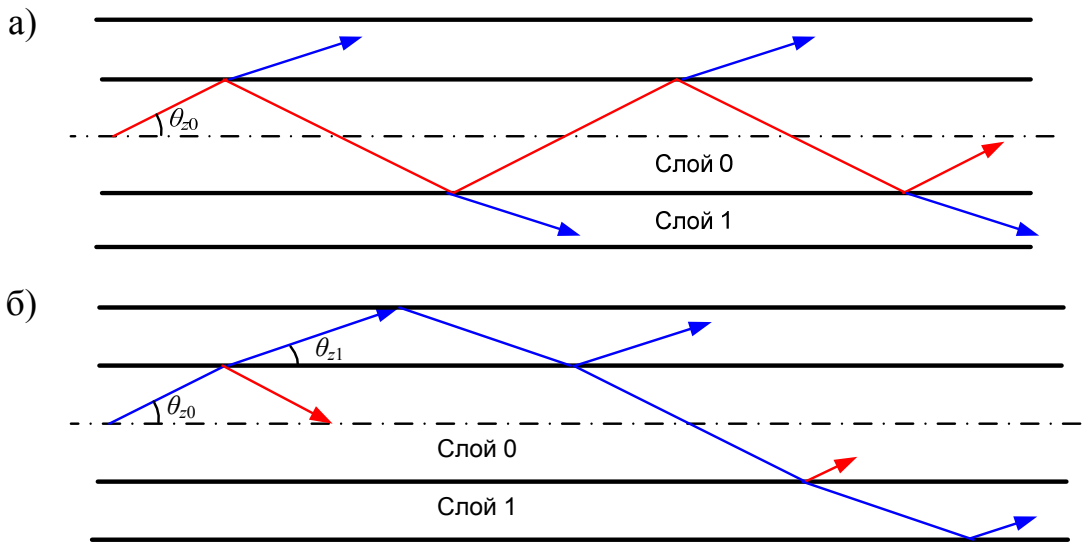


Рис. 2. Лучи в двухслойном волокне, характеризующиеся одним и тем же инвариантом:
а) луч, распространяющийся только в центральном слое,
б) луч, распространяющийся в обоих слоях

Очевидно, что направляемые лучи, соответствующие одному значению β будут иметь разное удельное время распространения. Для луча, испытывающего ПВО на границе слоев j и $j + 1$ оптическая длина пути и полупериод траектории, входящие в (5), определяются выражениями:

$$L_{opt\,j}(\beta) = \sum_{m=0}^{j} \frac{\Delta r_m \cdot n_{cmg} \cdot n_{cm}}{\sqrt{n_{cm}^2 - \beta^2}}, \; L_{pj}(\beta) = \sum_{m=0}^{j} \frac{\Delta r_m \cdot \beta}{\sqrt{n_{cm}^2 - \beta^2}}, \tag{8}$$

где Δr_m – толщина m-го слоя, n_{cmg} – групповой ПП m-го слоя. В (8) номер слоя j изменяется от 0 до $N_s - 1$.

При оценке параметров многослойного ПОВ для каждого значения β обычно учитывают только луч с номером $N_s - 1$ [4]. Однако расчет МД по выражению (6) с использованием этого приближения дает завышенные результаты, причем погрешность возрастает с увеличением числа слоев. Для уменьшения погрешности предлагается учитывать все направляемые лучи, которые несут значительную часть энергии. Для определения энергетических характеристик луча предлагается вычислять энергетические коэффициенты его отражения от каждой границы двух соседних слоев. Энергетический коэффициент отражения $R_{i\,(i+1)}$ от границы слоев i и $i + 1$ равен:

$$R_{i(i+1)} = 0{,}5\left(r^2_{i(i+1)p} + r^2_{i(i+1)s}\right), \tag{9}$$

$$r_{i(i+1)p} = \frac{\mathrm{tg}\left(\theta_{z(i+1)} - \theta_{zi}\right)}{\mathrm{tg}\left(\theta_{z(i+1)} + \theta_{zi}\right)},\ r_{i(i+1)s} = \frac{\sin\left(\theta_{z(i+1)} - \theta_{zi}\right)}{\sin\left(\theta_{z(i+1)} + \theta_{zi}\right)}, \tag{10}$$

где $r_{i\,(i+1)\,p}$ и $r_{i\,(i+1)\,s}$ – коэффициенты отражения от границы слоев i и $i + 1$ по напряженности для излучения, поляризованного в плоскости и перпендикулярно плоскости падения соответственно. Мощность P_j, переносимую лучом, испытывающим при распространении отражение от границы слоев j и $j + 1$ ($0 \le j \le N_s - 1$), можно рассчитать по выражению:

$$P_j / P = \left(\prod_{i=0}^{j-1} T^2_{i\,i+1} \cdot R_{j\,j+1}\right)^{INT\left[L/L_{pj}\right]}, \tag{11}$$

где P – общая мощность, переносимая направляемыми лучами в ПОВ, L – длина ПОВ, INT – функция, означающая целую часть числа.

На рис. 3 (см. ниже) представлены результаты расчета зависимости удельного времени распространения от величины инварианта для ПОВ с числом слоев 5 и 20. Основным материалом сердцевины ПОВ был выбран полиметилметакрилат (ПММА), ПП которого можно описать уравнением Селлмейера:

$$n_{c0}(\lambda) = \sqrt{\sum_{i=0}^{N} \frac{A_i \cdot \lambda^2}{\lambda^2 - \lambda_i^2} + 1}, \tag{12}$$

где A_i и λ_i – коэффициенты аппроксимации, значения которых приведены в таблице 2, $N = 3$ – число слагаемых, λ – длина волны. Числовая апертура ПОВ на оптической оси была выбрана равной 0,3. Полагалось, что высоты слоев Δn_i и числовая апертура не зависят

ТАБЛИЦА. 2. Коэффициенты аппроксимации для (8) [3]

A_0	8,51149
λ_0, мкм	12,1885
A_1	1,47329
λ_1, мкм	0,09247
A_2	–0,11807
λ_2, мкм	$1{,}7 \cdot 10^{-9}$
A_3	–0,13311
λ_3, мкм	$3{,}6 \cdot 10^{-9}$

от длины волны. Все расчеты проводились на длине волны 0,65 мкм, расположенной в одном из окон прозрачности ПММА. При расчете учитывались направляемые лучи, мощность которых составляла не менее 10 % P. Расчет проведен для ПОВ со слоями равной высоты, так как авторами установлено, что оно имеет меньшую МД, чем ПОВ с тем же числом слоев равной толщины.

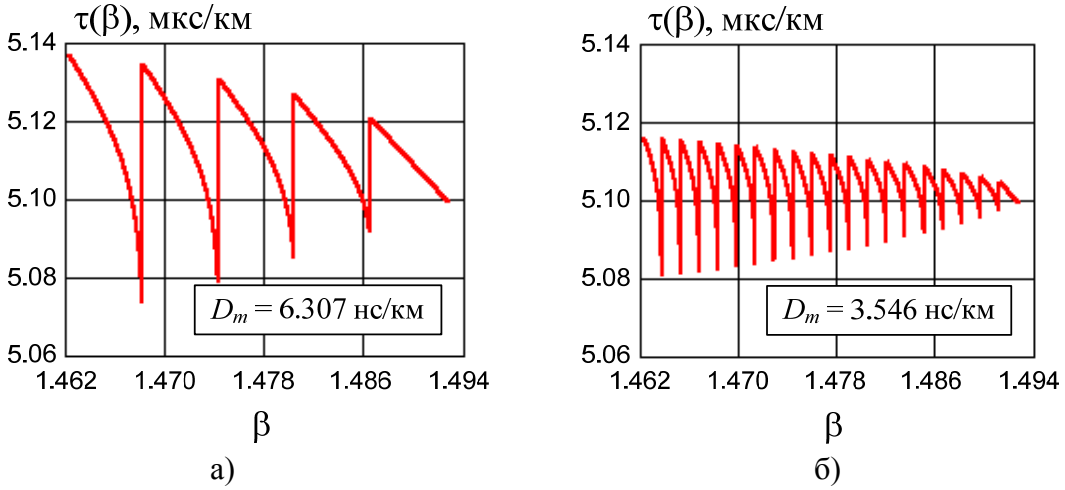


Рис. 3. Удельное время распространения направляемых лучей в многослойном ПОВ с 5-ю (а) и 20-ю (б) слоями равной высоты

На рис. 4 представлены результаты расчета зависимости МД и широкополосности многослойных ПОВ с сердцевиной из ПММА со слоями равной высоты от числа слоев. Для сравнения на рисунке показаны соответствующие параметры ступенчатого ПОВ и градиентного ПОВ с усеченным параболическим ППП. Из рисунка видно, что с увеличением числа слоев параметры многослойного ПОВ постепенно приближаются к параметрам градиентного ПОВ.

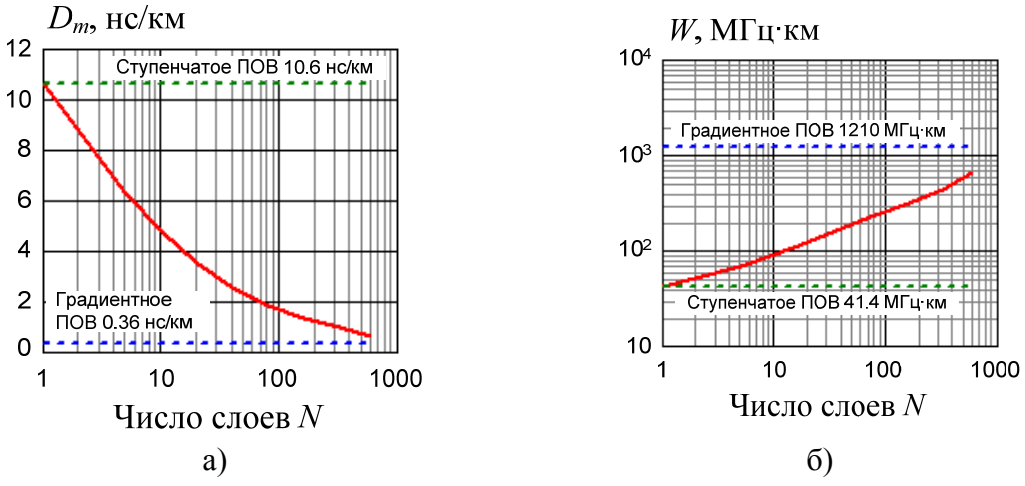


Рис. 4. Зависимости межмодовой дисперсии и широкополосности многослойного ПОВ с сердцевиной из ПММА от числа слоев

Проведенные расчеты позволяют оценить предельные возможности многослойных ПОВ по дисперсии. Из рис. 4 видно, что для ЛВС со скоростью передачи 1 Гбит/с и максимальной длиной сегмента 100 м достаточно иметь ПОВ, состоящее из 12 слоев.

Список используемых источников

1. IEEE 802.3bv Physical Layer Specifications and Management Parameters for 1000 Mb/s Operation Over Plastic Optical Fiber.

2. Снайдер А., Лав Дж. Теория оптических волноводов : пер. с англ. М. : Радио и связь, 1987. 656 с.

3. Былина М. С., Воробьева Т. С., Глаголев С. Ф. Возможность использования полимерных волокон в локальных вычислительных сетях // Фотон-Экспресс. 2008. N 7–8. С. 38–40.

4. Olaf Ziemann, Jurgen Krauser, Peter E. Zamzow, Werner Daum. POF Handbook. Optical Short Range Transmission Systems. Second edition. – Berlin, Springer, 2008. P. 902.

УДК 004.056.53
ГРНТИ 81.93.29

МЕТОДИКА ОБНАРУЖЕНИЯ ВРЕДОНОСНОЙ ИНФОРМАЦИИ В ИНФОРМАЦИОННОМ ПРОСТРАНСТВЕ СОЦИАЛЬНЫХ СЕТЕЙ

К. А. Валиева[1], Л. А. Виткова[1,2], Е. В. Смирнов[1]

[1]Санкт-Петербургский государственный университет телекоммуникаций им. проф. М. А. Бонч-Бруевича
[2]Санкт-Петербургский институт информатики и автоматизации Российской академии наук

Наибольшая острота проблемы обнаружения вредоносной информации проявляется при попытках распознавания целевых информационных каналов, траекторий распространения контента, и снижении негативного влияния подобной информации на субъекты (индивидуальных или коллективных, например, на человека, семью, группу или организацию). В работе представлен анализ некоторых существующих систем обработки сетевого контента и возможности их применения в рамках методики обнаружения вредоносной информации. Результатом работы методики является повышение уровня защищенности пользователей от вредоносной информации в социальных сетях.

вредоносная информация; мониторинг; сетевой контент; система обработки; сервисы сетевой аналитики.

В современном мире Интернет стал одним из главных информационных ресурсов, а социальные сети являются одной из самых используемых информационных площадок во всем мире. Пользователи могут свободно

и удобным образом высказывать свое мнение, делиться информацией с окружающими. Это дает основания утверждать, что социальные сети могут являться не только средством для общения, но и инструментом распространения информации практически любого характера, в том числе и вредоносного [1].

Под вредоносной понимается информация, не являющаяся конфиденциальной, но обуславливающая необходимость охраны и защиты прав и законных интересов личности, общества и государства в силу возможного вреда, который нанесет этим субъектам ее распространение (применение). Она может быть выражена в виде рекламы товаров, услуг или фирм, политических или экономических заказов в плане информационного устранения конкурента или наоборот, продвижение заказанного лица, фирмы, информационного ресурса, и т. д. [2].

К вредоносной информации можно условно отнести пять основных категорий:

1) информацию, направленную на *разжигание ненависти, вражды и насилия* (в том числе возбуждающую социальную, расовую, национальную или религиозную ненависть, вражду, превосходство, рознь, нетерпимость; информацию, содержащую призывы к войне) [3];

2) ложную информацию (в том числе недобросовестную, недостоверную, заведомо ложную рекламу – из ФЗ «О рекламе» от 13.03.2006 №38-ФЗ) [4];

3) информацию, содержащую *посягательства на честь, доброе имя и деловую репутацию* других лиц [5];

4) *непристойную информацию* (в том числе порнографию, неэтичную рекламу);

5) информацию, оказывающую *деструктивное воздействие на здоровье людей* (в том числе рекламу со скрытыми вставками) [6].

На сегодняшний день существует множество факторов, способствующих массовому распространению вредоносной информации в социальных сетях. Задача противодействия этим явлениям крайне актуальна. В ее основе лежит мониторинг и анализ социальных сетей (понимание и оценка процессов за счет сбора и систематизации данных), моделирование и методы предсказания (выявление авторов и путей распространения информации), а также методы управления медиа пространством (приведения сети в требуемое состояние) [7].

На данный момент в свободном доступе существует множество мониторинговых систем, направленных на аналитику социальных сетей, которые могут быть использованы для обнаружения вредоносной информации. Примерами могут служить Semanticforce, IQBuzz, YouScan, SCAN, Babkee, Angry Analytics, и др. Рассмотрим подробнее первые три сервиса с точки зрения пригодности для поиска вредоносной информации.

Semanticforce это платформа для мониторинга и анализа интернет СМИ, социальных сетей, видео, форумов, блогов и других видов онлайн-медиа. После задания поискового запроса она позволяет указать три типа слов: якорные (дословный поиск), контекстные (некий фильтр, накладывающийся на якорные слова) и стоп-слова (исключаемые результаты). При выдаче результатов под каждым источником указывается окно разметки, в нем могут быть указаны категории, теги, тональность (позитив и негатив). При поиске и анализе информации на предмет вредоносности такие возможности позволят сократить итоговую выборку и более объективно оценивать посыл, заложенный в контент [8].

Сервис IQBuzz предоставляет возможность задания рубрик для поиска информации, внутри которых существует возможность настроить сортировку поиска по ключевым словам, которые должны встречаться в тексте, а также тех, которых быть не должно. Также, существует возможность выставить параметры анализа, такие как персоны, организации, даты и время, деньги и др. Подобный инструментарий удобен для поиска вредоносных данных, так как позволяет анализировать информацию адресно, применительно к конкретным людям или фирмам, а также дает возможность конкретизировать рамки поисковых запросов. Отчеты представлены графически, с возможностью настроек различных отображений, что позволяет детально изучить их на предмет вредоносности контента и получить статистику по активности темы [9].

В сервисе YouScan также существуют фильтры запросов, возможности графического отображения результатов и их эмоциональная оценка. Особенностью YouScan является возможность анализировать не только контент, но и авторов. Отобразив источники, публикующие определенную информацию, с наибольшим количеством подписчиков, можно выявить лидеров мнений, и оценить их тональность. Помимо смешанных мнений, они могут как высказываться негативно в сторону конкретных лиц, организаций или социальных групп, тем самым разжигая враждебное отношение или нетерпимость, так и демонстрировать положительное мнение о некоторых заказанных товарах, ресурсах или лицах, тем самым порождая их продвижение и лидирование над конкурентами [10].

На основе всего этого можно сделать выводы, что существующие сервисы сетевой аналитики могут служить удобными инструментами для поиска вредоносной информации, ее источников и путей распространения.

Сформулируем и рассмотрим сущность этапов методики обнаружения вредоносной информации в информационном пространстве социальных сетей:

1. Формулировка система запросов. Данный процесс является крайне важным, поскольку от качества сбора информации зависит конечная стати-

стика. Чрезмерный сбор информации, который может произойти, если данный процесс плохо отлажен будет существенно затруднен повторами и анализом данных, представляющими собой «информационный шум», т. е. бесполезной. В связи с этим процесс сбора данных должен быть исполнен максимально точно, т. е. необходимо иметь четкое представление об исследуемой области, а также иметь предельно корректно сформулированную систему запросов.

Рассмотренные ранее сервисы сетевой аналитики позволяют на этапе формировании запроса выставить нужные фильтры, указать категории и использовать ключевые слова, чтобы исключить из финальной выборки те результаты, которые могут быть схожи по некоторым фразам, но относится к другой тематике. Например, по запросам: «мы лучше всех», «ненавижу», «превосходство» − можно найти художественные фильмы не несущие розни, поэтому представляется разумным исключить из выборки публикации, содержащие слово «фильм».

2. Поиск вредоносной информации. Данный этап полностью возложен на сервисы сетевой аналитики, которые за счет собственных, индивидуальных механизмов работы, по обозначенным входным запросам производят сбор данных, присваивают им категории, теги и тональность, строят различные графики. Выводимые данные могут отличаться, в зависимости от выбранного инструмента анализа.

3. Анализ полученных данных. Получаемая в результате информация представлена в виде списка публикаций, в котором можно оставлять свои пометки, формировать собственные категории, перестраивать его по определенным параметрам, например, вывести только тот контент, который имеет негативную эмоциональную оценку.

При анализе данных происходит изучение собранного контента и принятие решения по каждой публикации с присвоением ей определенной подкатегории. Для облегчения этого используются инструменты, которые предоставляет сервис, но их применение полностью зависит целей анализа. Так, например, при исследовании информации связанной с враждой или превосходством можно использовать отображение авторов географически, а изучая данные связанные с неэтичной рекламой, можно использовать сочетание поиска по ключевым славам внутри собранной выборки и негативного отношения авторов публикаций.

4. Обработка вредоносной информации. Данный этап зависит от целей использования методики. В нем предполагается принятие мер, способствующих удалению вредоносного контента из пространства социальных сетей, а также другие операции, связанные с отслеживанием путей его распространения или поиском его источников. Так, с помощью сортировки по авторам с наибольшим количеством подписчиков, можно обнаружить лидеров мне-

ний, а используя аналитику ссылок, можно выявить первоисточник, на какой ссылаются т. н. ретрансляторы постов, распространяющие, но не генерирующие подобный контент.

Для устранения из пространства социальных сетей вредоносного контента существуют различные варианты, например, самым простым представляется обращение к администрации социальной сети с требованием заблокировать информацию и/или ее источники. Также, существует возможность законодательно заблокировать авторов или сообщества через судебную систему.

Представленная методика может быть использована в настоящий момент для решения задач обнаружения вредоносной информации в пространстве социальных сетей за счет сервисов сетевой аналитики, даже несмотря на их коммерческую направленность. Невзирая на то, что в их основе лежит задача отслеживания имиджа лица или бренда, инструменты, которые для этого предлагаются, подходят и для целей сетевой аналитики.

Методика может быть реализована в интересах оперативных структур управления политикой борьбы с нежелательной, сомнительной и вредоносной информацией, а также может найти свое применение при использовании частными лицами с целью обезопасить себя или свою деятельность от распространения недобросовестной информации о них или посягательств на репутацию.

Работа выполнена при частичной финансовой поддержке Российского научного фонда (проект № 18-71-10094) в СПИИРАН.

Список используемых источников

1. Головлева Ю. А., Виткова Л. А., Ковцур М. М., Дмитриева Е. В. Конвергенция информационных технология для повышения эффективности управления информационным пространством Санкт-Петербурга // Информационная безопасность регионов России (ИБРР-2017) : материалы конференции. 2017. С. 510–512.

2. Виткова Л. А., Проноза А. А., Сахаров Д. В., Чечулин А. А. Проблемы безопасности информационной сферы в условиях информационного противоборства // Актуальные проблемы инфотелекоммуникаций в науке и образовании (АПИНО 2018). VII Международная научно-техническая и научно-методическая конференция : сб. науч. ст. в 4-х т. СПб. : СПбГУТ, 2018. С. 191–195.

3. Федеральный закон от 27.07.2006 № 149-ФЗ «Об информации, информационных технологиях и о защите информации» [Электронный ресурс]. Режим доступа: http://www.consultant.ru/document/cons_doc_LAW_61798/ (дата обращения 11.03.2020).

4. Федеральный закон от 13.03.2006 N 38-ФЗ «О рекламе» [Электронный ресурс]. – Режим доступа: http://www.consultant.ru/document/cons_doc_LAW_58968/ (дата обращения 11.03.2020).

5. Закон РФ от 27.12.1991 № 2124-1 «О средствах массовой информации» [Электронный ресурс]. – Режим доступа: http://www.consultant.ru/document/cons_doc_LAW_1511/ (дата обращения 11.03.2020).

6. Федеральный закон от 29.12.2010 № 436-ФЗ «О защите детей от информации, причиняющей вред их здоровью и развитию» [Электронный ресурс]. Режим доступа: http://www.consultant.ru/document/cons_doc_LAW_108808/ (дата обращения 11.03.2020).

7. Виткова Л. А., Дойникова Е. В. Поддержка принятия решения по противодействию нежелательной информации // Информационные технологии в управлении (ИТУ-2018) : материалы конференции. 2018. С. 398–403.

8. SemanticForce – Система мониторинга социальных медиа и онлайн-СМИ [Электронный ресурс]. – Режим доступа: http://www.semanticforce.net/ru/ (дата обращения 14.03.2020).

9. IQBuzz – Сервис для мониторинга социальных медиа [Электронный ресурс]. Режим доступа: http://iqbuzz.pro/ (дата обращения 14.03.2020).

10. YouScan – Система мониторинга социальных медиа и социальных сетей [Электронный ресурс]. Режим доступа: https://youscan.io/ru/ (дата обращения 14.03.2020).

Статья представлена доцентом кафедры ЗСС СПбГУТ, кандидатом технических наук А. А. Браницким.

УДК 654.1
ГРНТИ 49.34.06

НЕЙРОСЕТЕВАЯ САМООБУЧАЮЩАЯСЯ МОДЕЛЬ ПРОГНОЗИРОВАНИЯ НАГРУЗКИ КОНТАКТ-ЦЕНТРА

Н. И. Васылив[1], С. В. Кисляков[1,2]

[1]Санкт-Петербургский государственный университет телекоммуникаций им. проф. М. А. Бонч-Бруевича
[2]ООО «НТЦ Аргус»

Работа посвящена исследованию нейросетевой модели прогнозирования количества поступающих вызовов в контакт-центр. Для расчета оптимальных параметров модели использованы выгрузки реальных входных нагрузок контакт-центров. Актуальность решаемой задачи обуславливается пониманием того, что поступающая нагрузка определяет количество привлекаемых к работе операторов, что в свою очередь определяет затраты на оплату труда операторов. Для обеспечения необходимого качества обслуживания при минимальном числе операторов контакт-центра необходимо заранее знать (или прогнозировать с максимально возможной точностью) число входящих вызовов. Настоящая работа посвящена анализу зависимости параметра качества предсказания рекуррентной нейросетевой модели от объёма исторических данных (входящих вызовов). Такая, казалось бы, простая постановка задачи исследования, позволяет ответить на вопрос: сколько времени потребуется работать модели, чтобы достигнуть максимального качества предсказания, и каковы могут быть при этом финансовые потери (или выигрыши) самого контакт-центра.

колл-центр, оператор, нейронные сети, LSTM, прогнозирование.

Введение

При создании контакт-центра всегда необходимо знать предполагаемую нагрузку в виде количества поступающих вызовов за единицу времени. Это поможет грамотно распределить ресурсы, как сетевые, так и человеческие, в смысле количества операторов, обслуживающих вызовы. Исходя из нагрузки можно знать сколько операторов должно быть нанято в контакт-центр и выведено в работу. Чем точнее мы знаем какая нагрузка поступает на контакт-центр, тем большая вероятность задействовать необходимое количество операторов соответственно нагрузке, следовательно, обслужить вызовы с заданным качеством и грамотно распределить денежные ресурсы на оплату труда. Это значит, что экономия денежного ресурса зависит о того, как точно предсказана нагрузка за определенный промежуток времени. Причем чем меньший промежуток времени и точней прогноз, тем мы лучше знаем сколько нужно операторов и сколько должны заплатить за часы их работы.

Сейчас существует большое количество методов решения задач предсказания. Помимо моделей для решения задач предсказания временных рядов [1] применяются также и регрессионные модели [2]. Среди предсказательных методов того и иного типа для предсказания нагрузки могут быть использованы, например, модели типа Holt-Winters' Method, учитывающие тренд и сезонную составляющую, и ARIMA [3].

Современной теоретической альтернативой таким методам прогнозирования могут быть Deep Learning (глубокое обучение) методы прогнозирования, в частности LSTM [4] нейронные сети. Считается, что такие модели могут давать результаты лучше, чем обычные регрессионные и предсказательные методы [1].

Постановка задачи

Исходный набор данных выглядит как представлено на рис. 1. Требуется построить нейросетевую модель и, обучая ее на известных данных, выяснить, какой объем исторических данных требуется для введения модели в эксплуатацию.

	Начало временного интервала	Количество поступивших вызовов в очередь
01.01.16	00:00 - 00:15	39
01.01.16	00:15 - 00:30	39
01.01.16	00:30 - 00:45	56
01.01.16	00:45 - 01:00	56
01.01.16	01:00 - 01:15	46
01.01.16	01:15 - 01:30	46
01.01.16	01:30 - 01:45	36
01.01.16	01:45 - 02:00	36

Рис. 1. Количество поступивших вызовов за первые 2 часа

В нейронную сеть будут поступать последовательно только значения нагрузки, то есть временные интервалы, представленные в виде каждых пятнадцати минут работы контакт-центра. Нейронная сеть будет настраивать веса исходя из подаваемой обучающей выборки, а на тестовой выборке мы выясним насколько хорошо работает модель. В итоге построим

предсказание и сравним с реальными данными. В качестве критерия оценки обучения нейросети мы возьмем такой показатель как среднеквадратическая ошибка (*Mean Squared Error, MSE*) (1):

$$MSE = \frac{1}{n}\sum_{i=1}^{n}(\hat{y}_i - y_i)^2 \quad (1)$$

где y_i – i-е значение из выборки, $\hat{y}_i$ – i-е значение, возвращенное моделью, n – количество значений.

Первый показывает, как отличается выходное значение нейронной сети от реального, а второй на сколько хорошо работает модель, где отрицательное значение будет показывать неправильность работы сети. Нулевое значение отображать эталонную модель. А единица – идеальную модель. Для написания кода нейронной сети используем библиотеку Keras, средой проектирования будет платформа Colaboratory от Google.

Анализ временного ряда и построение модели

Так как данные нагрузки меняются во времени, задачу можно характеризовать как задачу прогнозирования временного ряда. Перед тем, как составить модель для прогнозирования временной ряд следует привести к стационарности. Стационарность ряда обуславливается отсутствием таких характеристик временного ряда как тренд, сезонность и цикличность [5]. Для того чтобы понять стационарен ли ряд используется тест Дикки-Фуллера [5]. Для того чтобы заранее убрать недельную и месячную сезонность в году, уменьшить время обучения модели, и удобства работы с данными, было решено выделить среди всей выборки только понедельники. После отделения понедельников был проведен тест Дикки-Фуллера, по итогу которого, выяснилось, что этого было достаточно для приведения ряда к стационарности, значение *p-value* = $2{,}906694*10^{-30}$ Ряд может считается стационарным при значениях *p-value* < 0,01 [5] .

Построение модели. Модель архитектурно состоит из двух LSTM слоев с конечным полносвязным стандартным слоем для свертки в массив размерности (1:96) по числу пятнадцатиминутных интервалов в сутках. Используется активационная функция ReLu. Особенность модели состоит в том, что используются слои dropout [6] и earlystopping [7] между слоями нейронов, и LSTM слои находятся в состоянии stateful [6]. В нейронную сеть для обучения и получения промежуточных результатов будут подаваться значения трех понедельников на обучение и одному на отклик со смещением в один понедельник. Соответственно, начиная с четвертой недели, модель начинает обучаться на реальных данных, настраивается, далее происходит смещение на одну неделю, модель обучается на значениях понедельников со второй по четвертую неделю со значениями отклика пятой недели и так далее. Массив значений последнего понедельника будет взят для сравнения с предсказанием нейронной сети.

Результаты работы нейронной сети и предсказание

После получения результатов и отображения их на графиках, можем заметить, что в ходе обучения, нейронная сеть не достигла минимальной ошибки, однако очень приблизилась к этому значению. Если ошибка и растет на последних эпохах, то не значительно - на графике заметить это получится с трудом (рис. 2). Тем не менее ошибка уменьшается по ходу всего обучении и нет точки, в которой можно сказать, что ошибка достигла минимума.

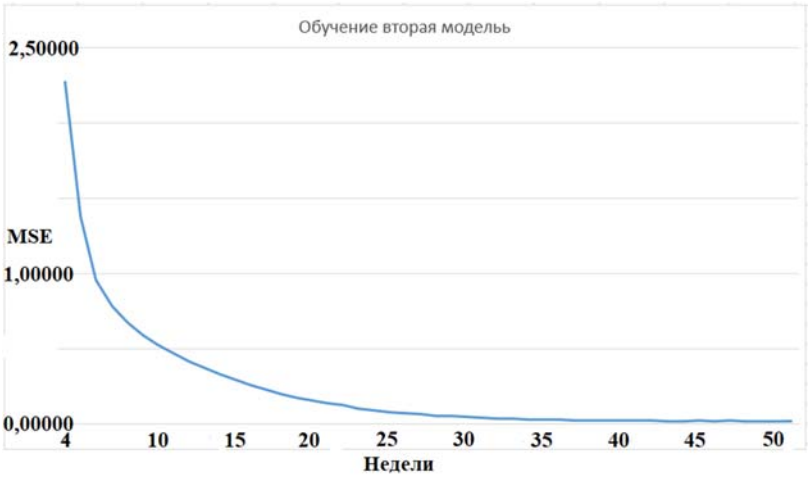


Рис. 2. Результаты обучения

Построим прогноз на последний понедельник в году и сравним с реальными значениями (рис. 3, см. ниже). Несмотря на то, что значения, полученные от нейронной сети, изменяются не так же линейно, как реальные, нейронная сеть верно отражает суточный тренд с определенной ошибкой. Среднеквадратическая ошибка, полученная от сравнения реальных значений понедельника и предсказанного, получилась равной 0,05868. Соотнеся со значениями ошибок, полученными на обучении, она находится между 24 (*MSE* = 0,0685) и 25 (*MSE* = 0,057) неделями.

Выводы

Из текущих результатов можно сделать вывод, что для ввода в эксплуатацию модели необходимы реальные значения за год. Тем не менее после определенного момента в обучении значение ошибки начинает снижаться слабее. Из соотнесения полученной среднеквадратической ошибки при предсказании и ошибками при обучении, можно сделать вывод о том, что с 25 недели модель можно вводить в эксплуатацию, не дожидаясь конца обучения, но и не заканчивая его. На данном этапе можно сказать о том, что при решении поставленной задачи более целесообразно использовать несколько LSTM слоев рекуррентной нейронной сети с stateful состоянием

и dropout слоями (четвертая модель), а также метод early stopping. В дальнейших исследованиях следует ввести методику работы с большим количеством данных, для анализа не только на понедельниках, но и на всех значениях в году. Также следует понять, есть ли возможность и как сократить время на обучение модели, действительно ли необходимо ждать полгода для введения модели в работу.

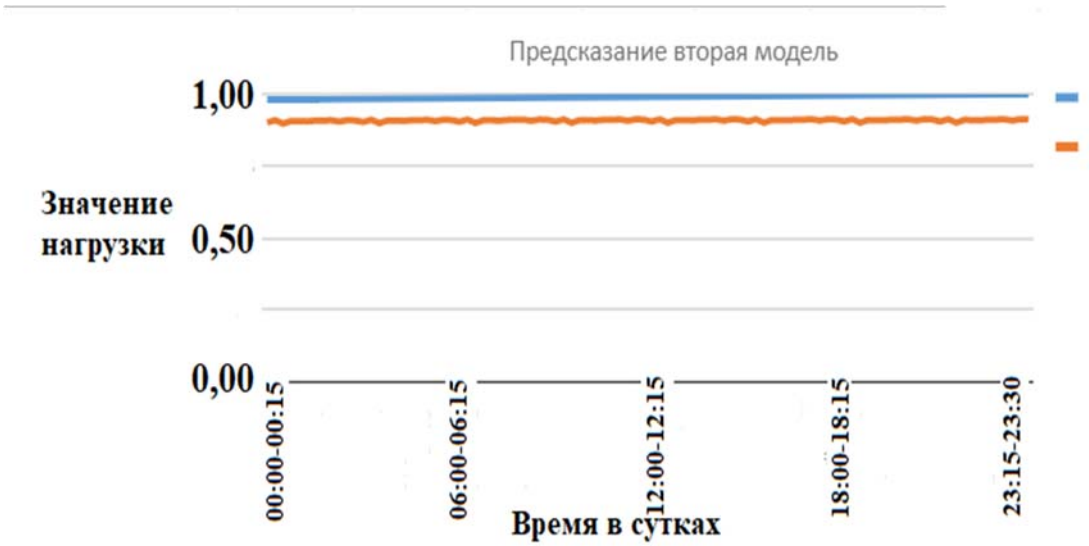


Рис. 3. Результаты предсказания: верхняя линия отражает реальные значения нагрузки, нижняя – предсказание нейронной сети

Список используемых источников

1. Youru Li, Zhenfeng Zhu, Deqiang Kong, Hua Han, Yao Zhao. EA-LSTM: Evolutionary Attention-based LSTM for Time Series Prediction [Электронный ресурс] // Knowledge-Based Systems: электрон. науч. журн. 2018. N 181. С. 104785–104794. URL: https://www.sciencedirect.com/science/article/abs/pii/S0950705119302400(дата обращения 15.02.2020).

2. Фёрстер Э., Рёнц Б. Методы корреляционного и регрессионного анализа. Руководство для экономистов : пер. с нем. и пред. В. М. Ивановой. М. : Финансы и статистика, 1983. 304 с.

3. Mathijs Jansen. Call Centre Forecasting : MasterThesis : 01.04.2010 / Тилбург, 77 с.

4. S. Hochreiter, J. Schmidhuber. Long short-term memory // Neural computation 1997. N 9. PP. 1735–1780.

5. Brownlee J. Introduction to Time Series Forecasting with Python: How to Prepare Data and Develop Models to Predict the Future. Machine Learning Mastery, 2017. 367 с.

6. Brownlee J. Better Deep Learning: Train Faster, Reduce Overfitting, and Make Better Predictions. Machine Learning Mastery, 2018. 575 с.

7. Brownlee J. Deep Learning with Python: Develop Deep Learning Models on Theano and TensorFlow Using Keras. Machine Learning Mastery, 2017. 245 с.

УДК 004.75
ГРНТИ 50.41.17

ИССЛЕДОВАНИЕ ПРОИЗВОДИТЕЛЬНОСТИ ОТКАЗОУСТОЙЧИВОГО ПРОГРАММНО-КОНФИГУРИРУЕМОГО ХРАНИЛИЩА В ГИПЕРКОНВЕРГЕНТНЫХ СИСТЕМАХ

А. В. Васюткин, А. А. Швидкий

Санкт-Петербургский государственный университет телекоммуникаций им. проф. М. А. Бонч-Бруевича

В статье приведены основные свойства и функции программно-конфигурируемых хранилищ, описаны параметры оценки производительности и выявлены узкие места SDS. Рассмотрена архитектура реализации SDS – Ceph. Приведены результаты тестирования производительности Ceph кластера в качестве основной системы хранения данных виртуальных машин.

гиперконвергентная инфраструктура, распределённая система хранения данных, программно-конфигурируемое хранилище.

В настоящее время большую популярность получили гиперконвергентные инфраструктуры. Программно-конфигурируемые хранилища, как одна из основных составляющих таких инфраструктур, стали основными системами хранения данных для многих сервисов. Гиперконвергентной называют инфраструктуру, состоящую из узлов, содержащих вычислительные ресурсы, средства хранения, технологии сетевого взаимодействия и виртуализации, объединение и предоставление которых происходит на программном уровне [1].

Основным свойством программно-конфигурируемого хранилища является виртуализация средств хранения данных, что позволяет объединить различные устройства хранения в пулы, которые будут предоставляться по сети, тем самым исключая изолированные участки средств хранения. Плюсами такой организации СХД является.

– Гибкость, программно-конфигурируемое хранилище может быть реализовано на любом оборудовании без привязки к конкретному производителю.

– Горизонтальная масштабируемость.

Существующие реализации SDS (*Software-defined storage* – программно-конфигурируемые хранилища) отличаются друг от друга архитектурным решением, и часто предоставляют свой внутренний набор параметров

для конфигурирования. Однако, программно-конфигурируемые СХД используют ОС для взаимодействия с аппаратным обеспечением, при этом, разделяя вычислительные мощности с другими составляющими гиперконвергентной системы. В общем случае от взаимодействия ОС с аппаратным обеспечением, а также конфигурации самого SDS зависит производительность всей системы хранения.

Производительность СХД, оценивается при помощи следующих параметров:

– количество операций ввода/вывода в секунду – IOPS;
– объем записанных/прочитанных данных в секунду – BW (Байт/с);
– задержка отклика операций ввода/вывода – latency (сек):
  при чтении – время с момента получения запроса на чтение блока информации до получения запрошенной информации;
  при записи – время с момента получения данных на запись до подтверждения записи.

Необходимая пропускная способность СХД описывается следующая выражением:

$$BW_{sds} = \sum_{N} IOPS_{appN} * BLOCK_{SIZE\,appN}.$$

В случае, когда при наличии очереди операций ввода/вывода, хранилище не может обеспечить необходимую BW ($BW_{sds} < BW_{app}$), задержка операций будет возрастать.

Первичным фактором, влияющим на производительность, является скорости чтения/записи устройств хранения, которая может отличаться для различных размеров блока. Однако, ввиду разделяемых сетевых ресурсов, потенциальная скорость чтения/записи может быть ограничена пропускной способностью сети. В случае, когда скорость чтения/записи устройств хранения в одном узле превышает пропускную способность сети основным узким местом становится пропускная способность сети по которой происходит обмен данными между пользователем и SDS, а также, при обеспечении отказоустойчивости на уровне домена, выше узла, пропускной способность кластерной сети хранения. Поэтому важно, чтобы сетевая подсистема имела поддержку различных политик QoS, для регулирования трафика гостевых ОС [2, 3].

Распределённая система хранения данных – Ceph

Ceph – открытый программный продукт, позволяющий построить объектный кластер хранения, не имеющий единой точки отказа.

Основой функционирования Ceph кластера являются 2 службы:

– MON – служба мониторинга кластера, отвечает за карту состояния кластера.

– OSD – служба хранилища, отвечает за хранение и репликацию объектов в кластере.

Ceph кластер – реализует отказоустойчивость, распределяя объекты по группам размещения *pg (placement group)*, каждая из которых, в зависимости от фактора репликации *k,* хранится в *k* OSD, физически расположенных в различных единицах домена отказа. Каждая *pg* принадлежит одному логическому пулу, и закреплена за *k* OSD. При отказе любого из *k* OSD, *pg* назначается новое OSD и данные реплицируются на него. Клиент записывает данные в *pg* на первичное OSD, затем на основе ***k***, первичное OSD реплицирует данные в другие OSD, за которыми закреплена необходимая *pg.* После подтверждения записи во всех OSD, клиенту возвращается подтверждение записи (транзакционная запись). Чтение производится из первичного OSD с проверкой контрольной суммы объекта (рис. 1) [4].

Рис. 1. Процесс записи/чтения при $k = 3$

Для обмена данными между OSD часто выделяют, недоступную извне, кластерную сеть. Как можно заметить, наиболее сложной операцией является запись, на *N* байт трафика записи возникает $(k - 1) * N$ трафика в кластерной сети.

Для тестирования производительности Ceph кластера использовался интерфейс взаимодействия RBD (RADOS *block device)* и утилита fio (*Flexible* I/O)*,* в роли клиента выступал гипервизор QEMU-KVM. Чтение и запись производились блоками по 4 Кбайт, что соответствует стандартному блоку данных во многих ОС. Тестируемая инфраструктура приведена на рис. 2. Технические характеристики узлов указаны в таблице.

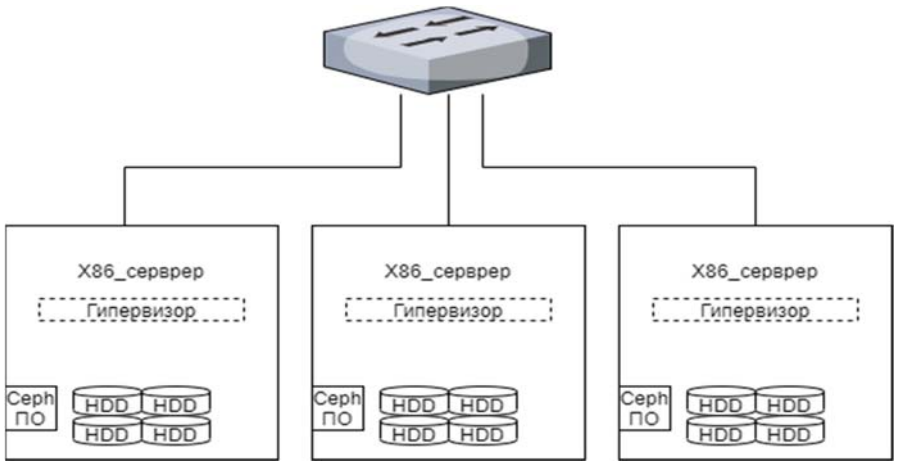


Рис. 2. Тестируемая инфраструктура

ТАБЛИЦА. Технические характеристики узлов

CPU	Intel Xeon E5606
RAM	24G
ОС	CentOS7 ядро 3.10.0-1062.4.1.el7.x86_64
Гипервизор	qemu-kvm
NIC	Intel Gigabit 82576 (2x)
HDD/SDD	Seagate Barracuda7200(4x)/Intel730

Результаты измерения производительности операций записи в зависимости от фактора репликации данных (рис. 3) показали существенное падение количества операций записи с ростом фактора репликации.

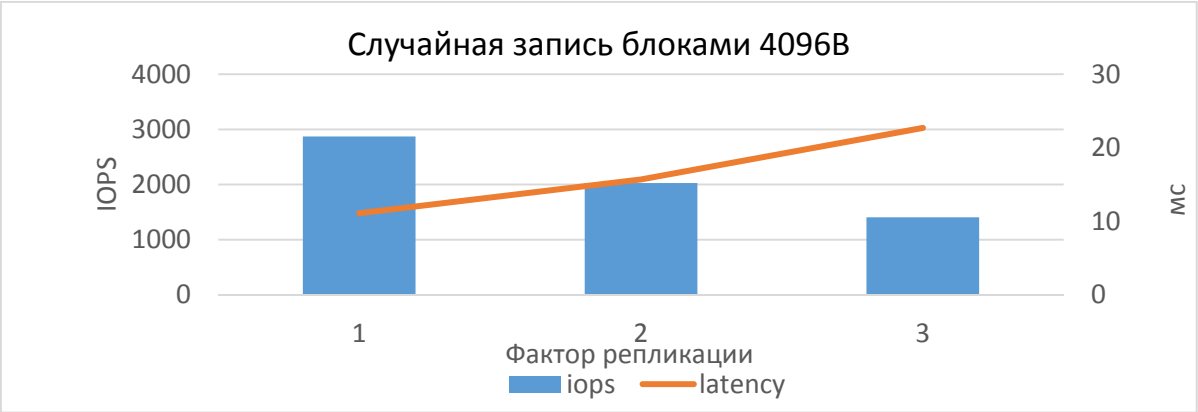


Рис. 3. Производительность при различном факторе репликации

Измерение производительности при $k = 3$ в зависимости от роста количества клиентов (виртуальных машин) (рис. 4).

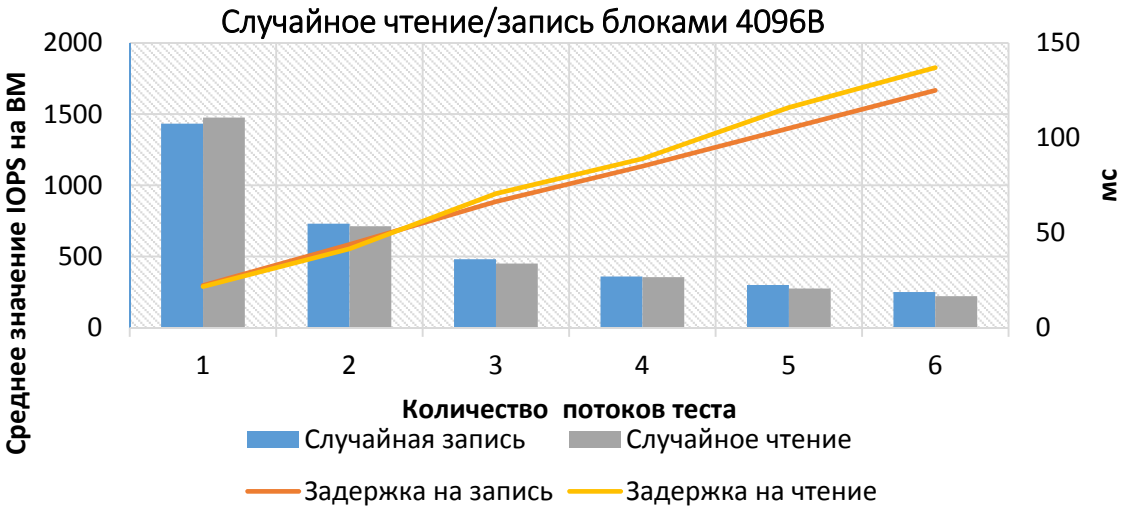


Рис. 4. Производительность при различном количестве клиентов

Список используемых источников

1. Гиперконвергенция: ИТ-инфраструктура на раз, два, три. [Электронный ресурс] // URL: https://www.osp.ru/lan/2016/05/13049349/

2. Зарубин А. А., Швидкий А. А., Савельева А. А. Особенности моделирования нагрузки на РСХД // Вестник связи. 2018. № 8. С. 7.

3. Зарубин А. А., Швидкий А. А., Савельева А. А., Моделирование нагрузки на распределенную систему хранения данных // Вестник связи. 2018. № 7. С. 13.

4. Руководство по Ceph [Электронный ресурс] // URL: https://docs.ceph.com/docs/master/architecture/

Статья представлена заведующим кафедрой ИКС СПбГУТ, кандидатом технических наук, доцентом А. А. Зарубиным.

УДК 004.5
ГРНТИ 49.40.49

СТРУКТУРА СЕТИ ДЛЯ ТЕСТИРОВАНИЯ ПРИЛОЖЕНИЙ ДОПОЛНЕННОЙ РЕАЛЬНОСТИ

Р. В. Киричек, Е. А. Кузнецова

Санкт-Петербургский государственный университет телекоммуникаций им. проф. М. А. Бонч-Бруевича

В данной работе рассматриваются устройства и приложения дополненной реальности в сетях передачи данных. На основе существующих устройств и приложений была разработана архитектура программно-аппаратного комплекса. С помощью раз-

работанной архитектуры программно-аппаратного комплекса была создана структура сети для проведения тестирования систем дополненной реальности. На основе разработанной сети было проведено исследование свойств трафика от устройств и приложений дополненной реальности. Данная структура сети может быть использована для проектирования систем нагрузочного тестирования сетей связи на устойчивость к трафику дополненной реальности.

дополненная реальность, виртуальная реальность, анализ трафика, AR, VR.

Дополненная реальность или AR (*augmented reality*) – это технология наложения информации в форме текста, графики, аудио и других цифровых виртуальных объектов на реальные объекты в режиме реального времени.

Для работы дополненной реальности необходимо устройство с камерой (смартфон, планшет или смарт-очки) и необходимое ПО. Если направить устройство на объект, ПО распознает его с помощью технологии компьютерного зрения. Затем устройство загружает информацию об объекте из облака. Таким образом, видимая пользователем реальность дополняется данными из облака. При движении пользователя размер и ориентация дисплея *AR* автоматически корректируются. Ненужная информация исчезает, а новая появляется.

На протяжении нескольких лет сильно развиваются технологии, связанные с VR/AR, это обуславливается возрастанием популярности данных технологий [1]. В настоящее время технологии VR/AR, становятся всё более тесно связаны со всевозможными сферами жизни человека и получают широкое распространение в различных областях деятельности (рис. 1, см. ниже). Пока в структуре глобального рынка VR/AR 45 % приходится на сегмент развлечений [2]. По прогнозам, через несколько лет его доля будет значительно меньше из-за перераспределения в пользу других отраслей.

В настоящее время трафик, связанный с приложениями Виртуальной и Дополненной реальности обладает достаточно высокими требованиями к сетевым характеристикам. Именно поэтому необходимо протестировать системы дополненной реальности на возможность передачи разного вида трафика.

Для сбора и анализа трафика используются сетевые приложения, включающие в себя технологии Дополненной реальности:

1. *Google* Переводчик – мобильное приложение известного переводчика, которое использует дополненную реальность для перевода через камеру.

2. *Ingress* – многопользовательская онлайн-игра с дополненной реальностью.

3. *Devar* – обучающее приложение для детей, где виртуальные герои помогают изучать материал.

4. *Assemblr AR* – платформа для 3D дизайна, позволяющая создавать объекты непосредственно в своём окружении.

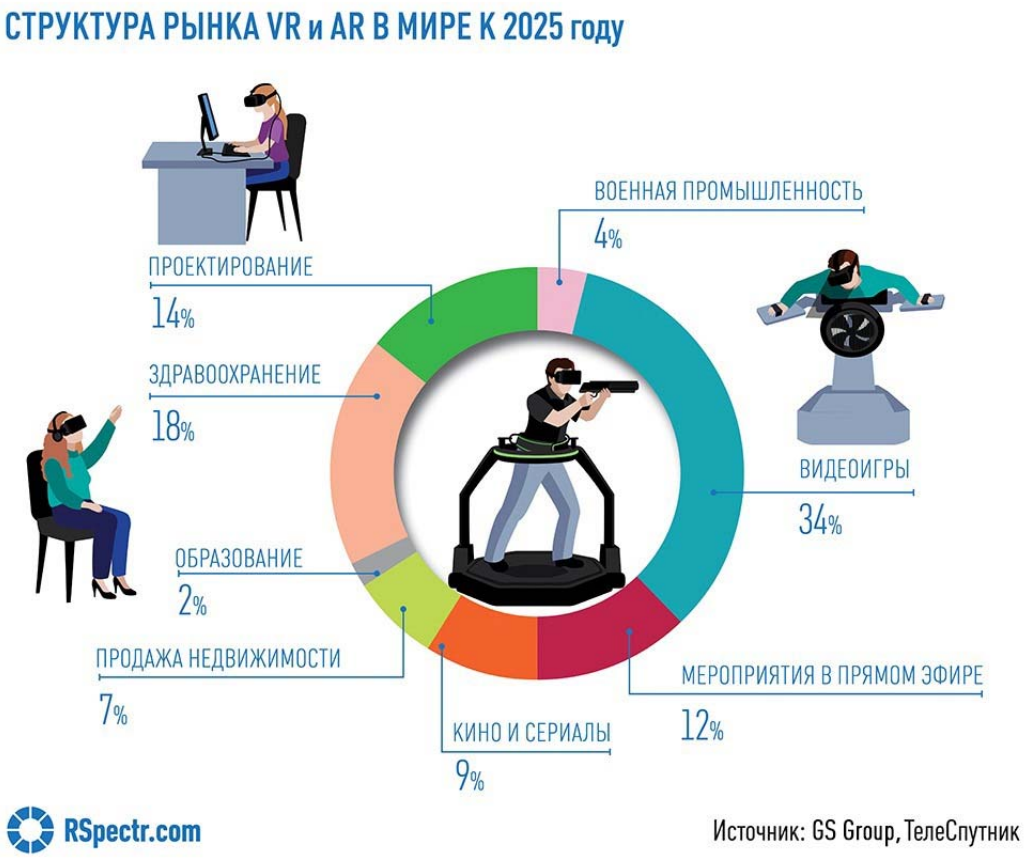


Рис. 1. Структура рынка VR и AR в мире к 2025 году

Реализация сервера AR довольно трудная задача, поэтому было решено перехватывать трафик, поступающий на смартфон, с внешних серверов игр и приложений. Для этого была спроектирована структура программно-аппаратного комплекса для перехвата и анализа трафика, изображённого на рис. 2.

Программно-аппаратный комплекс состоит из следующих элементов:

– смартфон – мобильное вычислительное устройство на базе операционной системы *AndroidOS* или *iOS*, с установленными приложениями и играми для тестирования;

– Wi-Fi роутер (маршрутизатор) – устройство *MikrotikRB951Ui-2nD*, выполня-

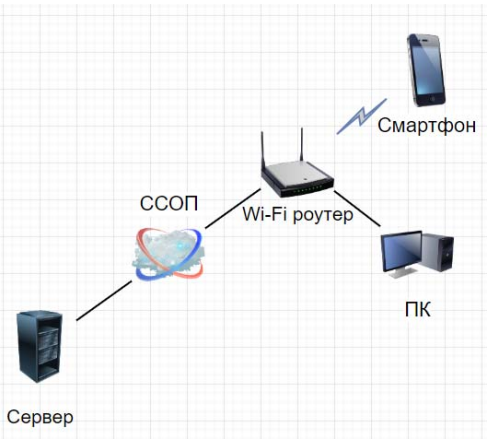


Рис. 2. Структура программно-аппаратного комплекса для перехвата и анализа трафика

ющее функции коммутации кадров, маршрутизации пакетов, предоставляющее доступ устройствам в локальной сети к ресурсам, расположенных во внешних сетях;

– ПК – персональный компьютер на базе операционной системы *Windows* 10 и установленным пакетным анализатором *Wireshark*;

– ССОП – сеть связи общего пользования, комплекс взаимодействующих сетей электросвязи, предназначенный для оказания услуг любому пользователю услугами связи;

– сервер – вычислительная машина для выполнения сервисного программного обеспечения, содержащая данные для установленных приложений.

Для перехвата и анализа трафика, генерируемого смартфоном необходимо настроить Wi-Fi роутер на зеркалирование трафика. В качестве Wi-Fi роутера был выбран Mikrotik, который легко настроить с помощью программного обеспечения Mickrotik WinBox [5] под операционной системой Windows. После запуска Winbox необходимо выбрать нужное оборудование в списке «Neighbors», ввести его логин и пароль, затем нажать на клавишу «Connect», как изображено на рис. 3. При первом подключении устройства пароль не требуется.

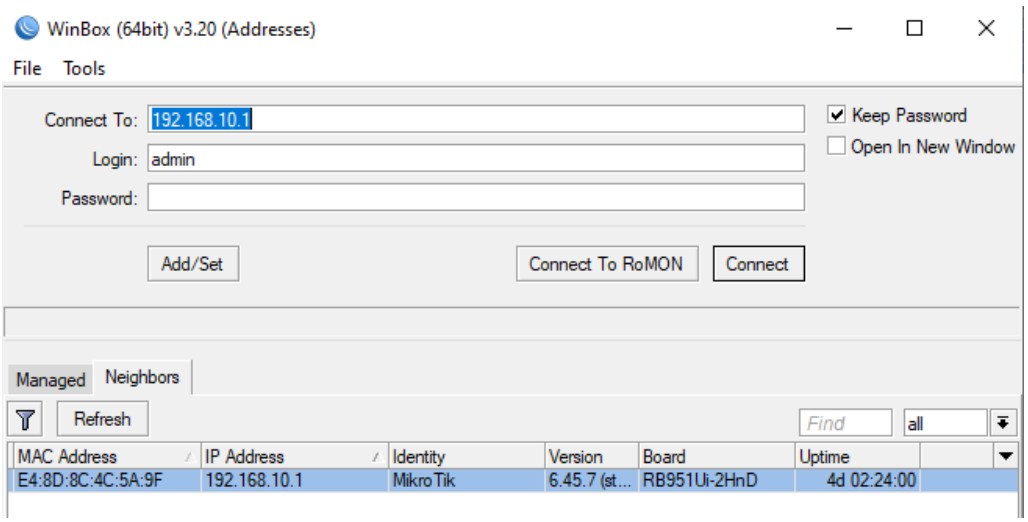


Рис. 3. Подключение к роутеру

Для настройки зеркалирования трафика необходимо выбрать пункт Swith и зайти в настройки оборудования switch1. В данном пункте необходимо выбрать в поле «mirrorsource» – «ether1», а в пункте «mirrortarget» – «eter4» и нажимаем кнопку «Apply», как изображено на рис. 4.

При анализе полученных данных рассматривались показатели: пропускная способность, задержки, джиттер, которые сопоставлялись приказу министерства информационных технологий и связи Российской Федерации № 113 [6].

Полученные результаты отображены в таблице (см. ниже).

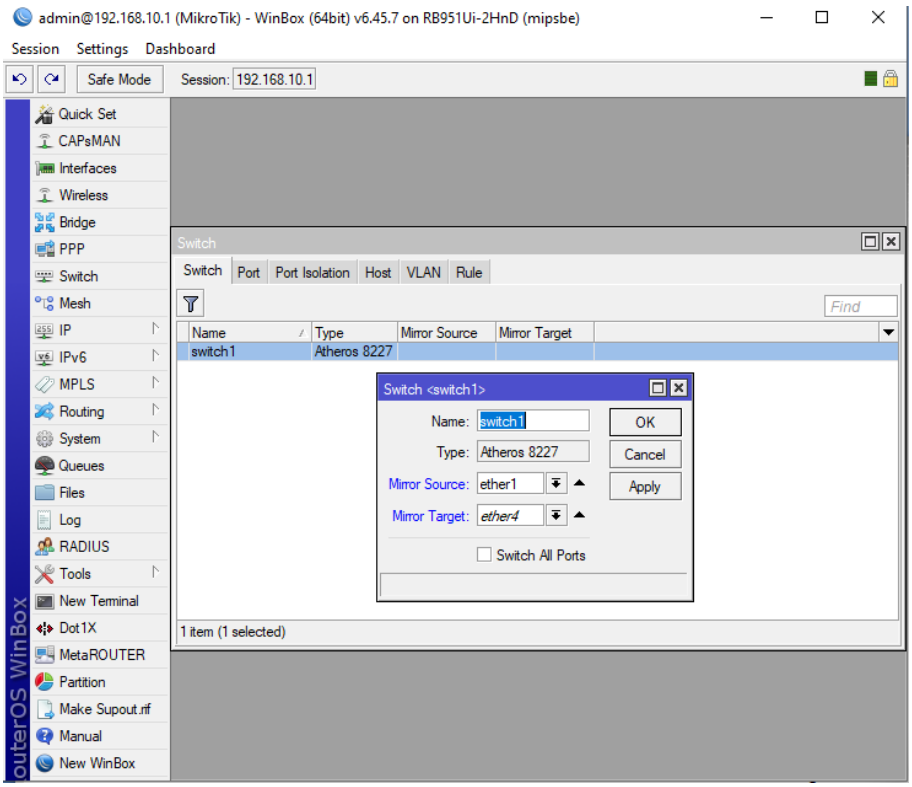


Рис. 4. Настройка зеркалирования

ТАБЛИЦА. Результаты анализа

Приложение AR	Пропускная способность, байт/с	Задержки, мс	Джиттер, мс
Google Переводчик	2637,48	515,66 ± 14,16	18,98
Ingress	56827,76	346,60 ± 14,34	139,18
Devar	1452,36	362,86 ± 14,68	139,49
Assemblr AR	3482,42	359,94 ± 17,32	149,67

Вывод

В данной статье были получены показатели сети, такие как джиттер, задержки и пропускная способность.

Данный трафик имеет высокие показатели задержек, это может говорить, что большинство серверов расположены территориально далеко. Для приложения Google переводчик джиттер имеет не высокие показатели отклонения, поэтому трафик стабильный, что нельзя сказать про показания к играм, требующие больше ресурсов. При субъективной оценке, некоторые приложения было не комфортно использовать, так как иногда были заметы задержки.

Согласно приказу министерства информационных технологий и связи Российской Федерации для интерактивного вида трафика должны быть со-

блюдены технические показатели сети передачи данных: задержка – не более 100 мс, джиттер – не более 50 мс. Приложение Google переводчик соблюдает требования Минкомсвязи РФ только по показателю джиттера, но субъективно работает стабильно, что может говорить о том, что для трафика дополненной реальности требования к показателям сетей связи могут отличаться.

Для исследования характеристик существующей сетевой инфраструктуры на соответствие требованиям, предъявляемым к приложениям дополненной реальности, будет разработан программно-аппаратный комплекс.

Список используемых источников

1. Маколкина М. А., Окунева Д. В., Кулик В. А., Тельтевская В. А., Щербак А. С., Киричек Р. В. Исследование взаимодействия приложений дополненной реальности с облачными сервисами «1С» // Электросвязь. 2017. С. 49–.3

2. https://www.rspectr.com/articles/507/vr-v-rf-budushee-tumanno

3. Маколкина М. А., Парамонов А. И., Кучерявый А. Е. Характеристики сетей связи и приложения дополненной реальности // Проблемы техники и технологий телекоммуникаций (ПТиТТ-2016). Первый научный форум «Телекоммуникации: теория и технологии» ЗТ-2016. 2016. С. 137–138.

4. Маколкина М. А., Парамонов А. И., Гоголь А. А., Кучерявый А. Е. Распределение ресурсов при предоставлении услуги Дополненной реальности // Электросвязь. 2018. № 8. С. 23–30.

5. Mikrotik Winbox. URL: https://mikrotik.com/download.

6. Приказ Министерства информационных технологий и связи Российской Федерации от 27.09.2007 № 113 «Об утверждении Требований к организационно-техническому обеспечению устойчивого функционирования сети связи общего пользования». URL: https://digital.gov.ru/ru/documents/3921/

УДК 004.056.55; 535.14; 530.145
ГРНТИ 47.35.41

ПРИМЕНЕНИЕ КВАНТОВОГО РАСПРЕДЕЛЕНИЯ КЛЮЧЕЙ (QKD) В СЕТЯХ WDM PON

К. В. Вершинина, А. Р. Салтыков

Санкт-Петербургский государственный университет телекоммуникаций им. проф. М. А. Бонч-Бруевича

Обеспечение безопасности абонентов пассивных оптических сетей требует применения передовых технологий, к которым относятся криптографические методы. Работа посвящена рассмотрению возможности применения в PON метода квантовой криптографии, известного как квантовое распределение ключей. Квантовая криптогра-

фия использует квантовый канал для безопасного обмена ключами и защищает конфиденциальную информацию от нежелательных сторон и злоумышленников. QKD применяется для совместного использования случайного секретного ключа путем кодирования информации в квантовых состояниях. В статье также рассматриваются базовые принципы работы QKD, начиная от теорем квантовой механики и заканчивая протоколом BB84. При этом основной акцент посвящен вопросам возможной интеграции технологии QKD в мультиплексированные пассивные оптические сети с разделением длин волн.

квантовое распределение ключей (QKD), мультиплексированная пассивная оптическая сеть с разделением длин волн (WDM PON), квантовая криптография (QC), квантовая механика (QM), протокол BB84.

Квантовая криптография (QC) является одним из новейших методов обеспечения безопасности в мире шифров и определяется как предельный уровень безопасности. QC включает в себя законы квантовой механики (QM) для создания новых криптографических методов [1].

Метод квантового распределения ключей (QKD) базируется на модели, способной производить двусторонние криптопреобразования над данными и подтверждать время отправки сообщения. Такая модель называется квантовой криптосистемой, которая обладает механизмом преобразования ключей. Криптосистема основана на принципах квантовой физики, и информация в такой системе переносится с помощью объектов квантовой механики. В линиях волоконно-оптической связи такими объектами являются фотоны.

На рис. 1 (см. ниже) представлена схема квантовой криптосистемы, где исходный текст отправителя – это информация, подвергающаяся алгоритму шифрования. По открытому каналу передаётся служебная информация классическими методами. По квантовому каналу – фотоны, в которых кодируются шифровальные ключи. После алгоритма дешифрования вторая сторона получает зашифрованный текст.

Квантовая криптография, основанная на QM-законах, обеспечивает безусловную безопасность, используя принцип неопределенности Гейзенберга, явление фотонной (квантовой) запутанности и теорему об отсутствии клонирования [2].

Квантовая запутанность представляет собой квантовомеханическое явление, при котором квантовые состояния объектов оказываются взаимозависимыми. Такая взаимозависимость сохраняется, даже если эти частицы разнесены в пространстве. Измерение параметра одной частицы приводит к мгновенному прекращению запутанного состояния другой [3]. Таким образом, квантовая запутанность – это связанные состояния квантовых объектов.

Принцип неопределенности Гейзенберга заключается в невозможности одновременно и точно измерить положение и скорость частицы. Неопреде-

ленность связана с тем, что процесс измерения – это взаимодействие, которое влияет на состояние квантового объекта, поэтому точно можно измерить только один из параметров квантовой частицы [4].

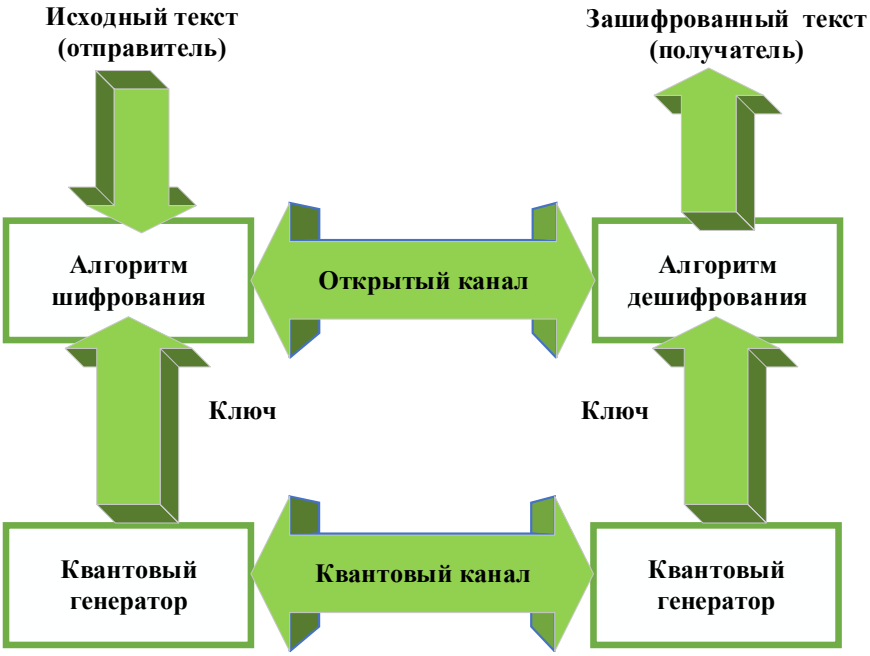


Рис. 1. Структурная схема квантовой криптосистемы

Суть квантовой теоремы об отсутствии клонирования состоит в предотвращении создания копий неизвестного квантового состояния [5]. Это еще один механизм защиты информации в квантовой теории, поскольку копирование неизвестных квантовых состояний позволит точно измерить копии и избежать ограничений принципа неопределенности Гейзенберга, а также воспрепятствовать созданию перехватчиком копий квантовой информации, передаваемой по квантовому каналу.

Реализация метода QKD в сетях пассивных оптических сетях (PON) осуществляется с применением протокола BB84 [6]. Схема работы протокола BB84 приведена на рис. 2 (см. ниже), где Алиса – блок отправителя, Боб – блок получателя, Ева – перехватчик конфиденциальной информации.

Протокол BB84 работает с состояниями поляризации фотонов, используемыми для передачи телекоммуникационной информации со случайной сменой фотонов, сохраняя высокий уровень безопасности в случае вмешательства Евы. В качестве источника света используется лазер, в качестве проводника – оптоволокно. Для передачи информации используются поляризованные фотоны.

Протокол BB84 включает три последовательных этапа: обмен необработанными ключами, фильтрация ключей, дистилляция ключей. На первом этапе информация передается по квантовому каналу от Алисы для измерения Бобом. Алиса поляризует фотоны в двух разных базисах – под углом

0 и 90 градусов, либо 45 и 135 градусов, выбирая базисы каждый раз случайным образом. Далее Боб получает фотоны и измеряет их состояния, выбирая базисы также случайно. Если Боб выбирает правильно, то поляризация записывается точно, иначе – вся информация о начальной поляризации фотона теряется [7].

Рис. 2. Структурная схема работы протокола BB84

Последующие 2 этапа называются «классической постобработкой», так как осуществляются на уровне открытого канала. На этапе фильтрации ключей, Алиса и Боб решают – какое измерение будет использовано для секретного ключа, транслируя свой выбор базиса для каждого фотона. Базисы сравниваются, и любой фотон, который был обработан с использованием несоответствующих базисов, отбрасывается из исходного ключевого материала. При этом результаты измерений по открытому каналу не передаются, но в тоже время Алиса и Боб получают ключ – одинаковую последовательность нулей и единиц. Еве не известен базис, поэтому, при попытке перехвата данных, Ева не получит верных данных. Кроме того, момент несанкционированного измерения изменит поляризацию, следовательно, ошибки обнаружат Алиса и Боб, отбросив повреждённую часть данных [8].

На этапе дистилляции ключей осуществляется исправление ошибок и усиление конфиденциальности, то есть постобработка оставшихся битов секретного ключа, а также аутентификация реализации, которая препятствует атакам посредника (MITM) [9].

Потребность в обеспечении безопасности данных конечных пользователей привела к необходимости применения QKD в сетях доступа. Оптические сети доступа способны обеспечить высокую скорость передачи данных на большие расстояния и для оптимального числа пользователей, поэтому стандарт PON подходит для целей QKD [10].

Мультиплексированная пассивная оптическая сеть с разделением длин волн (WDM PON) или «спектральное уплотнение каналов» имеет преиму-

щество перед другими архитектурами, предлагая неограниченную пропускную способность на абонента и демонстрирует QKD на скорости 10 Гбит/с [11]. Поэтому, WDM PON можно назвать ведущей технологией для QKD. Также в представленной системе не требуются оптическое усиление или оптико-электрооптическое преобразование, которые препятствуют интеграции канала QKD. Мультиплексирование с разделением по длине волны позволяет собирать в одно оптическое волокно несколько потоков оптического сигнала. Каждый поток транслируется на своей длине волны. Все сигналы перед вводом в оптическое волокно, объединяются оптическим мультиплексором (MUX). На приёмном конце сигналы аналогично разделяются оптическим демультиплексором (DEMUX). Структурная схема реализации мультиплексирования на квантовом уровне представлена на рис. 3.

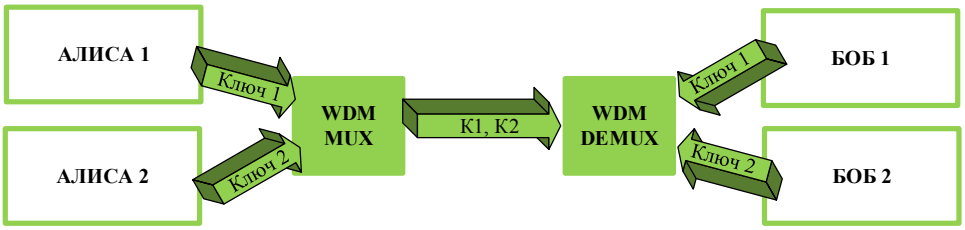


Рис. 3. Структурная схема реализации QKD в WDM-PON

В результате исследования было определено, что квантовое распределение ключей — это метод обмена ключами, реализованный в квантовой криптографии для создания случайного ключа, который разделяется между отправителем и получателем, то есть является для них общим и конфиденциальным. Принципы и теоремы, основанные на QM-законах, предполагают создание ключей с помощью элементарных частиц – фотонов, благодаря чему QKD обеспечивает высокий уровень безопасности в оптические каналах связи.

Внедрение QKD в сети WDM PON позволяет реализовать многоканальную оптическую связь с сохранением оптимальных технические характеристик классических и квантовых каналов в волоконно-оптических линиях связи.

Список используемых источников

1. Martinez-Mateo J., Ciurana A., Martin V. Quantum Key Distribution Based on Selective Post-Processing in Passive Optical Networks // IEEE photonics technology letters. 2014. Vol. 26, No. 9, pp. 881–884.

2. Archana B., Krithika S. Implementation of Noise Immune QKD using BB84 Protocol In Time Division Multiplexing – Passive Optical Networks // International Journal on Recent and Innovation Trends in Computing and Communication. 2015. Vol. 3, No. 4, pp. 1854–1859.

3. Wei Li, Le Wang, Shengmei Zhao. Phase Matching Quantum Key Distribution based on Single-Photon Entanglement // Scientific Reports. 2019. Vol. 9, No. 1.

4. Arevalo Aguilar L. M., Garcia Quijas C. P., Robledo C. The Improvement of the Heisenberg Uncertainty Principle // Advanced in Quantum Mechanics. 2013. Vol. 4, pp. 67–77.

5. Winiarczyk P., Zabierowski W. BB84 analysis of operation and practical considerations and implementations of quantum key distribution systems // CADSM. 2011, pp. 23–25.

6. Бирин Д. А. Квантовое распределение ключей в пассивной оптической сети // T-Comm. 2012. № 7. С. 27–29.

7. Sharma A., Ojha V., Lenka S. K. Security of entanglement based version of BB84 protocol for Quantum Cryptography // IEEE International Conference on Computer Science and Information Technology (ICCSIT). 2010. PP. 83–89.

8. Wang Yong, Wang Huadeng, Li Zhaohong, Huang Jinxiang. Man-in the-middle Attack on BB84 Protocol and its Defence // IEEE International Conference on Computer Science and Information Technology (ICCSIT). 2009. PP. 438–439.

9. Cai Q. Y. Eavesdropping on the two-way quantum communication protocols with invisible photons // Physics Letters A. 2006. Vol. 351, No. 1–2, pp. 23–25.

10. Kyongchun Lim, Heasin Ko, Changho Suh, June-Koo Kevin Rhee. Security analysis of quantum key distribution on passive optical networks // Optics Express. 2017. Vol. 25, No. 10, pp. 11894–11909.

11. Iris Choi, Robert J. Young, Paul D. Townsend. Quantum key distribution on a 10Gb/s WDMPON // Optics Express. 2010. Vol. 18, No. 9, pp. 9600–9612.

Статья представлена заведующей кафедрой ФиЛС СПбГУТ, кандидатом технических наук, доцента М. С. Былиной.

УДК 65.012.8
ГРНТИ 10.19.61

ЗАЩИТА ПЕРСОНАЛЬНЫХ ДАННЫХ В СИСТЕМАХ ЭЛЕКТРОННОГО ДОКУМЕНТООБОРОТА

А. Ю Викулова, В. А. Волостных, П. А. Кононов

Санкт-Петербургский государственный университет телекоммуникаций им. проф. М. А. Бонч-Бруевича

В настоящее время для передачи документированной информации применяются различные системы электронного документооборота. Ряд передаваемых документов содержит информацию, являющуюся персональными данными. В статье рассмотрен предлагаемый порядок создания системы электронного документооборота предприятия, предназначенной для передачи документов, содержащих информацию конфиденциального характера, в том числе персональные данные. В статье изложены основные мероприятия по выполнению требований законодательства о персональных данных. Статья может быть полезна специалистам служб делопроизводства и подразделений технической защиты информации.

документооборот, электронный документооборот, система электронного документооборота, защита персональных данных, средства защиты информации, средства криптографической защиты информации документооборота.

В настоящее время большинство предприятий переходят к электронному документообороту (ЭДО). Актуальность перехода обусловлена значительным рядом преимуществ ЭДО по сравнению с классическим документооборотом основанном на применении бумажных носителей информации и «бумажных» технологий [1].

К основным достоинствам электронного документооборота относятся:

– высокая скорость доставки документа;

– удобство использования полученного документа при ответе на запрос;

– возможность хранения большого количества документов в ограниченном пространстве и др.

Очевидно, что наряду с организационными, техническими и другими документами в системах управления предприятий обрабатывается достаточно большое количество документов, содержащих персональные данные работников предприятия, а в ряде случаев и других граждан Российской Федерации. Известно, что законодательством Российской Федерации установлены достаточно жесткие требования к обеспечению безопасности персональных данных (ПДн) и установлена ответственность должностных лиц за невыполнение этих требований. Исходя из этого, возникает необходимость разработки мероприятий, обеспечивающих требуемый уровень защищенности персональных данных при их обработке в системах электронного документооборота.

Если в системе ЭДО обрабатываются персональные данные, то она относится к классу информационных систем персональных данных, автоматизированных систем [2]. Системы, предназначенные для обработки персональных данных должны быть защищенными и обеспечивать требуемый уровень защиты от актуальных угроз [3].

Возможными угрозами безопасности ПДн, обрабатываемых в системах ЭДО могут являться:

модификация, блокирование, уничтожение документированной информации с ПДн при воздействии на них вредоносного программного обеспечения;

модификация, уничтожение и блокирование документов, содержащих ПДн, сотрудниками предприятия – по необученности или злому умыслу;

нарушение конфиденциальности ПДн при их обработке на автоматизированных рабочих местах (АРМ) работников предприятия при несанкционированном доступе к системе ЭДО и разглашение полученной информации;

нарушение конфиденциальности ПДн при передаче электронных документов с ПДн по незащищенным каналам связи и разглашение их или использование в корыстных целях;

модификация или фальсификация электронных документов, содержащих ПДн, передаваемых по незащищенным каналам связи.

Как показывает практика основными источниками угроз безопасности ПДн обрабатываемых в системах ЭДО являются:

работники предприятия, обязанные обрабатывать документы, содержащие ПДн (нарушители по неумению или по злому умыслу);

работники предприятия необязанные обрабатывать документы, содержащие ПДн, но получившие доступ к системе ЭДО (нарушители по неумению или по злому умыслу);

злоумышленники, не являющиеся работниками предприятия и не имеющие корыстной мотивации доступа к информации в системах ЭДО (хакеры);

злоумышленники, не являющиеся работниками предприятия, но имеющие цели (корыстная мотивация) доступа к информации в системах ЭДО (работники конкурентных организаций, специальные службы иностранных государств);

отказы технических и/или программных средств обработки информации.

Обеспечение безопасности ПДн, обрабатываемых в системах ЭДО достигается [4]:

определением угроз безопасности персональных данных (ПД) при их обработке в системах ЭДО;

применением организационных и технических мер по обеспечению безопасности персональных данных при их обработке в системах ЭДО, необходимых для выполнения требований к защите ПД, исполнение которых обеспечивает установленные Правительством РФ уровни защищенности ПДн [3];

применением прошедших в установленном порядке процедуру оценки соответствия программных и технических средств защиты информации;

применением средств криптографической защиты информации, в том числе средств электронной подписи;

учетом машинных носителей ПДн;

установлением правил доступа к ПДн, обрабатываемым в системах ЭДО, а также обеспечением регистрации и учета всех действий, совершаемых с ПДн в системах ЭДО;

подготовкой персонала к работе в системе ЭДО и обеспечению безопасности, обрабатываемой информации;

обнаружением фактов несанкционированного доступа к ПДн и принятием мер;

восстановлением ПДн, модифицированных или уничтоженных вследствие несанкционированного доступа к ним;

контролем за принимаемыми мерами по обеспечению безопасности ПДн и уровня защищенности системах ЭДО.

На основе рекомендаций, изложенных в [5], предлагается следующая последовательность создания и внедрения на предприятии систем ЭДО, предназначенных для обработки документированной информации, содержащей информацию конфиденциального характера, в том числе персональные данные.

1. Анализ состава электронных документов и их проектов, маршрутов их движения, предполагаемых способов их обработки, уровень конфиденциальности информации, требуемый уровень защищенности информации, требуемый уровень юридической значимости документов в системе ЭДО.

2. Анализ структуры и топологии системы ЭДО предприятия, структуры и топологии системы обмена документами между предприятием и другими субъектами бизнес-процессов.

3. Формирование требований к системе ЭДО предприятия, в том числе требований о применении средств электронной подписи.

4. Анализ технической оснащенности АРМ системы ЭДО и условий их размещения и применения. Анализ процессов обработки информации, используемого программного обеспечения. Анализ состава и уровня обученности персонала предприятия, допускаемого к АРМам системы ЭДО.

5. Определение требуемого уровня защищенности системы ЭДО на основе Постановления Правительства РФ [3].

6. Определение угроз, анализ угроз безопасности информации и системы ЭДО – разработка модели угроз.

7. Формирования совокупности предположений о возможностях, которые могут использоваться при создании способов, подготовке и проведении атак, и определение на этой основе и с учетом типа актуальных угроз требуемого класса СКЗИ [6].

8. Анализ рисков организации при реализации угроз безопасности.

9. Проектирование системы ЭДО:

выбор программного обеспечения системы ЭДО;

определение решений по применению средств электронной подписи (вид электронной подписи, программное обеспечение, ключевые носители) [7];

определение решений по созданию или модернизации АРМов системы ЭДО – выбор аппаратных и программных продуктов, их настроек и др.

10. Проектирование системы обеспечения безопасности информации и системы ЭДО.

10.1. Определение решений по обеспечению инженерной укрепленности помещений для размещения АРМов системы ЭДО:

укрепленность дверей, стен, окон;

создание системы охранной и пожарной сигнализации;

оборудование помещений устройствами для хранения носителей документов и ключей электронной подписи.

10.2. Определение решений по защите системы ЭДО от НСД:

защита средствами операционной системы;

защита специальным ПО защиты от НСД.

10.3. Определение необходимости межсетевого экранирования системы ЭДО организации.

10.4. Определение необходимости применения средств криптографической защиты информации для передачи документированной информации в сторонние организации.

11. Выбор моделей средств защиты информации.

12. Приобретение средств защиты информации.

13. Монтаж и установка средств обработки информации и средств защиты информации.

14. Подготовка персонала к работе с системой ЭДО и применению средств защиты информации.

15. Опытная эксплуатация системы ЭДО.

16. Аттестация системы ЭДО.

17. Ввод в действие системы ЭДО.

18. Контроль эффективности системы ЭДО и системы защиты документированной информации.

Выводы и предложения

1. Защита электронных документов и их проектов в системе ЭДО может быть эффективной только при комплексном подходе к обработке информации, включая технические, организационные решения, а также подготовку должностных лиц участников документооборота.

2. При создании систем ЭДО предлагается формировать модель электронного документооборота, основанную на производственных процессах (бизнес-процессах) предприятия, с учетом функциональных обязанностей должностных лиц.

3. При создании систем ЭДО предназначенных для обработки документированной информации, содержащей персональные данные в основу работ, предлагается положить «ГОСТ Р 51583-2014 Защита информации. Порядок создания автоматизированных систем в защищенном исполнении. Общие положения».

4. При создании систем ЭДО предлагается устанавливать программное обеспечение, сертифицированное по требованиям защищенности информации (например – СЭД «ИВК БюрократЪ»).

Список используемых источников

1. Волостных В. А., Карганов В. В. Проблемы организации защищенного электронного документооборота // Актуальные проблемы инфотелекоммуникаций в науке и образовании. VII Международная научно-техническая и научно-методическая конференция : сб. науч. ст. в 4-х т. СПб. : СПбГУТ, 2018. Т. 4. С. 143–147.
2. Федеральный закон от 27.07.2006 № 152-ФЗ «О персональных данных».
3. Постановление Правительства РФ от 01.11.2012 № 1119 «Об утверждении требований к защите персональных данных при их обработке в информационных системах персональных данных».
4. Приказ ФСТЭК России от 18.02.2013 № 21 «Об утверждении Состава и содержания организационных и технических мер по обеспечению безопасности персональных данных при их обработке в информационных системах персональных данных».
5. ГОСТ Р 51583-2014 Защита информации. Порядок создания автоматизированных систем в защищенном исполнении. Общие положения. URL: http://docs.cntd.ru/document/1200108858
6. Приказ ФСБ России от 10 июля 2014 года № 378 «Об утверждении состава и содержания организационных и технических мер по обеспечению безопасности персональных данных при их обработке в информационных системах персональных данных с использованием средств криптографической защиты информации, необходимых для выполнения установленных Правительством Российской Федерации требований к защите персональных данных для каждого из уровней защищенности».
7. Федеральный закон от 6 апреля 2011 г. № 63-ФЗ «Об электронной подписи».

УДК 004.056.53
ГРНТИ 81.93.29

МОДЕЛЬ И АЛГОРИТМЫ ЗАЩИТЫ ОТ ВРЕДОНОСНОЙ ИНФОРМАЦИИ В СОЦИАЛЬНЫХ СЕТЯХ

Л. А. Виткова

Санкт-Петербургский государственный университет телекоммуникаций им. проф. М. А. Бонч-Бруевича
Санкт-Петербургский институт информатики и автоматизации Российской академии наук

В современном мире цифровая трансформация общества и государства стала реальностью. Еще в начале 2000-х годов компьютерные сети и Интернет были рабочей средой для небольшого круга специалистов. Сегодня младенец вместе с первыми шагами уже осваивает сенсорные экраны и цифровые устройства. Социальные сети плотно вошли в жизнь каждого, независимо от уровня дохода и профессии. Вместе с тем появились и новые типы преступлений. Так, например, всем известны сейчас понятия фейки, спам, навязчивая реклама. Программные решения и компоненты (антивирусы, приложения) предлагают пользователю различные способы защиты от такой информации. Однако общей, универсальной модели вредоносной информации пока нет. В связи

с этим разработка модели и алгоритмов защиты в социальных сетях, представляется важной и актуальной задачей. Автор предлагает модель вредоносной информации и ее распространителя, которая отличается от существующих тем, что содержит новые компоненты: иерархические связи между сообщениями с вредоносной информацией и ее распространителем, а также учитывает информационный признак вредоносной информации, характеристики связей, типы сообщений и дискретные признаки распространителя

вредоносная информация, информационно-признаковая модель, распространитель информации, информационная безопасность, анализ социальных сетей.

Введение

Сегодня, к 2020 году существует только небольшое количество научно-технических решений, направленных на решение проблемы выявления запрещенной информации в социальных сетях. Известные автоматизированные средства обнаружения и защиты от вредоносной информации (ВИ), системы родительского контроля, антивирус в социальных сетях (СС) не отвечают требованиям к скорости, полноте, точности и объективности принимаемых решений. Существует необходимость разработки нового класса систем обнаружения и защиты от вредоносной информации, основанных на применении статистических методов, способов распознавания тематики документа и алгоритмов машинного обучения [1].

Одновременно с этим, само понятие вредоносная информация обсуждается экспертами разных наук, и пока ими консенсус не достигнут. Государственная система противодействия распространению вредоносной информации находится на стадии формирования, об этом свидетельствуют постоянно обновляемые нормативные правовые акты. И определения, термина «вредоносная информация» в российских нормативных и законодательных документах нет [2].

Конституция Российской Федерации в ст. 29 п. 2 содержит ограничения на пропаганду расизма и национальной ненависти или вражды [3]. Основополагающим источником, ограничивающим распространение вредоносной информации, является Федеральный закон «Об информации, информационных технологиях и защите информации» [4].

Федеральный закон от 29 декабря 2010 года № 436-ФЗ «О защите детей от информации причиняющей вред их здоровью и развитию» [5] не содержит термина вредоносная информация, однако в нем имеется понятие информации, причиняющей вред здоровью и (или) развитию детей. Международно-правовые акты также содержат только виды вредоносной информации. Так, например, в [6] включены запреты на пропаганду войны и призывы к национальной, расовой или религиозной ненависти.

Изучением вопросов противодействия распространению вредоносной информации стали заниматься еще в 1990 г. Так, например, В. Н. Лопатин

входил в состав парламентской комиссии Верховного Совета СССР и отвечал за вопросы информационной безопасности. В своих работах определял вредоносную информацию как угрозу информационной безопасности. Он относил к такой информации распространение порнографии; клевету; недобросовестную рекламу [7]. Там же В. Н. Лопатин дал краткую характеристику «вредной информации» (MI, *malicious information*) – это такая информация, распространение которой наносит вред обществу, личности и государству.

Анализ современного состояния исследования показывает, что сами признаки вредоносной информации определены и установлены косвенно, как законодателем, так и учеными. В своем исследовании автор преследует цель формализовать их и предлагает универсальную модель, которая может быть адаптирована в будущем под разную вредоносную информацию, будь то недобросовестная реклама, клевета или другие нарушения требований законодателя.

Синтез

При построении модели вредоносной информации и ее распространителя в социальных сетях будем исходить из того, что в момент присоединения к такой СС пользователь проходит процесс регистрации, создает сетевой профиль – аккаунт (*account*) принадлежит множеству ACCOUNT и получает уникальный ID. Пользователь всегда к нему привязан, хотя находится на границе между виртуальным и реальным миром. Пользователь может не добавлять никакой о себе информации после регистрации, однако это не помешает ему в будущем распространять информацию в социальной сети.

Пользователь формирует аккаунт путем заполнения данных о себе в сетевом профиле и тогда он создает свою собственную страницу (PAGEac). Страница аккаунта принадлежит множеству PAGEac.

Пользователь может создать сообщество и в этот момент оно получает свой уникальный адрес и профиль (*group*). Сообщества в социальных сетях образуют множество GROUP, после заполнения профиля сообщества формируется его страница (PAGEg). Страницы групп принадлежат множеству PAGEg.

При этом, PAGE = {PAGEac ∪ PAGEg}.

Пользователь может распространить информацию в социальных сетях через сообщения (*message*). Все сообщения социальной сети образуют множество MESSAGE. Сообщение – это любой пост в статусе, на стене аккаунта, на стене группы, в комментариях и др. Тогда, когда пользователь создает сообщение и публикует его в открытом доступе от имени своего аккаунта или от имени группы, он (пользователь) является автором (*author*).

Все пишущие пользователи социальных сетей образуют множество AUTHOR.

В процессе анализа сообщения можно определить страницу, на которой оно опубликовано и его автора. Таким образом возможно обнаружить распространителя (*source*). Все распространители в социальных сетях образуют множество (SOURCE).

В целях формализации введем следующие объекты информационного обмена в социальных сетях и характеристики (табл.).

ТАБЛИЦА. Объекты социальной сети

Название	Объект	Характеристики
Пользователь	user	физическое лицо
Аккаунт	account	профиль пользователя, через который и от имени которого он может распространять информацию
Сообщество	group	профиль сообщества, через который и/или от имени которого пользователь может распространять информацию
Страница	page	страница пользователя или группы, через которую может распространяться информация
Сообщение	message	пост в статусе, на стене аккаунта, на стене группы, в комментариях, который распространяется в открытом доступе
Автор	author	пользователь, создавший сообщение от имени своего аккаунта или от имени сообщества
Распространитель	source	страница пользователя, на которой размещено сообщение

На рисунке (см. ниже) показано соотношение различный уровней модели. Автор формирует сообщение и размещает его в источнике распространения, на странице либо аккаунта, либо группы. Именно этот источник распространения признается распространителем (не автор). Сообщения могут содержать, а могут не содержать признаки вредоносной информации. Признаки формируют уровень угроз информационной безопасности и позволяют оценить угрозу. Таким образом, собрав информацию на странице какого-либо распространителя возможно определить, какие из этих сообщений относятся к вредоносным и оценить уровень угроз, который представляет информация для пользователей социальных сетей. И тогда уже, может быть принято решение о противодействии.

Для повышения точности классификации распространителей предлагается алгоритм оценки распространителя.

Алгоритм делится на 2 этапа:

Первый этап – подготовительный – разбиение массива (M) на отдельные сообщения (*mi*) и формирование списков распространителей по типам (рис.) (аккаунт, группа).

Второй этап – оценка потенциала распространителя.

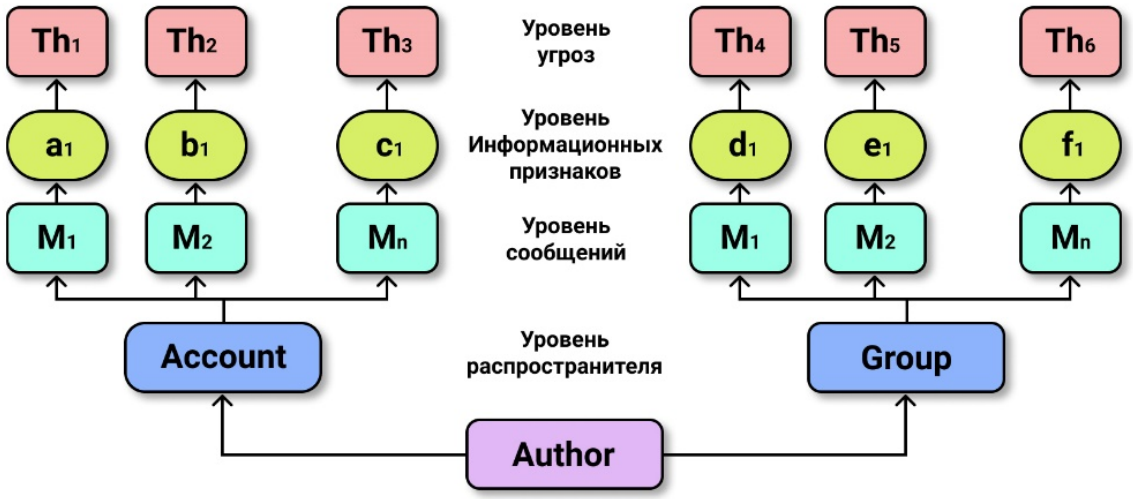


Рис. Модель вредоносной информации и ее распространителя в социальных сетях

Для отдельных сообщений, на втором этапе вычисляется степень вложенности в дереве сообщений.

Каждое сообщение располагается на некотором уровне в дереве сообщений. Если это пост в группе или аккаунте, оно является корнем дерева. В этом случае сообщение получает рейтинг 1. Если это ответ на пост, то сообщение располагается на втором уровне дерева, и его рейтинг в 2 раза меньше – 0,5. Ответ на ответ занимает тритий уровень, и его рейтинг еще в половину меньше – 0,25. Таким образом производится оценка расположения сообщения в ветке обсуждения

Модель и алгоритмы защиты от вредоносной информации и ее распространителя в социальных сетях позволяют:

1) проводить мониторинг вредоносной информации в социальных сетях путем сбора, агрегации и анализа сообщений, опубликованных в социальных сетях;

2) формировать исходные данные для задач защиты от угроз распространения ВИ;

3) обнаруживать и оценивать распространителей (источники распространения) вредоносной информации;

4) формировать контрмеры, направленные на противодействие распространение вредоносной информации в социальных сетях.

Работа выполнена при финансовой поддержке Гранта РНФ (проект РНФ № 18-71-10094) в СПИИРАН.

Список используемых источников

1. Андрианов В. И., Виткова Л. А., Волкогонов В. Н. Вопросы информационной безопасности с точки зрения психологии и виктимологии // Актуальные проблемы инфотелекоммуникаций в науке и образовании. IV Международная научно-техническая и научно-методическая конференция: сб. науч. ст. в 2 т. СПб. : СПбГУТ, 2015. С. 190–193.

2. Лукина Е. И. Вредоносная информация: сущность и содержание понятия // Пробелы в российском законодательстве. 2016. № 4. URL: https://cyberleninka.ru/article/n/vredonosnaya-informatsiya-suschnost-i-soderzhanie-ponyatiya (дата обращения: 10.11.2019).

3. Конституция Российской Федерации: принята Всенародным голосованием 12 декабря 1993 года // Российская газета. – 25.12.1993. – № 23.

4. Об информации, информационных технологиях и о защите информации: Федеральный закон от 27 июля 2006 г. № 149-ФЗ (ред. от 01.05.2019 г.) // Собр. законодательства РФ. – 2006. – № 31(1 ч.). – Ст. 3448.

5. О защите детей от информации, причиняющей вред их здоровью и развитию: Федеральный закон от 29 декабря 2010 г. № 436-ФЗ // Собр. законодательства Рос. Федерации. – 2011. – № 1. – Ст. 48.

6. Международный Пакт от 16.12.1966 «О гражданских и политических правах» // СПС «Консультант Плюс – 2019».

7. Лопатин В. Н. Информационная безопасность России : дисс. ... докт. юрид. наук : 12.00.01 / Лопатин Владимир Николаевич, СПб., 2000. 433 с.

Статья представлена научным руководителем, доцентом кафедры ЗСС СПбГУТ, кандидатом технических наук Д. В. Сахаровым.

УДК 004.056
ГРНТИ 81.93.29

РАЗРАБОТКА МЕХАНИЗМОВ АНАЛИЗА НЕЖЕЛАТЕЛЬНОЙ ИНФОРМАЦИИ В СОЦИАЛЬНЫХ СЕТЯХ

Л. А. Виткова[1, 2], Т. О. Гамидов[1], М. М. Ковцур[1]

[1]Санкт-Петербургский государственный университет телекоммуникаций им. проф. М. А. Бонч-Бруевича
[2]Санкт-Петербургский институт информатики и автоматизации Российской академии наук

На начало 2020 года более четырёх с половиной миллиарда человек используют всемирную сеть Интернет, а аудитория социальных сетей перешла за отметку в 3,8 миллиарда. Однако с увеличением количества пользователей в социальных сетях,

растёт количество информации, а, следовательно, и количество нежелательного контента. Становится всё сложнее выявлять и останавливать его распространение. Каждый пост, содержащий контент, распространение которого запрещено, анализируется и блокируется по отдельности. Нет единого механизма, позволяющего выявлять источник распространения нежелательной информации. В работе предложен подход к созданию единой модели данных для нескольких социальных сетей Вконтакте, Facebook, Instagram. Предполагается, что единая модель данных позволит выявлять источник распространения нежелательной информации в нескольких социальных сетях одновременно.

анализ социальных сетей, SNA, модель, данные, модели данных, информация, нежелательная информация, источник, распространение, источник распространения.

Цифровые технологии всё больше становятся частью нашей повседневной жизни, люди все больше проводят времени в Интернете. На начало 2020 года больше 4,5 миллиарда человек пользуются сетью Интернет, а аудитория социальных сетей перешла за отметку в 3,8 миллиарда человек [1, 2]. Почти 60 % населения планеты уже онлайн, и есть причины полагать, что к середине года половина людей на планете будет пользоваться социальными сетями [3]. По статистике за 2020 год в мире увеличилось количество интернет-пользователей на 7 % до 4,54 миллиардов, что на 298 миллионов больше при сравнении с данными за январь 2019 года. Аудитория социальны сетей увеличилась на 9 % до 3,80 миллиардов, что на 321 миллион больше чем в 2019 году [4]. Также увеличилось количество пользователей мобильными устройствами на 2,4 % до 5,19 миллиарда человек, что на 124 миллиона больше, чем за 2019 год. В России общее значение пользователей Интернета, по данным Digital 2020, достигло 118 миллионов, что говорит о том, что Интернет используют 81 % россиян. Численность пользователей соцсетей в России на начало 2020 года составила 70 миллионов пользователей, 48 % от всего населения страны. С увеличение количества пользователей в социальных сетях, увеличивается и количество распространителей нежелательной информации. Каждый пост с нежелательной информацией в социальных сетях анализируется и блокируется отдельно, что занимает много времени. В данной работе, в качестве примера, будут рассмотрены модели данных 3-х социальных сетей: Вконтакте, Facebook, Instagram, а также предложен подход создания единой модели данный для анализа нежелательной информации в социальных сетях.

На рис. 1 (см. ниже) представлена модель данных для социальной сети Вконтакте.

Данная модель данных построена на основе 4-х объектов: пользователь (*user*), группа (*group*), пост (*post*), комментарий *(comment*). Объект «пользователь» описывает характеристики пользователя, «группа» описывает характеристики группы, «пост» описывает характеристики созданной

пользователем или группой публикации, «комментарий» описывает характеристики каждого комментария, созданных пользователями или группами.

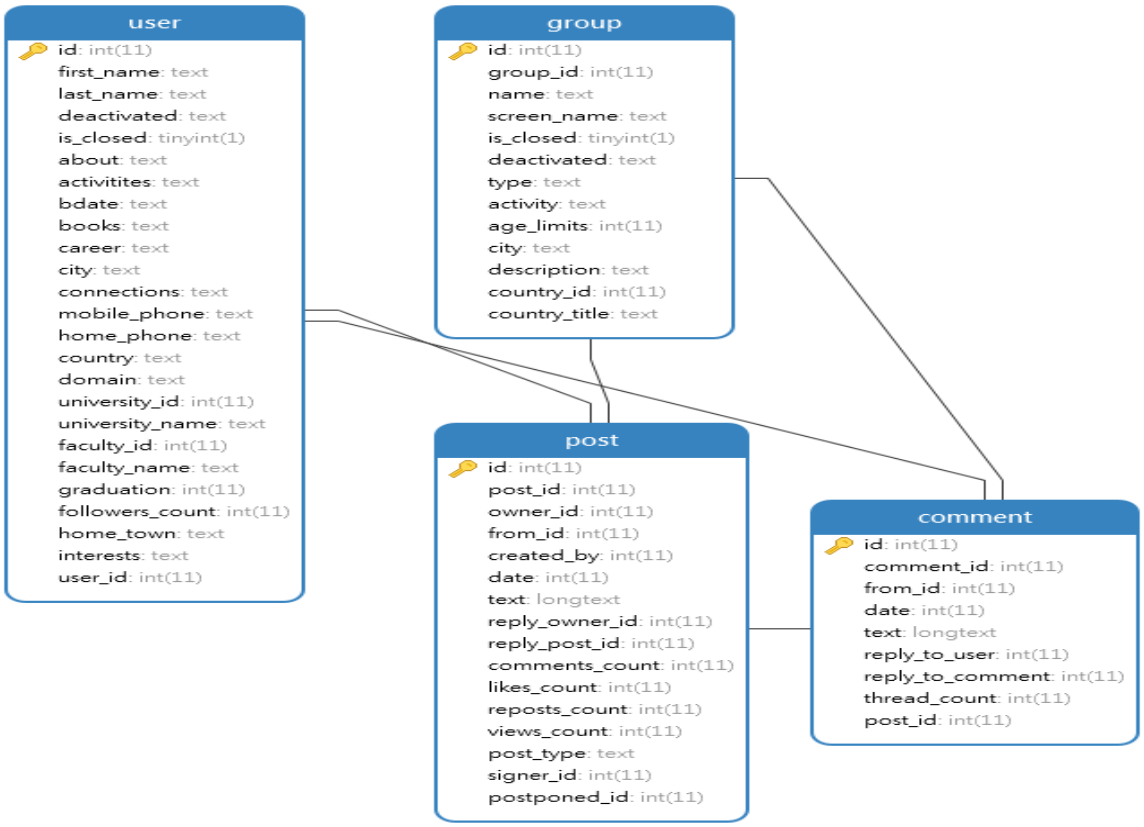


Рис. 1. Модель данных для социальной сети Вконтакте

Объект «пользователь» включает в себя характеристики:
1) user_id – уникальный идентификатор пользователя;
2) first_name – имя пользователя;
3) last_name – фамилия пользователя;
4) deactivated – показывает, забанен или удален профиль пользователя:
5) is_closed – показывает закрыт ли профиль пользователя;
6) about – содержимое поля «О себе» из профиля;
7) activities – содержимое поля «Деятельность» из профиля;
8) bdate – дата рождения пользователя и др.

Объект «группа» включает в себя характеристики:
1) group_id – уникальный идентификатор группы;
2) name – название группы;
3) screen_name – сокращенное название группы;
4) is_closed – показывает закрыта ли группа;
5) deactivated – показывает закрыта ли группа;
6) type – показывает тип сообщества;
7) activity – показывает тематику группы;
8) age-limits – показывает возрастное ограничение; и др.

Объект «пост» включает в себя характеристики:

1) post_id – идентификатор записи;

2) owner_id – идентификатор владельца стены, на которой размещена запись;

3) from_id – идентификатор автора записи;

4) created_by – идентификатор администратора, который опубликовал запись;

5) date – время публикации записи;

6) text – текст записи;

7) reply_owner_id – идентификатор владельца записи, в ответ на которую была оставлена текущая;

8) reply_post_id – идентификатор записи, в ответ на которую была оставлена текущая;

9) comments_count – количество комментариев;

10) likes_count – число пользователей, которым понравилась запись;

11) reposts_count – число пользователей, скопировавших запись;

12) views_count – число просмотров записи;

13) post_type – тип записи;

14) signer_id – идентификатор автора, если запись была опубликована от имени сообщества и подписана пользователем;

15) postponed_id – идентификатор отложенной записи.

Объект «комментарий» включает в себя характеристики:

1) comment_id – идентификатор комментария;

2) from_id – идентификатор автора комментария;

3) date – дата создания комментария;

4) text – текст комментария;

5) reply_to_user – идентификатор пользователя или сообщества, в ответ которому оставлен текущий комментарий;

6) reply_to_comment – идентификатор комментария, в ответ на который оставлен текущий;

7) thread_count – количество комментариев в ветке;

8) post_id – идентификатор записи, к которой оставлен комментарий.

Для сравнения в работе рассматривается также и модель данных Facebook (рис. 2, см. ниже). Она состоит из 4-х объектов: пользователь (*user*), группа (*group*), пост (*post*), комментарий (*comment*). Как и в случае с Вконтакте, объект «пользователь» описывает характеристики пользователя, объект «группа» описывает характеристики группы, объект «пост» описывает характеристики записи пользователя или группы, а объект «комментарий» описывает характеристики оставленных пользователем или группой комментариев к публикации. Однако в отличии от социальной сети ВК, Facebook отдает гораздо меньше информации для анализа.

Общая модель данных для 3-х социальных сетей построена на основании одинаковых характеристик у объектов из 3-х социальных сетей (ВК, *Facebook* и *Instagram*). Общая модель данных состоит из 3-х объектов: профиль (*profile*), пост (*post*), комментарий (*comment*). Объект «профиль» включает в себя характеристики, описывающие профиль пользователя, объект «пост» включает в себя характеристики, описывающие запись, созданную пользователем, а объект «комментарий» включает в себя характеристики, описывающие комментарии, оставленные пользователем.

Рис. 2. Модель данных для социальной сети Facebook

Общая модель данных для 3-х социальных сетей показана на рис. 3.

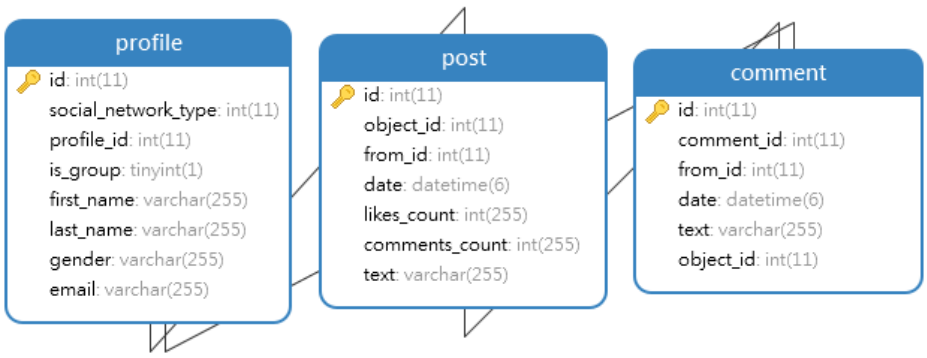


Рис. 3. Общая модель данных для 3-х социальных сетей

Новым элементом является social_network_type – социальная сеть, к которой принадлежит профиль пользователя.

Было выявлено, что социальные сети со временем становятся всё более популярными, а количество информации в социальных сетях продолжает неуклонно расти, что в свою очередь усложняет анализ и выявление нежелательной информации в социальных сетях. Были разработаны и рассмотрены модели данных для социальных сетей: Вконтакте, Facebook и Instagram. На основе рассмотренных моделей данных можно сделать вывод, что наибольшее количество информации о пользователе и его взаимодействии с другими пользователями можно получить из модели данных социальной сети Вконтакте, второй по количеству отдаваемых данных является Facebook, а на последнем месте расположилась социальная сеть Instagram. На основе данных моделей была разработана единая модель данных, способная хранить информацию по выбранной тематике, что позволит выявлять распространителей нежелательной информации в нескольких социальных сетях одновременно.

Работа выполнена при частичной финансовой поддержке Российского научного фонда (проект № 18-71-10094) в СПИИРАН.

Список используемых источников

1. Виткова Л. А. Обзор Степени разработанности темы мониторинга и противодействия угрозам информационно-психологической безопасности в социальных сетях // Информационные технологии и телекоммуникации. 2018. Т. 6. № 3. С. 1–9.

2. Вильчинская Э. А., Виткова Л. А., Парсон И. М. Актуальные проблемы правового регулирования средств массовой информации // Право и информация: вопросы теории и практики сборник материалов международной научно-практической конференции. Сер. «Электронное законодательство» ФГБУ «Президентская библиотека имени Б. Н. Ельцина». 2017. С. 102–108.

3. Виткова Л. А., Проноза А. А., Сахаров Д. В., Чечулин А. А. Проблемы безопасности информационной сферы в условиях информационного противоборства // Актуальные проблемы инфотелекоммуникаций в науке и образовании. VII Международная научно-техническая и научно-методическая конференция : сб. науч. ст. в 4-х т. СПб. : СПбГУТ, 2018. С. 191–195.

4. Науменко К. А. Конвергенция традиционных и социальных медиа как тренд медиапотребления современной Италии // Медиачтения СКФУ. Материалы Третьей Международной научно-практической конференции / Отв. ред О. И. Лепилкина, А. М. Горбачев, Н. Н. Борисенко, Д. А. Шевцова. 2019. С. 127–129.

УДК 621.395.34
ГРНТИ 49.39.29

ИССЛЕДОВАНИЕ МЕХАНИЗМОВ ИНТЕГРАЦИИ ТЕЛЕКОММУНИКАЦИОННОЙ ПЛАТФОРМЫ АГАТ CU 72XX

Л. А. Виткова, В. Н. Диордица, М. М. Ковцур, А. И. Таргонская

Санкт-Петербургский государственный университет телекоммуникаций им. проф. М. А. Бонч-Бруевича

В работе рассматривается технические и функциональные возможности Агат CU 72XX, профессиональной телекоммуникационной платформы для обеспечения телефонной инфраструктуры. Главным образом описываются возможности платформы, какие задачи с помощью нее можно решить, а также интеграция со сторонними корпоративными системами. Проведен анализ существующего на данном этапе функционала Агат CU 72XX, с рассмотрением возможного его расширения путем использования дополнительных опций.

IP-телефония, LDAP, АТС, интеграция.

Среди компаний среднего и малого бизнеса все чаще поднимается тема IP-телефонии. Данная технология позволяет сократить расходы на обеспечение связи, а также обеспечить централизованное управление. В-первую очередь, плюсом для компаний является возможность снижения затрат на телефонную связь. Использование IP-телефонии позволяет достигнуть значительной экономии на услугах международной и междугородней связи из-за низких тарифов, а также не требуется прокладка новых коммуникаций, поскольку используются уже существующие интернет подключения [1]. Во-вторых, компании отдают предпочтения построению сети с применением IP-АТС. АТС – это автоматическая телефонная станция, другими словами, это устройство, обеспечивающие автоматическое соединение и поддержание телефонной связи между абонентами. Для реализации сети компании с использованием телефонии необходимо использования как клиентского, так и серверного разнородного оборудование.

В рамках статьи рассматривается технические и функциональные возможности профессиональной телекоммуникационной платформы Агат CU версии 72XX. Производителем является российская инновационная производственная компания «Агат – Российские технологии». Агат CU является новым продуктом, предоставляемым Агат-РТ. Выбор обуславливается актуальной в настоящее время темой импортозамещения. Продукция Агат-РТ разрабатывается и производится на территории Российской Федерации,

а также оборудования поставляется с сертификатами специальной проверки и специального исследования вспомогательных технических средств и систем [2].

В ходе изучения технических и функциональных возможностей телекоммуникационной платформы Агат CU серии 72XX были выделены следующие особенности: возможности autoprovision, управление очередями в реальном времени через web-интерфейс, запись разговоров, система оповещений, сервер конференция, интеграция с внешними информационными система и т. д. Именно возможность интеграции со сторонними системами является преимуществом IP-АТС Агат CU и рассматривается в данной статье. Производителем заявляется возможность интеграции с помощью привязки корпоративной телефонной книги к LDAP, синхронизация телефонной книги с Microsoft Exchange и синхронизация со справочниками информационных систем, работающих на платформе 1С 8.3. Данные интеграции являются наиболее популярными и актуальными, поскольку большинство компаний малого и среднего бизнеса отдают предпочтения именно продуктам 1С, пакету Microsoft Office и технологиям Active Directory. Также возможна интеграция с сервером видеоконференций Mind.

Прежде чем перейти к непосредственной разработке и анализу схемы интеграции телекоммуникационной платформы со сторонними внешними информационными системами [3], был изучен список сетевых протоколов, поддерживаемых Агат CU 72XX:

– SNMP – протокол для управления сетевыми устройствами;
– SNTP – протокол синхронизации времени по сети;
– SMTP – протокол для передачи электронной почты по сети;
– UDP – протокол обмена дейтаграммами;
– TCP – протокол для обеспечения надежной доставки данным на транспортном уровне;
– ICMP – сетевой протокол для передачи сообщений об ошибках и других исключительных ситуациях;
– LDAP – протокол для доступа к службе каталогов;
– SIP – протокол сигнализации IP-телефонии;
– RTP – протокол передачи медиаданных.

Таким образом, основываясь на поддерживаемых протоколах, можно построить схемы интеграции АТС с внешними информационными ресурсами. Разработанная схема представлена на рис. (см. ниже).

В результате проделанной работы представлена схема интеграции автоматической телефонной станции со внешними информационными ресурсами. Интеграция со сторонними ресурсами является важным элементом в организации телефонной сети в компаниях малого и среднего бизнеса. Интеграция – это объединение разнородных систем в единую среду. Таким об-

разом, компания получает готовую к работе систему, а не разнородные части, каждой из которых необходимо администрирование. Из этого следует, что улучшается функционирование системы, а также упрощается ее поддержание администраторами. Рассмотрим, что из себя представляют отдельные части. Во-первых, это необходимая практически в каждой фирме система CRM (*Customer Relationship Management*), иными словами система управления взаимоотношениями с клиентами. Обмен пакетами происходит по протоколу TCP. В качестве CRM может выступать 1С 8.3. Во-вторых, это корпоративная база данных, без которой в большинстве случаев не обходится ни одна система. «Общение» между информационными системами происходит по протоколу доступа к каталогам LDAP. Для подключения требуются IP-адрес LDAP сервера, логин и пароль. А также указать имя базы данных. Помимо этого, Агат CU поддерживает сервер видеоконференций Mind и пакеты передаются по протоколу UDP.

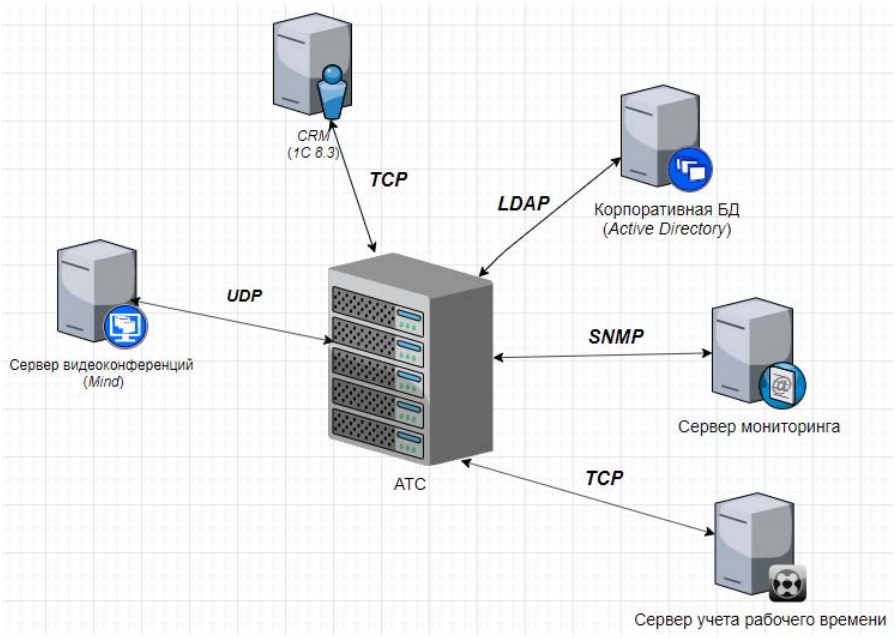


Рис. Схема интеграции АТС с внешними ресурсами

Сервер мониторинга выступает еще одним важным звеном в системе. Информирование об авариях происходит по протоколу SNMP. В качестве информационной системы для контроля трудовой дисциплины среди сотрудников выступает система учета рабочего времени [2]. Система помогает анализировать и фиксировать все входы и выходы сотрудников предприятия, отслеживать опоздания, преждевременные уходы и отсутствие на рабочем месте. Данные с этой системы передаются по протоколу TCP.

Исходя из изученного материала можно сделать вывод, что Агат CU благодаря своим возможностям интеграции с внешним информационными

ресурсами, выступает многофункциональным инструментом для корпоративной инфраструктуры и помогает компаниям создать рабочую и удобную систему для поддержки телефонии.

Список используемых источников

1. Гольдштейн Б. С., Пинчук А. В., Суховицкий А. Л. IP-телефония. М. : Радио и связь, 2001. 336 с.

2. Коммутационная платформа АГАТ CU [Электронный ресурс]. URL: https://agatrt.ru/telefonizaciya-predpriyatiya/kommutacionnaya-platforma-agat-cu/ (дата обращения 25.02.2020).

3. Ушаков И. А., Котенко И. В., Крылов К. Ю. Анализ методик применения концепции больших данных для мониторинга безопасности компьютерных сетей // Информационная безопасность регионов России (ИБРР-2015) : материалы конференции. 2015. С. 75–76.

УДК 004.056.53
ГРНТИ 81.93.29

АНАЛИЗ АЛГОРИТМОВ РАСПОЗНАВАНИЯ КЛАВИАТУРНОГО ПОЧЕРКА И ИХ ПОКАЗАТЕЛЕЙ ЭФФЕКТИВНОСТИ

Л. А. Виткова, Е. А. Донсков

Санкт-Петербургский государственный университет телекоммуникаций им. проф. М. А. Бонч-Бруевича

На сегодняшний день имеется множество средств для идентификации человека с высоким уровнем достоверности. Некоторые из них строят свои алгоритмы на основе определения клавиатурного почерка. Клавиатурный почерк – это определенная биометрическая характеристика, которая позволяет получить описания динамики ввода, его скорости, наличия задержек, а также частоты возникновения ошибок. Однако, для корректной оценки качества алгоритмов клавиатурного почерка, необходимо определить некоторые критерии, оценивая которые можно делать заключение, базируясь на критериях эффективности, как их еще называют. В данной работе рассматриваются именно такие алгоритмы, а также показатели эффективности.

аутентификация, идентификация, пароль, клавиатурный почерк, нейронная сеть, персептрон, far, frr.

Введение

На сегодняшний день существует и успешно функционирует огромное количество различных организаций. Государственные и частные организа-

ции, крупные и малые производства, частные предприниматели. Большинство из которых нуждаются в наемных сотрудниках. Количество их варьируется от масштаба организации и может достигать нескольких сотен тысяч человек, которые должны быть учтены и зарегистрированы в корпоративной сети, чтобы иметь доступ к различной документации и другим необходимым для ведения рабочего процесса документам. Современный уровень развития информационных систем диктует новые правила организации информационной безопасности, что особенно актуально в условиях необходимости защиты конфиденциальный данных [1, 2, 3].

Наиболее классическим способом защиты данных является наличие у пользователя данных его аутентификации в системе – логина и пароля. Но не все пользователи относятся с должной серьезностью к данному процессу, что приводит к взломам системы, а также утечке конфиденциальных данных. На сегодняшний день существует огромное количество программных инструментов, которые позволяют злоумышленникам получать доступ к персональным данным пользователей и конфиденциальным данным организации.

Стоит учитывать, что при использовании одного пароля, даже если настроены все необходимые политики, включающие как смену пароля, так и блокировку учетной записи при некотором конкретном количестве попыток некорректного введения данных аутентификации, система все равно остается незащищенной. Главной причиной утечки информации является сам пользователь, невольно передающий свой пароль мошенникам или оставляющий зафиксированным в письменном виде на рабочем месте. В таком случае злоумышленнику не составит труда получить доступ к конфиденциальной информации.

В мире существует множество решений, нацеленных на предотвращение доступа к конфиденциальной информации при раскрытии секретного ключа. Одним из примеров которой могут служить многофакторная аутентификация, физические токены, биометрические данные и т. п. Однако, наиболее перспективной инновацией является аутентификация с помощью клавиатурного почерка.

Понятие клавиатурного почерка

Каждый человек самостоятельно воспринимает информацию и делает это уникально, то есть отличительно от других. Например, каждый человек на планете имеет уникальный стиль почерка, а также уникальную подпись.

Такой же принцип действует и при необходимости быстрого набора текста с использованием обеих рук и компьютерной клавиатуры. Используя две руки у каждого человека, создается индивидуальный подход к набору текста. Выходит, что клавиатурный почерк аналогичен подписи в докумен-

тах, так как является уникальным для человека стилем печати с использованием компьютерной клавиатуры, но с учетом корректной фиксации стиля с использованием различных метрик.

Клавиатурный почерк – это набор динамических параметров работы с использованием клавиатуры. Индивидуальность стиля набора пользователя складывается из следующих параметров:

– скорость набора символов;
– наличие привычек нажатия клавиш и их комбинаций;
– особенности набора отдельных символов, каких-либо временных задержек при наборе конкретных символов и т. д.

С точки зрения эффективности аутентификации этот метод сравним с биометрическими данными, которые уникальны для каждого человека (отпечаток пальца, сетчатка глаза). Однако, в случае реализации обоих вариантов аутентификации (и биометрического, и клавиатурного), то аутентификация по клавиатурному почерку будет являться более эффективной, так как для реализации необходима лишь компьютерная клавиатура и программное обеспечение, а не дорогостоящее биометрическое оборудование.

Для создания алгоритмов аутентификации с использованием клавиатурного почерка чаще всего используют:

– статистические расчеты;
– использование нейронных сетей;
– векторный анализ.

В данной работе рассматривается концепция разработки алгоритма аутентификации с использованием клавиатурного почерка на базе нейронных сетей, а в частности, самообучающейся нейронной сети на базе многослойного персептрона.

Необходимо учитывать, что в основе сети на базе многослойного персептрона может быть сколько угодно слоев, но не менее 3.

Первый слой (*input layer*) будет отвечать за передачу входного сигнала всем персептронам следующих слоев (*hidden layer*), которые отвечают за сами вычисления на основе ранее рассчитанных весов (рис. 1, см. ниже).

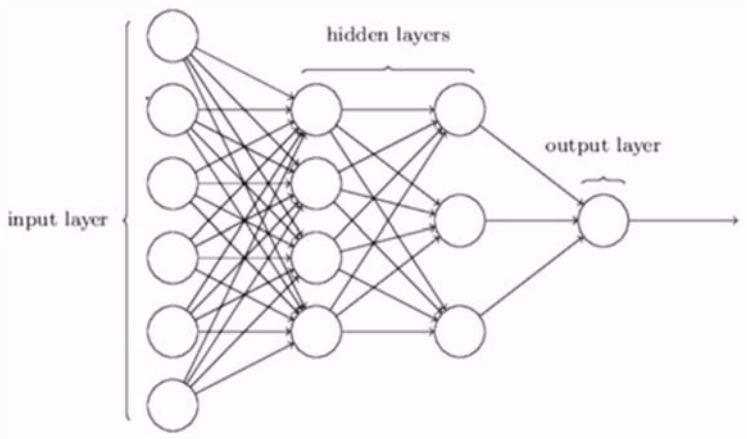


Рис. 1. Структура многослойного персептрона

Последний же слой (*output layer*) чаще всего состоит из одного персептрона, который отвечает за наиболее значимый процесс – на основе рассчитанных данных делает

«предсказание», которое сообщает системе валидный ли пользователь пытается аутентифицироваться в системе.

После анализа представленных подходов и решений можно заметить, что все подходы используют в своих расчетах вероятностные вычисления, а значит всегда будет вероятность того, что валидный пользователь может не аутентифицироваться, в отличие от злоумышленника. Такие вероятности называются показателями эффективности алгоритмов.

Показатели эффективности алгоритмов

Для анализа эффективности алгоритмов клавиатурного почерка наиболее важными будут являться:

– FAR, или ошибка первого рода – коэффициент ложного пропуска, который отражает процент возникновения ситуаций, когда алгоритм дает доступ незарегистрированному пользователю;

– FRR, или ошибка второго рода – коэффициент ложного отказа, который отражает процент возникновения ситуаций, когда алгоритм отказывает в доступе зарегистрированным пользователям.

Показатели FAR и FRR зависят от уровня чувствительности алгоритма – чем выше чувствительность к передаваемым данным, тем больше ошибок второго рода, но меньше ошибок первого рода. Если чувствительность меньше, то ситуация обратная – ошибок второго рода меньше, а ошибок первого рода больше.

Также существуют ситуации, когда показания уровня чувствительности приводят к одинаковому количеству ошибок первого и второго рода. Такой показатель носит название EER, или равная частота ошибки. Эффективность алгоритма будет оцениваться на основе данного показателя – чем меньше значение EER, тем эффективнее считается алгоритм (рис. 2).

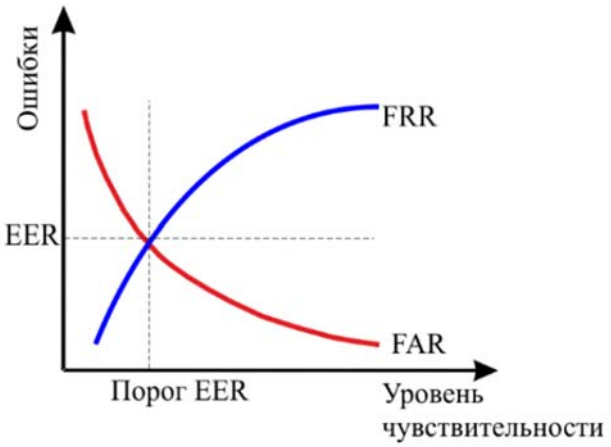


Рис. 2. График зависимости ошибок FAR и FRR от уровня чувствительности

В настоящее время не существует алгоритма, который позволил бы снизить значение ошибок первого и второго родов до нуля, а значит нет такой системы, которая гарантировала бы абсолютно корректную работу алгоритма при аутентификации валидных пользователей и отсутствии вероятности ошибочной аутентификации злоумышленника.

Главной итоговой целью разработки самообучающейся нейронной сети на базе многослойного персептрона является снижение количества данных для обучения сети, а также минимизация ошибок первого и второго родов.

Список используемых источников

1. Ворона В. А., Тихонов В. А. Системы контроля и управления доступом. М. : Горячая линия – Телеком, 2010. 274 с.

2. Fabian Monrose, Aviel D. Rubin. Keystroke dynamics as a biometric for authentication. 2017 [Электронный ресурс] // URL: https://www.cs.jhu.edu/~fabian/papers/fgcs.pdf (дата обращения: 16.03.2020).

3. D. Shanmugapriya, G. Padmavathi. A Survey of Biometric keystroke Dynamics: Approaches, Security and Challenges // International Journal of Computer Science and Information Security, Vol. 5, No. 1, 2009.

Статья представлена заведующим кафедрой ЗЗС СПбГУТ, кандидатом технических наук, доцентом А. В. Красовым.

УДК 004.8
ГРНРТИ 28.23

КЛАССИФИКАЦИЯ УЯЗВИМОСТЕЙ ИНТЕРФЕЙСОВ ТРАНСПОРТНОЙ ИНФРАСТРУКТУРЫ УМНОГО ГОРОДА

Л. А. Виткова[1,2], К. Е. Израилов[1,2], А. А. Чечулин[1,2]

[1]Санкт-Петербургский государственный университет телекоммуникаций им. проф. М. А. Бонч-Бруевича
[2]Санкт-Петербургский институт информатики и автоматизации Российской академии наук

В статье рассматривается задача классификации уязвимостей интерфейсов транспортной инфраструктуры умного города. Для этого применяется подход категориального деления уязвимостей по следующим парам: Человек VS Машина, Внутрь VS Наружу, Алгоритм VS Данные, Статический VS Динамический, комбинация которых позволяет выделить 16 классов. Также, приводится концептуальная модель транспортной инфраструктуры с интерфейсами и их уязвимостями.

уязвимости интерфейсов, умный город, транспортная инфраструктура, категориальное деление.

Введение

Одной из основных тенденций современного мира по праву может считаться интеллектуализация всех сфер жизнедеятельности. Причиной этого

являются возросшие потребности текущего общества потребителей при невозможности их удовлетворения существующими технологиями без реализации определенных творческих функций. Как следствие, появляются такие концепции, как «умный дом» и «умный город», цель которых заключается в улучшении качества жизни людей за счет информатики. Не считается исключением и транспортная инфраструктура умного города (далее – ТИ), перевод которой в разряд интеллектуальных систем, очевидно, сможет существенно повысить эффективность (т. е. результативность, оперативность и ресурсоэкономность) пассажир-перевозок, что существенно повлияет и на итоговую комфортность. Тем не менее, как и любая новая неотработанная технология, она несет определенные угрозы субъектам/объектам, для которых была разработана. Одной из причин этого можно считать уязвимости в ее элементах и процессах функционирования по причине сложности их предсказания и нейтрализации до непосредственного внедрения и «обкатки» [1]. Критичностью уязвимостей для ТИ является то, что даже одна реализованная в результате угроза может принести не только экономический ущерб, но и реальные человеческие жертвы (например, в результате ДТП).

Таким образом, *выявление уязвимостей ТИ* теоретическими методами – т. е. в отличии от практических, до реальных экспериментов – является актуальной **проблемой**. Инфраструктура обобщенно может быть представлена в виде следующих 3-х взаимодействующих групп элементов: людей – потребителей транспортных услуг; транспортных средств – подвижных объектов, обеспечивающих передвижение потребителей услуг; сервисов – элементов, обеспечивающих вспомогательные функции по координации, оптимизации, контролю выполнения услуг и пр. Также, важнейшей стороной функционирования ТИ можно считать взаимодействие этих групп. И если уязвимости (и, как следствие, результирующие угрозы) элементов каждой группы в некоторой степени можно считать изученными и частично нейтрализуемыми (например, для людей – в областях психологии, социологии, правил дорожного движения и пр., для транспортных средств – в областях конструктивной безопасности, эксплуатационных свойств автомобилей и пр., для сервисов – в областях безопасности программно-аппаратного обеспечения, теории массового обслуживания [2, 3, 4] и пр.), то уязвимостям, появляющимся на стыке элементов – т. е. в интерфейсах их взаимодействия – на сегодняшний день необходимого внимания не уделяется. Под интерфейсами понимается именно не идеализированное понятие, как общая граница между двумя функциональными объектами (изучение чего будет бесполезным с практической точки зрения), а совокупность средств, обеспечивающих передачу информации между объектами – дисплеи, клавиатуры, считыватели карт, GPS, Wi-Fi, громкоговорители, микрофоны и пр. При этом, для каждой такой передачи

средством используется пара компонент-антагонистов, работающих с различными *формами* информации (звуковыми, визуальными, тактильными, цифровыми и пр.), связанных понятным обоим сторонам информационным каналом, обеспечивающим корректную передачу *содержания* [5]. Уязвимости же в интерфейсах оказывают влияние на передаваемое содержание, поскольку оно начинает по-разному интерпретироваться противоположными обработчиками информации (из-за нарушения структуры форм). Концептуальная модель такой ТИ с интерфейсами и их уязвимостями показана на рис. 1 (серый цвет – ТИ, синий – элементы ТИ и их взаимодействие, зеленый – форма информации, оранжевый – передача содержание, красный – уязвимость интерфейса).

Согласно рис. некоторая информация в ТИ (ее содержание) передается от транспортного средства к человеку через интерфейс с уязвимостью (с преобразованием от Формы 1 к Форме 2), в результате чего содержание информации меняется. Например, автомобиль может предупредить о приближении опасного участка пути на незнакомом водителю языке, что не позволит последнему вовремя снизить скорость.

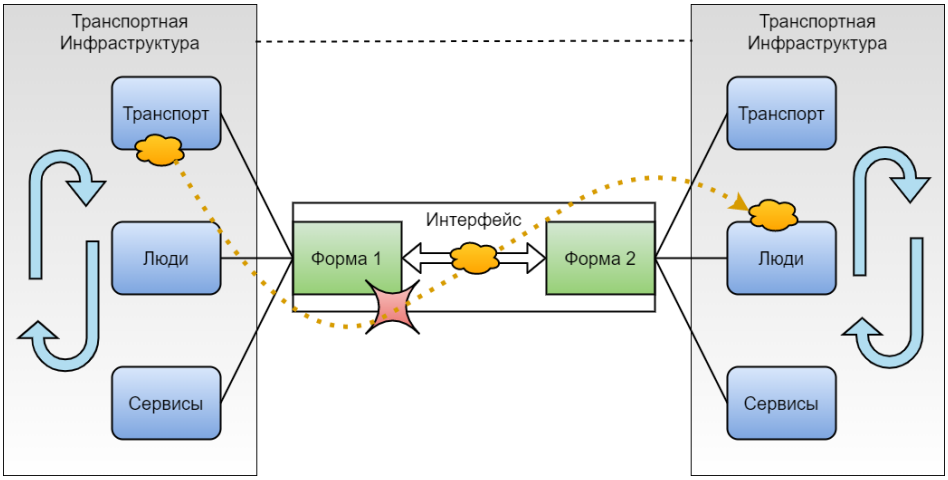


Рис. Концептуальная модель ТИ с интерфейсами и уязвимостями

Также, уже сейчас существует такой термин, как – «говорящие вирусы», обозначающий новое направление компьютерных атак, осуществляемых в интеллектуальных системах и проявляющихся в том, что «зараженные» выходные интерфейсы озвучивают некорректные голосовые команды, воспринимаемые входными интерфейсами тех же систем, что приводит к выполнению деструктивных действий.

Исходя их вышесказанного, актуальнейшей **задачей** можно считать *изучение* именно *уязвимостей интерфейсов ТИ*. Первым этапом решения задачи должно стать введение однозначной классификации таких уязвимостей, которая позволит как определить основной их состав, так и выделить особенности каждого класса.

Классификация уязвимостей

Достаточно хорошо себя зарекомендовавшим подходом, применимым для синтеза новых классификаций, обладающим при этом *необходимостью* (минимизацией объектов каждого класса, из чего, также, следует отсутствие их перекрытий) и *достаточностью* (покрытием классами всего множества объектов, что означает отсутствие «забытых» объектов) является категориальное деление [6, 7]. Идея последнего заключается в выделении набора категориальных пар (элементов, являющихся по некоторому признаку противоположными) с последующей комбинацией каждого элемента пары, давая таким образом 2^N классов, где N – количество пар. Это следует из того, что каждая пара как бы *расслаивает* классифицируемое множество на 2 противоположные группы; соответственно, две пары *расслаивают* множество на 4 группы и т. д.

В интересах решения задачи классификации уязвимостей было выполнено следующее их категориальное деление с выделением 4-х пар, каждая из которых отражает возможные аспекты нарушения содержания передаваемой информации (через ошибки в реализации ее форм-обработчиков). Во-первых, поскольку через интерфейсы ТИ может передаваться как человекоориентированная, так и машиноориентированная информация, то это позволяет выделить категориальную пару – **Ч**еловек VS **М**ашина. Во-вторых, каждый из интерфейсов может как получать информацию (работать на вход), так выдавать информацию (работать на выход), что позволяет говорить о категориальной паре – **В**нутрь VS **Н**аружу. Более логичным названием элементов данной пары могло быть стать использование терминов Вход/Выход; однако, как будет показано далее, это не позволит сделать именование получаемых классов лаконичным (из-за совпадения первых букв терминов). В-третьих, устройство-интерфейс, как и любое программно-аппаратное средство, состоит из некоторых алгоритмов (т. е. последовательно выполняемых шагов) и их данных (т. е. входных и собственных параметров алгоритмов), а значит целесообразно ввести категориальную пару – **А**лгоритм VS **Д**анные. И, в-четвертых, следуя из специфики ТИ, как системы подвижных объектов, взаимодействующих друг с другом и с неподвижным окружением, логично использовать категориальную пару – **С**татический VS **Д**инамический. Необходимо отметить, что каждая из предложенных пар разделяет множество всех уязвимостей на достаточно ровные множества (близкие по мощности), поскольку используемые для деления признаки категорий полностью отражают специфику интерфейсов ТИ – взаимодействие человека и машины, двухсторонний обмен информацией, программно-аппаратные решения, статико-динамическая система. Комбинация элементов всех пар позволяет ввести $2^4 = 16$ классов, которые, как было указано ранее, обладают необходимостью и достаточностью – т. е. являются в широком смысле «идеальным» делением уязвимостей интерфейсов.

При этом, каждый класс может быть проидентифицирован первыми буквами названий каждого из элементов пар (буквы выделены ранее жирным шрифтом): ЧВАС, МВАС, ЧНАС, МНАС, ЧВДС, МВДС, ЧНДС, МНДС, ЧВАД, МВАД, ЧНАД, МНАД, ЧВДД, МВДД, ЧНДД, МНДД.

Заключение

Применение категориального деления к уязвимостям интерфейсов ТИ позволило выделить 16 классов, каждый из которых отражает одну из особенностей уязвимостей интерфейсов. Однако, несмотря на корректность примененного методологического аппарата, данное деление все же носит чисто теоретический характер, основанный на ряде предположений; для обоснования же практической ценности проведенной классификации необходимо ее реальное применение. Для этого удовлетворительным может быть выделение нескольких типовых и качественно отличных уязвимостей интерфейсов ТИ и попытка отнесения их к выделенным классам. Успешность последнего подтвердит удачность классификации. Также, может потребоваться б***о***льшая детализация классов путем введение новых пар; например, с точки зрения числа источников/получателей информации – Один VS Много. Дальнейшим логичным продолжением будет классификация угроз, как используя подобное категориальное деление, так и взаимосвязь угроз с уже полученными классами уязвимостей. Все это планируется осуществить авторами в дальнейшем научном исследовании.

Работа выполнена при финансовой поддержке РФФИ (проект 19-29-06099 мк).

Список используемых источников

1. Vasily Desnitsky, Igor Kotenko, Andrey Chechulin. Configuration-based approach to embedded device security. Lecture Notes in Computer Science, Springer-Verlag // The Sixth International Conference "Mathematical Methods, Models and Architectures for Computer Networks Security" (MMM-ACNS-2012). October, 2012, St. Petersburg, Russia. PP. 270–285.

2. Lidia Vitkova, Vasily Desnitsky, Andrey Chechulin, Igor Kotenko. Approach to organizing of a heterogeneous swarm of cyber-physical devices to detect intruders // The 9th IFAC/IFIP/IFORS/IISE/INFORMS Conference "Manufacturing Modelling, Management and Control" (MIM 2019). August 2019, Berlin, Germany.

3. Десницкий В. А., Сахаров Д. В., Чечулин А. А., Ушаков И. А., Захарова Т. Е. Защита информации в центрах обработки данных : учебное пособие. СПб. : СПбГУТ, 2019. 92 с.

4. Буйневич М. В., Израилов К. Е. Исследование и моделирование угроз безопасности цифровой телекоммуникационной сети: отчет о НИР шифр «Цифровая угроза-2012» / СПбГУТ, 2012. рег. № 047-12-054. 219 с.

5. Израилов К. Е., Татарникова И. М. Подход к анализу безопасности программного кода с позиции его формы и содержания // Актуальные проблемы инфотелекомму-

никаций в науке и образовании (АПИНО 2019). VIII Международная научно-техническая и научно-методическая конференция : сб. науч. ст. в 4-х т. СПб. : СПбГУТ, 2019. С. 462–467.

6. Буйневич М. В., Израилов К. Е. Категориальный синтез и технологический анализ вариантов безопасного импортозамещения программного обеспечения телекоммуникационных устройств // Информационные технологии и телекоммуникации. 2016. Т. 4. № 3. С. 95–106.

7. Израилов К. Е., Покусов В. В., Столярова Е. С. Информационные объекты в системе обеспечения информационной безопасности // Теоретические и прикладные вопросы комплексной безопасности: материалы I Международной научно-практической конференции. 2018. С. 166–169.

УДК 004.056.53
ГРНТИ 81.93.29

ПРОТИВОДЕЙСТВИЕ РАСПРОСТРАНЕНИЮ НЕЖЕЛАТЕЛЬНОЙ ИНФОРМАЦИИ В ИНФОРМАЦИОННОМ ПРОСТРАНСТВЕ СОЦИАЛЬНЫХ СЕТЕЙ

Л. А. Виткова[1,2], М. А. Справцева[1]

[1]Санкт-Петербургский государственный университет телекоммуникаций им. проф. М. А. Бонч-Бруевича
[2]Санкт-Петербургский институт информатики и автоматизации Российской академии наук

Социальные сети используются для общения, в них открыто рассказывают о своих интересах и публикуют различные записи. И обеспечение информационной безопасности в социальных сетях является одной из приоритетных задач государства, так как сегодня такие сети являются и площадкой для распространения нежелательной информации. В статье рассматриваются различные методы, модели, алгоритмы и сервисы противодействия распространению нежелательной информации (кибербуллингу).

нежелательная информация, кибербуллинг, меры противодействия, социальные сети.

Согласно исследованиям, проведенным платформами We Are Social и Hootsite в 2019 году, в социальных сетях (СС) зарегистрировано 3,48 миллиарда пользователей. 2 часа 16 минут – столько времени проводит средний пользователь на социальных платформах [1, 2]. Такие платформы используются для общения, в них открыто рассказывают о своих интересах и публикуют различные записи. Но помимо этого СС используются для распространения нежелательной информации, что делает противодействие такой информации актуальной задачей для государства.

В настоящее время в социальных сетях можно встретить огромное количество нежелательной информации. Одним из типов такой информации является кибербуллинг. Кибербуллинг – это намеренные действия агрессивного характера, направленные на причинение морального вреда жертве посредством запугивания, оскорблений, унижений, травли, производимые в интернет пространстве через социальные сети и другие площадки [3]. Чаще всего, кибербуллингу подвергаются подростки. Согласно данным Регионального общественного центра интернет-технологий (РОЦИТ) 50 % подростков в возрасте от 14 до 17 лет становились жертвами кибербуллинга [4, 5].

На сегодняшний день в России на законодательном уровне пользователь социальных сетей не защищен от интернет-травли. Но одновременно с этим, Организация Объединённых Наций (ООН) расценивает кибербуллинг как психологическое и физическое насилие. Против этого действует ст. 19 Конвенции ООН по правам ребёнка [6].

В работе [7] авторы предлагают ряд мер, которые могут быть предприняты: как организационные, так и технические.

Ошибки в сообщениях в социальных сетях делают обнаружение кибербуллинга сложной задачей. Авторы в [8] предлагают новую сверточную нейронную сеть (PCNN). В работе использовались данные, собранные в Twitter и Formspring.me. Результаты эксперимента показали, что PCNN может достигать улучшенного запоминания и точности по сравнению с базовыми сверточными нейронными сетями.

В октябре 2017 года на хакатоне «ВКонтакте» был представлен проект PyTidor [9]. Были созданы бот для диалогов в Telegram и бот-фильтр для сообществ ВКонтакте. Эти боты являются обученной нейронной сетью, которая распознает, является ли текст агрессивным или токсичным. Помимо этого, боты могут предупреждать пользователя об агрессивном поведении и если поведение не меняется, то направляется оповещение администратору чата.

В [10] авторы предлагают использовать методы машинного обучения, такие как Random Forest, k-Nearest Neighbor, Sequential Machine Optimization, и Naive Bayes, чтобы выявлять и обнаруживать присутствие или отсутствие киберзапугивания в видео-комментариях YouTube. Эксперимент проводился с расширением инструментария Weka [11] и с использованием данных, собранных из комментариев на YouTube, в которых затрагивались такие важные темы, как раса, культура, пол, сексуальность и физические характеристики.

Сегодняшние юные пользователи Интернета создали интерактивный мир вдали от взрослых и их надзора. Только 17 % подростков, которые являются жертвами кибербуллинга, обращаются за помощью к родителям. И проблема в том, что существует разрыв в понимании технологий между

родителями и детьми. Родители расценивают Интернет и социальные сети как практические инструменты, к примеру, для помощи в образовании, но ребёнок же относится к этому абсолютно иначе и проводит там большинство своего времени, обмениваясь мгновенными сообщениями со сверстниками и делясь медиа-контентом. Microsoft Launcher [12] предлагает форму родительского контроля, которые позволяют родителям следить за интернет-активностью своих детей.

Также существуют такие приложения, как Net Kids [13], Kindergate Родительский контроль [14], компонент Kaspersky Internet Security [15], «Родительский контроль» от МТС [16] и Мегафон [17]. Эти средства блокируют опасные и мошеннические сайты, настраивают режим доступа в Интернет, ведут отчет с посещением различных информационных ресурсов. Однако алгоритмы обнаружения и противодействия кибербуллингу пока в них не используются.

В ходе исследовательской работы были рассмотрены существующие различные методы противодействию кибербуллингу. Исследование показало, что, несмотря на множество сервисов родительского контроля, внедренных алгоритмов противодействия кибербуллингу пока не существует. Представляется актуальным разработка моделей, алгоритмов и методик противодействия нежелательной информации (кибербуллингу) в сети Интернет.

Работа выполнена при частичной финансовой поддержке Российского научного фонда (проект № 18-71-10094).

Список используемых источников

1. Digital 2019: Global Internet Use Accelerate [Электронный ресурс]. URL: https://wearesocial.com/blog/2019/01/digital-2019-global-internet-use-accelerates

2. Левкин И. М., Науменко К. А., Виткова Л. А. Особенности информационно-психологического воздействия в Интернете // Информационная безопасность регионов России (ИБРР-2017) материалы конференции, 2017. С. 364–367.

3. Кибербуллинг [Электронный ресурс]. URL: https://dnevnik-znaniy.ru/znaj-i-umej/kiberbulling-chto-eto-kak-zashhitit-sebya-i-detej.html

4. Кибербуллинг вне закона [Электронный ресурс]. URL: https://rocit.ru/news/responsibility-for-cyberbullying

5. Виткова Л. А., Потехин И. Ю., Сахаров Д. В. Проблема выявления информационно-психологического воздействия в информационной инфраструктуре Российской Федерации // Актуальные проблемы инфотелекоммуникаций в науке и образовании. VI Международная научно-техническая и научно-методическая конференция : сб. науч. ст. в 4-х т. СПб. : СПбГУТ, 2017. С. 166–170.

6. Конвенция о правах ребенка [Электронный ресурс]. URL: https://www.un.org/ru/documents/decl_conv/conventions/childcon.shtml

7. Виткова Л. А., Дойникова Е. В., Котенко И. В. Модель мер противодействия нежелательной, сомнительной и вредоносной информации в сети Интернет // Актуальные проблемы инфотелекоммуникаций в науке и образовании. VIII Международная научно-

техническая и научно-методическая конференция : сб. науч. ст. в 3- х т. СПб. : СПбГУТ, 2019. С. 223–227.

8. Kumar, A., Nayak, S., & Chandra, N. (2018). Empirical Analysis of Supervised Machine Learning Techniques for Cyberbullying Detection // Lecture Notes in Networks and Systems, pp. 223–230.

9. PyTidor [Электронный ресурс]. URL: https://thevyshka.ru/15015-hakathon/

10. Kumar, A., Nayak, S., & Chandra, N. (2018). Empirical Analysis of Supervised Machine Learning Techniques for Cyberbullying Detection // Lecture Notes in Networks and Systems, 223–230.

11. Weka [Электронный ресурс]. URL: https://www.cs.waikato.ac.nz/~ml/weka/

12. Microsoft Launcher [Электронный ресурс]. URL: https://www.microsoft.com/en-us/launcher

13. Net Kids [Электронный ресурс]. URL: https://netkidscontrol.ru/

14. Kindergate Родительский контроль [Электронный ресурс]. URL: http://kindergate-parental-control.com/ru

15. Компонент Kaspersky Internet Security [Электронный ресурс]. URL: https://www.kaspersky.ru/internet-security

16. МТС «Родительский контроль» [Электронный ресурс]. URL: https://spb.mts.ru/personal/mobilnaya-svyaz/uslugi/mobilnaya-svyaz/kontrol-interneta

17. Мегафон «Родительский контроль» [Электронный ресурс]. URL: https://spb.megafon.ru/services/security/roditelskiy_kontrol/

Статья представлена научным руководителем, доцентом кафедры ЗСС СПбГУТ, кандидатом технических наук, доцентом А. А. Чечулиным.

УДК 004.5
ГРНТИ 81.93.29

ЭВРИСТИЧЕСКИЕ МЕТОДЫ АНАЛИЗА ТРАФИКА

Л. А. Виткова[1,2], В. И. Темченко[1], А. А. Чечулин[1,2]

Санкт-Петербургский государственный университет телекоммуникаций им. проф. М. А. Бонч-Бруевича
Санкт-Петербургский институт информатики и автоматизации Российской академии наук

Обнаружение сетевых атак является в данный момент одной из наиболее острых проблем информационной безопасности телекоммуникационных сетей. Существуют различные способы предупреждения атак – антивирус, межсетевой экран, системы предотвращения вторжений уровня хоста и др. Но зачастую таких «активных» мер бывает недостаточно и поэтому используются «пассивные» механизмы – системы обнаружения вторжений. При этом, большинство таких систем работает на основе сигнатурных подходов и методов. Практика показывает, что сигнатурного подхода недостаточно для обеспечения информационной безопасности сети. Авторы рассматривают эвристическое методы выявления аномальной активности в трафике и исследуют возможности применения таких подходов в системах обнаружения вторжений.

анализ трафика, методы обнаружения аномалий, эвристические методы анализа, аномалии трафика.

Введение

Обеспечение защиты от различного рода атак является одной из главных задач в современных системах и сетях. Существуют различные способы противодействия атакам и зачастую они все осуществляют защиту с использованием уже известной информации о атаке. Однако, все методы противодействия предполагают обнаружение атаки, но если у последней изменяется вид, профиль, способ воздействия или другой аспект, то такая атака может быть пропущена. Поэтому в настоящее время актуальной задачей является разработка систем обнаружения атак, основанных на новейших подходах к анализу данных. Существует много различных методов, на основе которых можно построить подобную систему, но всех их можно разделить на два типа: сигнатурные и эвристические. Сигнатурные методы связаны как раз с теми способами противодействия, указанными ранее – изменение этой самой сигнатуры, часто не дает верно определить опасность.

В данной работе представлен обзор различных методов эвристического анализа и оценена возможность их применения в системах обнаружения вторжений.

Принцип работы эвристического анализа

Для начала стоит понять, в чем основное отличие эвристического анализа от сигнатурного. Эвристический анализ очень сильно подвержен возможности ошибочного результата. Если за счет точного знания сигнатуры ошибиться нельзя – есть точные признаки для определения аномалии, то в случае с эвристическим методом – задается начальный набор общих параметров, на основе которых проверяется результат. Данный подход возможно использовать даже в том случае, если известно, что он выдает не верный результат, но только если этот случай можно хорошо выделить, или же в случае если результат неточен, но эта погрешность считается приемлемой.

В эвристическом анализе существует понятие оценки результата или так называемого «фильтра здравого смысла». На выходе результат критически оценивается – это приводит к тому, что ситуация улучшается: когда ошибка, выдаваемая подобным анализом, слишком мала, чтобы быть заметной – цена такой ошибки низка, а если пропущенная ошибка будет серьезной – значит она будет отсеяна «фильтрацией», следовательно, не нанесет существенного вреда.

Производить подобную фильтрацию способен человек – он видит выдаваемую ошибку и делает уточнение в настроенных параметрах. Но в реа-

лиях оценки аномалий трафика данных – это огромный объем работы, с которым человеку не справиться. Поэтому используются специальные механизмы, которые могут заменить человека на этом посту – машинное обучение и вычислительный интеллект. Человек будет производить такие же действия, как и в обычном случае оценки результата, но с той разницей, что при этом алгоритм будет определять – верен ли результат эвристического анализа, а человек – верен ли результат машины. Тем самым производится «обучение» алгоритма для определения ошибки анализа [1].

Классификация эвристических методов и их применение

Методы машинного обучения. Данные методы анализа сводятся к построению специализированных моделей (математические), которые, в случае с обнаружением аномалий, используют шаблоны поведения трафика сети, в виде основного набора данных. Используемые шаблоны могут включать как нормальное, так и аномальное поведение сетевого трафика.

Рассмотрим основные методы машинного обучения, применяемые для обнаружения аномального трафика более подробно.

Деревья решений – это специальное средство для поддержки в принятии решения, которое состоит из «веток» и «листьев». На рёбрах («ветках») дерева решения записаны атрибуты, от которых зависит целевая функция, в «листьях» записаны значения целевой функции, а в остальных узлах – атрибуты, по которым различаются случаи. Чтобы классифицировать новый случай, надо спуститься по дереву до листа и выдать соответствующее значение. Цель состоит в том, чтобы создать модель, которая предсказывает значение целевой переменной на основе нескольких переменных на входе [2]. При анализе трафика можно выставлять как атрибуты – основные составляющие IP-пакета и определять вероятность возможного события в случае принятия какого-либо решения. Основные преимущества – это простота интерпретации для человека, не требует подготовленных данных, работает с любыми переменными (в отличие от другие, которые работают только с определенным набором) и является надежным методом, так как даже при нарушении первоначальных предположений – продолжает хорошо работать.

Байесовские сети – это модель, кодирующая вероятностные отношения между переменными (событиями) и предоставляет возможность вычисления условных вероятностей их наступления [3]. Эта модель имеет такой же графово-вероятностный вид, как и деревья решений и по сути является направленным ациклическим графом, каждой вершине которого соответствует случайная переменная, а дуги графа кодируют отношения условной независимости между этими переменными. Байесовский метод является частным случаем модели байесовской сети, который называется наивным

байесовским классификатором. В этом случае предположения о независимости переменных будут являться строгими. За счет зависимости от строгости вероятностной модели – такие классификаторы очень эффективно обучаемы. В [4] авторы показали наглядный способ работы наивного байесовского классификатора, за счет которого смогли создать обучающие выборки для других методов, например, нейронные сети. Особенность данных выборок состоит в том, что они происходят на коротком интервале, позволяя сильно сократить время получения обучающей модели.

MAP-сплайны служат для построения аппроксимации поведения субъектов генерации трафика по определенным параметрам. Для этого избирается набор базисных функций, на основе которых вычисляются коэффициенты. Вычисление происходит линейно по заданному базису и обучающим векторам.

Также к этим всем методам относятся алгоритмы кластеризации и регрессии. Первое сводится к разбиению множества объектов на группы, которые называются кластеры, где внутри каждой группы должны оказаться объекты «похожие» друг на друга, а объекты разных групп должны максимально отличаться. Производится выборка объектов, затем определяется множество переменных, по которым оцениваются объекты выборки. После вычисляется значение меры сходства между объектами и применение метода кластерного анализа для создания групп схожих объектов [5].

Во втором производится моделирование измеряемых данных и исследование их свойств. Данные являются парами значений: зависимой переменной и независимой. Параметры модели настраиваются таким образом, что модель наилучшим образом приближает данные. Критерием качества приближения (целевой функцией) обычно является среднеквадратичная ошибка. Регрессионный анализ используется для прогноза, анализа временных рядов, тестирования гипотез и выявления скрытых взаимосвязей в данных [6].

Методы вычислительного интеллекта. Если предыдущий набор методов и алгоритмов причисляются как математические модели, то в случае методов вычислительного интеллекта берут свой принцип работы из биологических процессов, хотя тоже являются математическими моделями.

Нейронные сети является наиболее распространенным и известным методом. Они представляют собой набор обрабатывающих элементов – нейронов и связывающих их между собой – синапсы. Последние также преобразуют наборы входных значений в наборы желаемых выходных значений. Нейронные сети могут обучаться по образцам и обобщениям из неполных или зашумленных данных.

Генетические алгоритмы представляют собой имитацию биологических принципов естественного отбора. Формирование задачи идет так,

чтобы можно было закодировать в виде «генотипа» (вектора генов), где каждый ген может быть битом, числом или другим объектом. Будут выбрано множество решений («поколения») из которого выбираются лучшие (обычно лучшие «особи» имеют большую вероятность быть выбранными) и к ним применяются генетические операторы типа «скрещивания» и «мутации». Результатом данных действий будет являться получение новых решений. Данные набор действий повторяется итеративно, что и моделирует «процесс эволюции», который может продолжаться в несколько циклов, пока не выявятся критерии остановки генетического алгоритма [7].

Иммунные системы являются подобием человеческой иммунной системы, которые построены на принципах работы последней. Хотя иммунная система человека изучена далеко не до конца, уже на теориях её работы построены вычислительные прототипы иммунной системы. Основными механизмами являются обучение детекторов срабатывания, уничтожения детекторов с ложными срабатываниями и ответную реакцию на чужеродные объекты. Основным преимуществом будет являться наличие памяти у такого метода [8].

Среди других подходов стоит отметить нечеткую логику [9] и метод опорных векторов [10].

Заключение

В данной работе были рассмотрены различные методы эвристического анализа трафика и возможности их применения, а также проведена классификация данных методов. Данные методы довольно активно используются разработчиками и научным сообществом. Такой анализ позволяет производить выбор наиболее удобных методов не только для отдельного применения последних, но и для их совмещения. А также при знании сигнатурных методов возможно построение гибридных систем, которые будут представлять из себя более адаптивные методы решений по анализу аномалий трафика.

Работа выполнена при финансовой поддержке Минобрнауки России в рамках Соглашения о предоставлении субсидии № 05.607.21.0322 в СПИИРАН.

Список используемых источников

1. Браницкий А. А., Котенко И. В. Анализ и классификация методов обнаружения сетевых атак // Труды СПИИРАН. 2016. № 2 (45). С. 207–244. doi.org/10.15622/sp.45.13.

2. Носков А. Н., Чечулин А. А., Тарасова Д. А. Исследование эвристических подходов к обнаружению атак на телекоммуникационные сети на базе методов интеллектуального анализа данных // Труды СПИИРАН. 2014. № 6 (37). С. 208–224. doi.org/10.15622/sp.37.13.

3. Золотин А. А., Левенец Д. Г., Зотов М. А., Бирилло А. И., Березин А. И., Иванова А. В., Тулупьев А. Л. Алгоритмы обработки и визуализации алгебраических байесовских сетей // Образовательные технологии и общество. 2017. № 20 (1). С. 446–457.

4. Терновой О. С., Шатохин А. С. Использование байесовского классификатора для получения обучающих выборок, позволяющих определять вредоносный трафик на коротких интервалах // Известия Алтайского государственного университета. 2013. № 1–1 (77). С. 151–153.

5. Обзор алгоритмов кластеризации данных [Электронный ресурс]. URL: https://habr.com/ (дата обращения 22.03.2020).

6. Замятин А. В. Введение в интеллектуальный анализ данных : учеб. Пособие. Томск : Издательский Дом Томского государственного университета, 2016. 120 с. ISBN 978-5-94621-531-2.

7. Саймон Д. Алгоритмы эволюционной оптимизации. М. : ДМК Пресс, 2020. 940 с. ISBN 978-5-97060-812-8.

8. Чернышев Ю. О., Григорьев Г. В., Венцов Н. Н. Искусственные иммунные системы: обзор и современное состояние // Программные продукты и системы. 2014. № 4 (108). С. 136–142.

9. Зубков Е. В., Белов В. М. Методы интеллектуального анализа данных и обнаружение вторжений // Вестник СибГУТИ. 2016. С. 118–133.

10. Шкодырев В. П., Ягафаров К. И., Баштовенко В. А., Ильина Е. Э. Обзор методов обнаружения аномалий в потоках данных // Second Conference on Software Engineering and Information Management. 2017. С. 50–56.

УДК 004.75
ГРНТИ 20.53.17

ПРОГРАММНОЕ ОБЕСПЕЧЕНИЕ ДЛЯ ОРГАНИЗАЦИИ РЕЕСТРА ХРАНЕНИЯ ДАННЫХ НА ОСНОВЕ ТЕХНОЛОГИИ BLOCKCHAIN

С. С. Владимиров, В. Ф. Гарифуллин

Санкт-Петербургский государственный университет телекоммуникаций им. проф. М. А. Бонч-Бруевича

Работа представляет структуру программного обеспечения для организации децентрализованного реестра на основе технологии Blockchain. Предложен подход к реализации и вариант построения системы распределенного хранения данных. Задана минимально реализуемая структура Blockchain. Рассмотрены алгоритмы взаимодействия элементов системы и криптографические методы для обеспечения безопасного хранения и передачи данных. Предусмотрена реализация программного интерфейса пользователя для различных операционных систем, включая мобильные операционные системы. Задача обеспечивает реализацию реестра общего назначения с возможностью окончательного конфигурирования под требования пользователя.

blockchain, реестр, криптография, распределённые системы.

В современном мире надежность и безопасность размещения данных в онлайн-системах хранения информации становятся все более важными. Большое количество современных публичных реестров как правило построены по централизованному принципу с резервированием и одновременно работа происходит только с одним из серверов. Это приводит к тому, что надежность такого реестра в любой момент времени может понизиться, а часть информации в нем – изменена без чьего-либо ведома. В настоящее время существуют технологии для децентрализованного обмена данными. Наиболее распространенные из них: BitTorrent и Gnutella [1]. Для реализации надежного защищенного реестра необходимо обеспечить достоверность последовательности, добавляемой в него информации и предоставить возможность вносить любые записи только ограниченному кругу лиц. Для решения этих задач предлагается использовать технологию Blockchain.

Blockchain – это цепочка блоков. В его минимальной реализации каждый блок содержит некоторую хранимую информацию, свою хэш-сумму и хэш-сумму предыдущего блока данных [2]. С помощью контрольных хэш-сумм обеспечивается правильная последовательность блоков данных. Если третье лицо захочет изменить информацию в одном блоке, ему необходимо будет пересчитать и заменить контрольные суммы во всех блоках, стоящих после измененного (рис. 1, см. ниже).

Для хеширования в предлагаемом реестре используется алгоритм SHA-256, который является наиболее употребимой хэш-функцией в Blockchain проектах [3]. Преимуществами функции SHA-256 являются ее безопасность и производительность, доказанные результатами тестов [4].

Децентрализованность системы Blockchain подразумевает, что обмен блоками происходит между множеством узлов, которые хранят всю цепочку и проверяют соответствие хэшей. При попытке внести в цепочку блок с недостоверным хэшем, остальные узлы отклоняют этот блок.

Для организации взаимодействия между узлами реестра предполагается неструктурированная одноранговая peer-to-peer сеть узлов хранения данных. В зависимости от поддерживаемого набора функций отдельные узлы выполняют различные роли. Основу сети составляют мастер-узлы, которые хранят и синхронизируют между собой полную актуальную версию распределенного реестра и авторитетно проверяют любые транзакции пользователей. Мастер-узлы работают в глобальной сети Интернет и постоянно доступны. Обычные узлы хранения содержат подмножество записей реестра и для выполнения или проверки транзакций обращаются к мастер-узлам, которые выполняют роль маршрутизаторов транзакций, фактически предоставляя узлам доступ ко всему реестру. Обычные узлы хранения допускают работу из локальных сетей через NAT. Отдельно выделяют специ-

альный тип мастер-узлов – узлы-валидаторы, которые проверяют транзакции и формируют из них новые блоки данных для записи в реестр. Узлы-валидаторы необходимы для того, чтобы избежать разделения блокчейна на несколько параллельных цепочек.

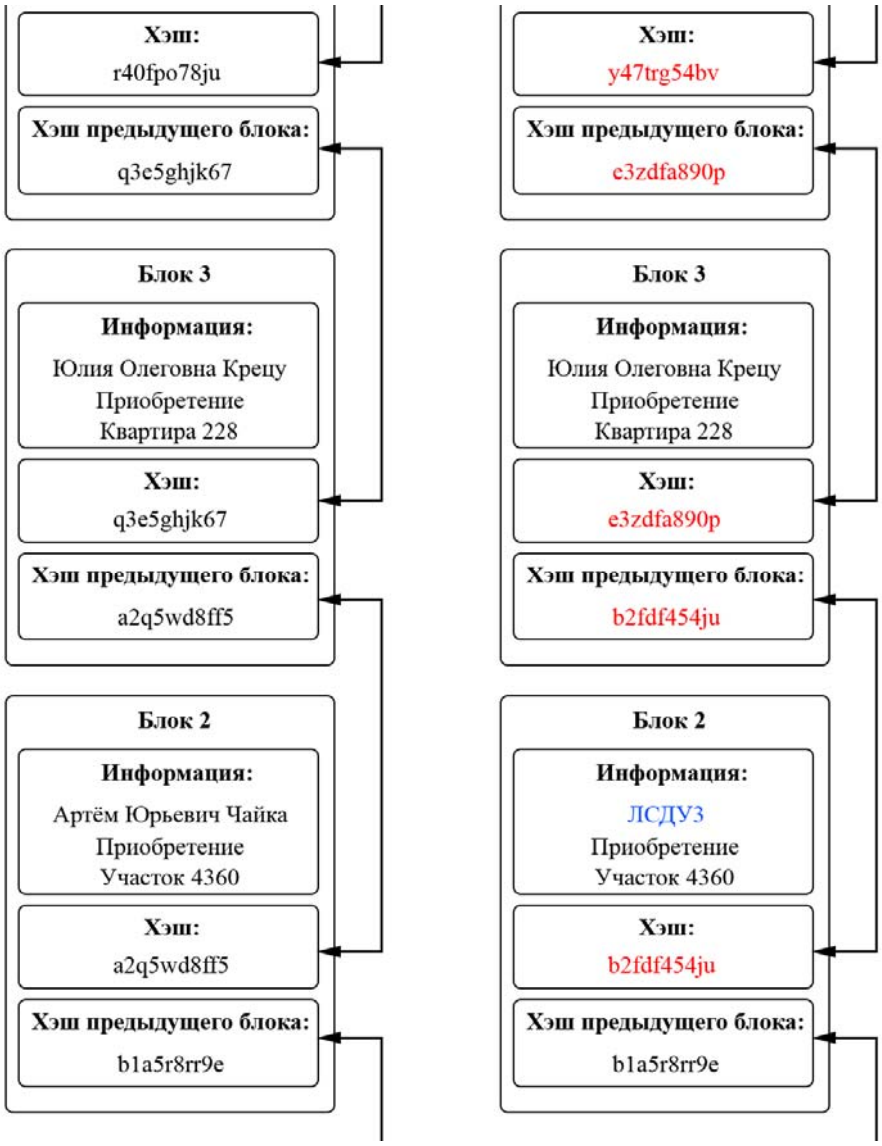


Рис. 1. Пример пересчёта хэшей при изменении информации в одном блоке

На рис. 2 изображен пример сети распределенного реестра, состоящей из двух узлов-валидаторов, одного мастер-узла, трех обычных узлов хранения и одного тонкого клиента. Тонким клиентом обычно является мобильное устройство, которое не хранит записи реестра, а лишь запрашивает и проверяет необходимые ему записи и проведенные транзакции у мастер-узла посредством специального интерфейса. В предлагаемом реестре для обмена информацией планируется использовать защищенный протокол HTTPS, а для организации работы с тонкими клиентами оптимально использовать веб-интерфейс.

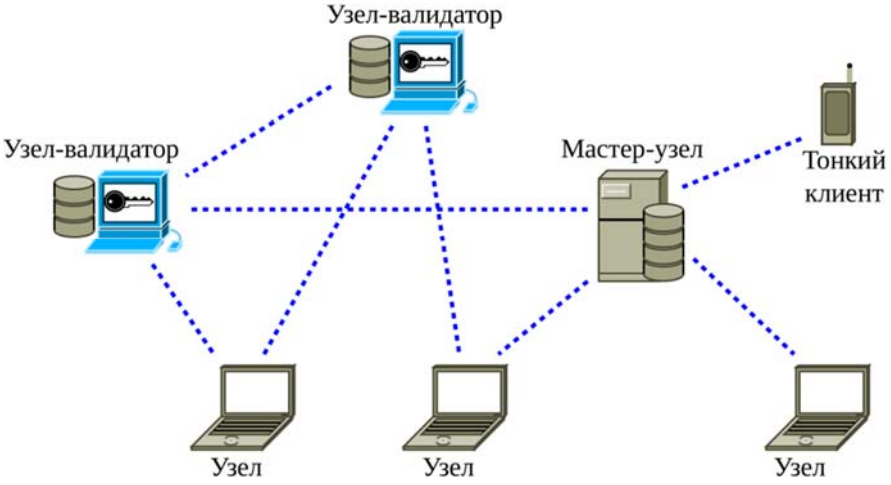


Рис. 2. Пример сети распределенного реестра

Для того чтобы дать возможность заносить данные в реестр только ограниченному кругу лиц, используется асимметричная криптография на эллиптических кривых [5]. Основное преимущество криптографии на эллиптических кривых – меньшая длина ключа. Аналогичный по уровню безопасности ключ алгоритма RSA будет длиннее в 26 раз [6]. Исходя из доступных средств разработки, тестов по безопасности [7] и производительности [8], оптимальным выбором криптографического алгоритма является Ed25519, основанный на схеме цифровой подписи EdDSA, использующей алгоритм хэширования SHA-512 и эллиптическую кривую, эквивалентную Curve25519 [9].

При одновременном добавлении информации в блокчейн не исключены коллизии [10]. Поэтому блоки формируются из нескольких транзакций и только после этого заносятся в блокчейн. В предлагаемом ПО транзакция с данными состоит из публичного ключа отправителя, типа транзакции, отправляемых данных, хэша транзакции и цифровой подписи отправителя. Для того, чтобы реестр можно было сконфигурировать под необходимую задачу, данные удобно представлять в формате JSON. Пример блока с одной транзакцией представлен в таблице (см. ниже).

При первоначальном развертывании реестра необходимо сгенерировать пары ключей (закрытый и открытый) для валидаторов и пользователей, имеющих право вносить информацию. Закрытые ключи хранятся только у их владельцев в зашифрованном с помощью алгоритма AES256 виде и доступны по паролю с локального устройства. Открытые ключи заносятся в самый первый блок данных реестра – генезис-блок, который поставляется вместе с программным обеспечением реестра на все узлы хранения.

Добавление новой информации в реестр происходит следующим образом:

1. Отправитель подписывает своим закрытым ключом данные, которые требуется внести в реестр.

ТАБЛИЦА. Пример блока с одной транзакцией

Описание	Пример данных
Публичный ключ валидатора	1FfmbHfnpaZjKFvyi1okTjJJusN455paPH
Хэш п редыдущего блока	25622fe23ca35eac3e32f9cdf77c381f7a536c5288c4f60421c5af3117a3534c
Транзакция	[{"from" : "1FfmbHfnpaZjKFvyi1okTjJJusN455paPH", "type" : "data", "data" : {"ФИО" : "Гарифуллин Валерий Флоритович", "Действие" : "Приобретение", "Собственность" : "Квартира 60" }, "hash" : "3EgVJs6d82ihMcTS7wkn477GnQUSzJJadG", "signature" : "90db022100e2ac980643b0b82c0e88ffdfec6b64e3e6ba35e7ba5fdd7d5d6cc8d25c6b2d3ee3738d9e1446618c4571d1941501"},]
Цифровая подпись валидатора	304502206e21798a42fae0e854281abd38bacd1aeed3ee3738d9e1446618c4571d190db d3ee3738d9e1446618c4571d19
Хэш блока	a665a45920422f9d417e4867efdc4fb8a04a1f3fff1fa07e998e86f7f7a27ae3

2. Данная транзакция отправляется напрямую или с помощью мастер-узла к узлам-валидаторам.

3. Узел-валидатор проверяет хэш транзакции и право отправителя информации добавлять данные в реестр с помощью цифровой подписи и открытых ключей в генезис-блоке.

4. Если цифровая подпись соответствует допустимому ключу в генезис-блоке, транзакция заносится в пул ожидающих транзакций.

5. По достижении лимита пула ожидающих транзакций выбирается узел-валидатор, который будет подписывать новый блок.

6. Выбранный узел-валидатор перепроверяет цифровые подписи и хэши ожидающих транзакций, формирует из них новый блок и подписывает его с помощью своего закрытого ключа.

7. При синхронизации реестра остальные узлы перепроверяют хэш-сумму и цифровую подпись нового блока и содержащихся в нем транзакций. Если проверка завершилась успешно, то блок сохраняется в памяти узла.

При необходимости в данной системе можно добавить или удалить валидаторы и пользователей, имеющих право вносить данные в реестр. Для подтверждения изменений среди существующих полноправных участников системы используется механизм голосования по большинству.

Предложенная система на базе технологии Blockchain может быть успешно применена для разработки публичных реестров с целью их децентрализации, увеличения надежности и прозрачности.

Список используемых источников

1. Erdely R., Kerle T., Levine B., Liberatore M., Shields C. Forensic Investigation of Peer-to-Peer File Sharing Network // Digital Investigation. 2010. Iss. 7. PP. 95–103.
2. Yaga D., Mell P., Roby N., Scarfone K. Blockchain Technology Overview // National Institute of Standards and Technology Interagency Report. 2018. 68 p.
3. Wang L., Shen X., Li J., Shao J., Yang Y. Cryptographic primitives in blockchains // Journal of Network and Computer Applications. 2019. Iss. 127. PP. 43–58.
4. Gupta P., Kumar S. A Comparative Analysis of SHA and MD5 Algorithm // International Journal of Computer Science and Information Technologies. 2014. Iss. 5. PP. 4492–4495.
5. Kikwai B. K. Elliptic Curve Digital Signatures and Their Application in the Bitcoin Crypto-currency Transactions // International Journal of Scientific and Research Publications. 2017. Iss. 7. PP. 135–138.
6. Sinha R., Srivastava H. K., Gupta S. Performance Based Comparison Study of RSA and Elliptic Curve Cryptography // International Journal of Scientific & Engineering Research. 2013. Iss. 4. PP. 720–725.
7. Bernstein D. J., Lange T. SafeCurves: choosing safe curves for elliptic-curve cryptography [Electronic resource]. URL: https://safecurves.cr.yp.to/ (Access date: 20.02.2020).
8. Shaikh J. R., Nenova M., Iliev G., Valkova-Jarvis Z. Analysis of standard elliptic curves for the implementation of elliptic curve cryptography in resource-constrained E-commerce applications // IEEE COMCAS. 2017. 4 p.
9. Samwel N., Batina L., Bertoni G., Daemen J., Susella R. Breaking Ed25519 in WolfSSL [Electronic resource] // Cryptology ePrint Archive. 2017. 20 p. URL: https://eprint.iacr.org/2017/985.pdf (Access date: 20.02.2020).
10. Gervais A., Karame G. O., Wust K., Glykantzis V., Ritzdorf H., Capkun S. On the Security and Performance of Proof of Work Blockchains [Electronic resource] // Cryptology ePrint Archive. 2016. 13 p. URL: https://eprint.iacr.org/2016/555.pdf (Access date: 19.02.2020).

УДК 621.396
ГРНТИ 49.37.29

РАЗРАБОТКА МОБИЛЬНОГО ЛАБОРАТОРНОГО СТЕНДА ДЛЯ ИССЛЕДОВАНИЯ ТЕХНОЛОГИИ LORA В ПЕРСПЕКТИВНЫХ СЕТЯХ ПЕРЕДАЧИ ДАННЫХ

С. С. Владимиров, А. С. Гутовский, И. Д. Неманов, А. И. Фомин

Санкт-Петербургский государственный университет телекоммуникаций им. проф. М.А. Бонч-Бруевича

Работа представляет мобильный лабораторный стенд для исследования технологии LoRa в перспективных сетях передачи данных. Приведены требования к техническим параметрам лабораторного стенда. Выполнен выбор аппаратной конфигурации приемопередатчиков LoRa и управляющих модулей элементов стенда с учетом особен-

ностей исследований. Проработан пользовательский управляющий интерфейс для стационарных и мобильных компьютерных терминалов. Представлены сценарии работы стенда при проведении исследований в рамках выполнения научно-исследовательских и опытно-конструкторских работ, а также варианты применения стенда в учебном процессе. Намечены шаги по дальнейшему развитию стенда.

лабораторный стенд, LoRa, измерения в радиосетях, IoV.

Технология беспроводной передачи данных LoRa (*Long Range*) представлена компанией Semtech для использования в системах Интернета вещей (*Internet of thing*s, IoT). Эта технология относится к радиотехнологиям большого радиуса действия и имеет низкое энергопотребление, относясь к технологиям Low Power Wide Area Network (LPWAN). Для технологии LoRa в Европе выделены частотные диапазоны 433 и 868 МГц [1].

LoRa получила широкое применение в сенсорных сетях [2], в системах сбора показаний счетчиков коммунальных платежей [3, 4], в сельском хозяйстве [5, 6] и системах «умного города» [7, 8]. Ведутся исследования по использованию технологии LoRa в перспективных сетях Интернета транспортных средств (*Internet of vehicles*, IoV) [9, 10].

Широкие возможности применения технологии LoRa вызывают необходимость изучения ее теоретических и практических аспектов в рамках соответствующих курсов университетского образования. На кафедре Сетей связи и передачи данных СПбГУТ разрабатывается мобильный лабораторный стенд, предназначенный как для обучения студентов, так и для проведения научно-практических исследований применимости LoRa в современных беспроводных сетях передачи данных.

Структура разрабатываемого стенда представлена на рис. 1. Прототип стенда состоит из четырех узлов, построенных на основе микроконтроллеров различного типа.

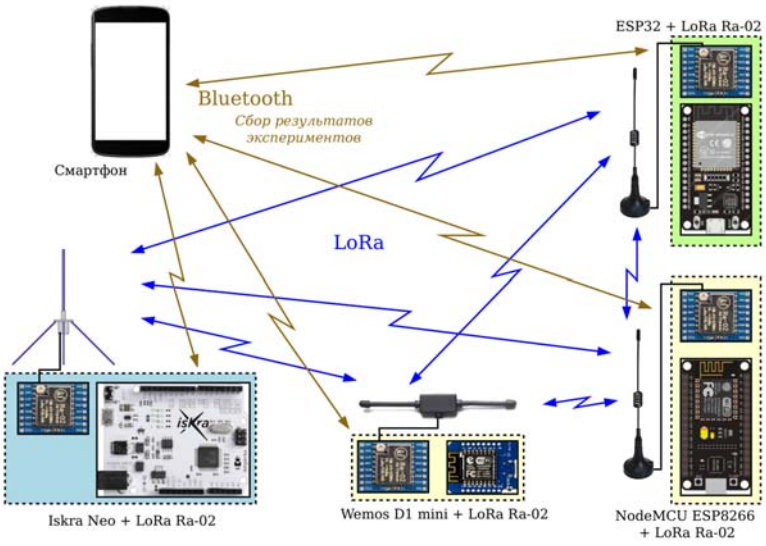


Рис. 1. Блок-схема прототипа мобильного лабораторного стенда LoRa

Блок-схема узла стенда показана на рис. 2.

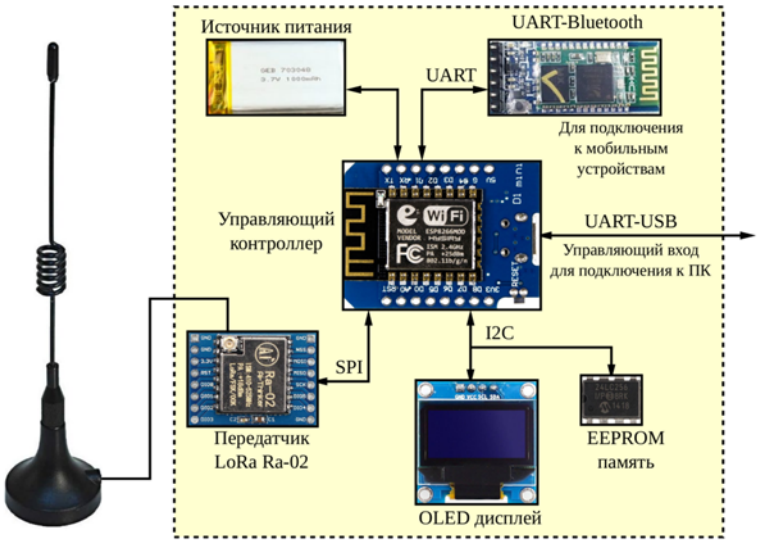


Рис. 2. Блок-схема узла мобильного лабораторного стенда LoRa

В качестве приемопередатчиков LoRa выбраны модули LoRa Ra-02 компании Ai-Thinker на основе чипа SX1278 производства Semtech. Модули подключаются по интерфейсу SPI и оснащены разъемом IPEX для подключения внешней антенны. Выбранные модули работают в безлицензионном частотном диапазоне LPD (от 433,075 до 434,750 МГц).

В таблице приведены параметры микроконтроллеров, управляющих работой узлов стенда.

ТАБЛИЦА. Параметры управляющих микроконтроллеров

Наименование	Iskra Neo	NodeMCU-32S	Wemos D1 Mini	NodeMCU V3
Тип контроллера	ATmega32U4	ESP32	ESP8266	
Процессор		Xtensa LX6	Xtensa L106	
Тактовая частота	16 МГц	2×160 МГц	80 МГц	
Память ОЗУ	2,5 КБ	520 КБ	96 КБ	
Память ПЗУ	32 КБ	448 КБ	4 МБ	64 КБ
Интерфейсы	UART, SPI, I2C, аналоговый вход (АЦП)			

Управление узлами сети предполагается производить двумя способами. Беспроводной интерфейс на основе модуля UART-Bluetooth позволит взаимодействовать с узлами посредством обычного смартфона и свободно распространяемой программы Serial Bluetooth Terminal. Для подключения к персональному компьютеру используется проводной UART интерфейс с переходным конвертером USB-UART. Вывод данных производится

на порт управляющего интерфейса или на дисплей, подключенный к узлу по последовательной шине I2C.

Для хранения настроек и состояния устройства используется микросхема флеш-памяти типа EEPROM, подключаемая четырехпроводной шиной I2C.

При использовании лабораторного стенда в рамках выполнения научно-исследовательских и опытно-конструкторских работ, а также в учебном процессе возможны два основных сценария:

1. Исследование соединений точка–точка для оценки уровня сигнала, отношения сигнал/шум и вероятности потери пакетов для различных дальностей передачи при различных параметрах сигнала и различных типов антенно-фидерных трактов.

2. Исследование сетей передачи данных, работающих поверх технологии LoRa, включая межсетевое взаимодействие с LAN и WAN сетями посредством шлюзового оборудования и протоколов.

Важным направлением использования стенда является изучение современных сетей интернета транспортных средств (IoV) – распределенной сети передачи данных в рамках взаимодействия самоорганизующихся автомобильных сетей (VANET) [11]. Наиболее актуальной задачей IoV становится предоставление автомобилям возможности взаимодействия в режиме реального времени с другими транспортными средствами, придорожной инфраструктурой и системами управления дорожным движением. Лабораторный стенд направлен на исследование сетевых сценариев взаимодействия автомобиль–автомобиль (V2V), которые поддерживают беспроводной обмен информацией о скорости и местоположении окружающих транспортных средств, и автомобиль–инфраструктура (V2I), соответствующих беспроводному обмену информацией между транспортным средством и вспомогательными придорожными устройствами (RSU) [10, 11].

Список используемых источников

1. Trinh L. H., Nguyen T., Phan D., Tran V., Bui V., Truong, N., Ferrero F. Miniature antenna for IoT devices using LoRa technology // 2017 International Conference on Advanced Technologies for Communications (ATC), Quy Nhon, Vietnam, 18-20 October 2017. IEEE, 2017. PP. 170–173.

2. Wixted A., Kinnaird P., Larijani H., Tait A., Ahmadinia A., Strachan N. Evaluation of LoRa and LoRaWAN for wireless sensor networks // 2016 IEEE Sensors, Orlando, FL, USA, 30 Oct. – 3 Nov. 2016. IEEE, 2017. PP. 1–3.

3. Таланов С. Б. Автоматизация учёта энергоресурсов ЖКХ с помощью сетей радиосвязи на основе технологии LoRa // Кулагинские чтения: техника и технологии производственных процессов: материалы XVIII Международной научно-практической конференции, г. Чита, 28–30 нояб. 2018 г. Чита : Изд. ЗГУ, 2018. С. 206–216.

4. Першина В. А., Титова Н. Д., Степанов Н. С. Построение автоматизированной системы сбора данных с приборов учета на базе стандарта LoraWAN // REDS: Телекоммуникационные устройства и системы. 2019. Т. 9. № 2. С. 3–9.

5. Tapashetti S., Shobha K. R. Precision Agriculture using LoRa // International Journal of Scientific & Engineering Research. 2018. Vol. 9. Iss. 5. PP. 2023–2028.

6. Петров М. Ю., Лебедев Н. В. LoraWAN: Интернет вещей в сельском хозяйстве // Инновационные подходы к развитию науки и производства регионов: материалы Национальной научно-практической конференции, г. Тверь, 12–14 фев. 2019 г. Тверь : Изд-во Тверской ГСХА, 2019. С. 433–435.

7. Панчук П. Интернет вещей в «умном городе» на примере сферы ЖКХ // Control Engineering Россия. 2019. № 1 (79). С. 42–44.

8. Мешкова Т. В. Умные города на базе Lora WAN // Мир дорог. 2019. № 121. С. 96.

9. Sanchez-Iborra R., Sanchez-Gomez J., Santa J., Fernandez P., Skarmeta, A. IPv6 Communications over LoRa for future IoV services // 2018 IEEE 4th World Forum on Internet of Things (WF-IoT), Singapore, 5–8 Feb. 2018. IEEE, 2018. PP. 92–97.

10. Vladimirov S. S., Karavaev D. A., Stepanov A. B., Yurchenko M. A., Vladyko A. G. An Application of LoRa Technology for SD-IoV Network // 11th International Congress on Ultra Modern Telecommunications and Control Systems and Workshops (ICUMT), Dublin, Ireland, 28–30 Oct. 2019. IEEE, 2019. P. 8970938.

11. Владимиров С. С., Владыко А. Г., Караваев Д. А., Помогалова А. В., Степанов А.Б. Испытательный стенд для исследования сети SD-IoV с технологией LoRa // Модернизация информационной инфраструктуры для сетей 5G/IMT 2020 и для других перспективных технологий в интересах трансформации регионов: материалы РОСИНФОКОМ-2019, Санкт-Петербург, 09 окт. 2019 г. СПб. : СПбГУТ, 2019. С. 21–30.

УДК 004.3, 51-37
ГРНТИ 50.33.14

АППАРАТНАЯ РЕАЛИЗАЦИЯ КАЛЬКУЛЯТОРА ЭЛЕМЕНТОВ ПОЛЯ ГАЛУА

С. С. Владимиров, С. С. Кошкин

Санкт-Петербургский государственный университет телекоммуникаций им. проф. М. А. Бонч-Бруевича

Работа представляет аппаратную реализацию калькулятора элементов двоичного поля Галуа, предназначенного для обеспечения учебного процесса. Выбраны алгоритмы для выполнения базовых операций над элементами поля. Приведены требования к техническим параметрам разрабатываемого устройства. Выполнен выбор аппаратной конфигурации калькулятора с учетом решаемых задач и заданных требований. Предложены варианты реализации интерфейса управления и аппаратного пользовательского интерфейса. Предлагаемая реализация представляет базовую модель и предусматривает дальнейшее развитие.

поля Галуа, микроконтроллер, ESP8266, пользовательский интерфейс.

Конечные поля Галуа являются важным элементом математического аппарата теории современных систем передачи данных (ПД). Элементы полей Галуа, в первую очередь двоичных, лежат в основе широко используемых методов помехоустойчивого кодирования и шифрования данных [1, 2]. Соответственно, знание математики конечных полей крайне важно для специалистов, занимающихся разработкой аппаратных и программных элементов систем ПД. В университетах при изучении теории помехоустойчивого кодирования и шифрования студенты должны решать практические задачи, связанные с расчетами в конечных полях Галуа. Расчеты в полях малых степеней могут сравнительно легко выполняться устно, однако, чем больше степень поля, тем сложнее проводить такие расчеты. В этих случаях необходимо применять соответствующие технические средства, к которым относятся системы компьютерной алгебры, такие как Matlab и GNU/Octave, и специализированные программы для расчетов в конечных полях [3, 4]. Однако, использование таких систем при выполнении аттестационных заданий ограничено, поскольку они работают на персональных ЭВМ общего назначения, с помощью которых учащиеся могут получить доступ к теоретической информации, что недопустимо при проведении текущей аттестации. Для решения данной проблемы на кафедре Сетей связи и передачи данных СПбГУТ была поставлена задача по разработке специализированного устройства, предназначенного для проведения расчетов в двоичных полях Галуа, так называемого аппаратного калькулятора Галуа.

Структура разрабатываемого калькулятора представлена блок-схемой на рис. 1. Ядро калькулятора выполнено на основе микроконтроллера, который производит все вычисления и осуществляет управление периферийными устройствами ввода-вывода и модулями оперативной и постоянной памяти.

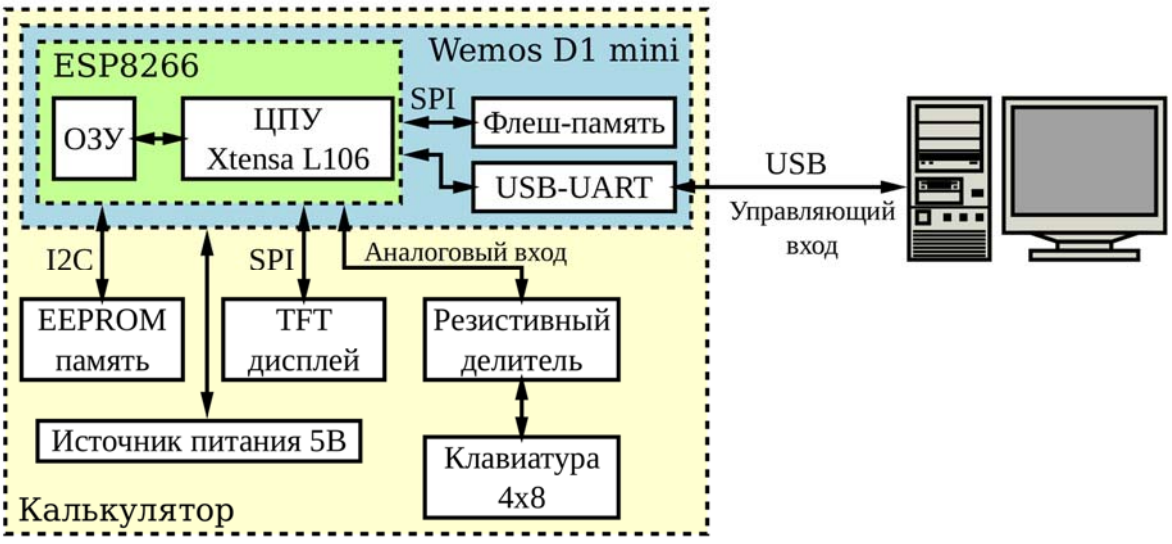


Рис. 1. Блок-схема аппаратного калькулятора Галуа

Для разработки прототипа был выбран модуль Wemos D1 mini на основе микроконтроллера ESP8266 компании Espressif Systems. Микроконтроллер включает в себя процессор Tensilica Xtensa L106 с тактовой частотой 80 МГц, интерфейсные шины SPI, UART, I2C, а также аналого-цифровой преобразователь с разрядностью 10 бит. Микроконтроллер содержит 80 КБ оперативной памяти для данных и 32 КБ – для инструкций. Для хранения микропрограммы используется встроенный в модуль чип флеш-памяти объемом 4 МБ. Выбор модуля в первую очередь обусловлен его малым размером и стоимостью при достаточном для планируемых вычислительных задач функционале.

В качестве пользовательского устройства ввода данных используется 32-кнопочная клавиатура матричного типа. Такое количество клавиш выбрано для того, чтобы обеспечить возможность ввода значений элементов поля, основных математических операций и задания служебных функций. Также часть свободных кнопок оставлена под дальнейшее расширение функционала. Для подключения клавиатуры используется блок резистивного делителя, который позволяет считывать нажатие кнопок через вход АЦП [5].

Основным устройством вывода является цветной TFT дисплей, подключаемый по интерфейсу SPI. Использование дисплея такого типа позволяет удобно выводить на экран значительный объем информации и производить выделение цветом для большей наглядности работы калькулятора.

Для хранения настроек и состояния устройства используется микросхема флеш-памяти типа EEPROM, подключаемая по интерфейсу I2C.

В качестве управляющего интерфейса, используемого для обновления программной прошивки калькулятора, применяется конвертер USB-UART, встроенный в модуль Wemos D1 mini и позволяющий подключать устройство к управляющему компьютеру через порт USB.

В начале работы с калькулятором пользователь задает двоичное поле Галуа $GF(2^m)$, с которым будет работать, вводя степень поля m и его образующий полином $p(x)$. Калькулятор проверяет правильность ввода полинома и в случае ошибки сообщает об этом пользователю. Далее пользователь вводит с помощью клавиатуры формулу, которую хочет вычислить. Вводимые символы при этом отображаются на экране, и параллельно записываются в строковую переменную в памяти калькулятора. После завершения ввода и нажатия клавиши «=» калькулятор приводит все введенные в степенном виде элементы поля ε^i к их значению d_i, представленному в десятичном виде, и конвертирует строку формулы в массивы элементов и операций, используя обратную польскую нотацию. После этого производится вычисление и результат выводится на экран в десятичном и степенном видах.

Для преобразования элемента поля из степенного вида ε^i в десятичный d_i используется операция антилогарифмирования, выполняемая посредством вычисления остатка от деления одночлена x^i на образующий полином [6]:

$$d_i = \text{alog}(i) = [x^i \bmod p(x)].$$

Для выполнения при выводе результата обратной операции логарифмирования производится определение степенной формы результирующего элемента поля. Для этого используется последовательный перебор элементов поля и сравнение их со значением искомого элемента. В случае полей большой степени для ускорения вычислений применяется метод контрольных точек [7]. Для хранения массивов контрольных точек используется внешняя память EEPROM.

Операция сложения элементов поля соответствует поразрядному сложению по модулю 2 и реализуется поразрядной операцией «исключающее-или» [6].

Умножение элементов поля ε^i и ε^j производится через сопровождающую матрицу F_j, соответствующую второму множителю [6]:

$$\varepsilon^i \cdot \varepsilon^j = \varepsilon^i \cdot F_j = \varepsilon^i \cdot \begin{bmatrix} \varepsilon^j \\ \varepsilon^{j+1} \\ \cdots \\ \varepsilon^{j+m-1} \end{bmatrix}.$$

Обращение элемента поля ε^i выполняется по алгоритму Евклида, который представлен на рис. 2 [6]. При рассмотрении алгоритма элемент поля ε^i удобно представлять в виде двоичного полинома $a(x)$.

Функция деления элемента поля ε^i на ε^j вначале вызывает функцию обращения элемента ε^j, а затем выполняет умножения ε^i на $(\varepsilon^j)^{-1}$.

Возведение в степень реализовано через последовательное выполнение операций умножения в цикле.

Предлагаемый калькулятор планируется использовать в рамках курса практиче-

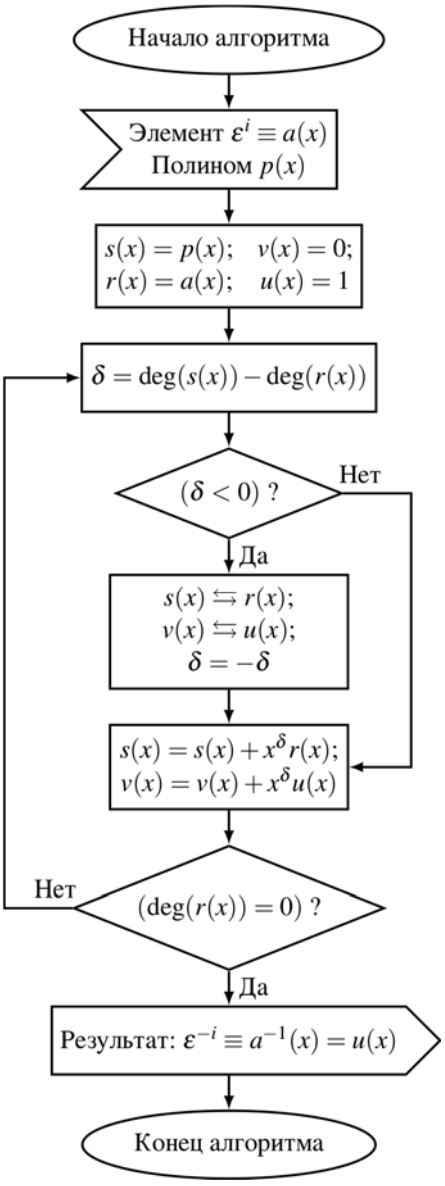


Рис. 2. Обращение элемента поля по алгоритму Евклида

ских работ и при проведении текущей аттестации по дисциплине «Теория и практика помехоустойчивого кодирования». Также устройство будет полезно при проведении научных исследований и разработок по тематике помехоустойчивых кодов.

Список используемых источников

1. Robert H. Morelos-Zaragoza The Art of Error Correcting Coding. Chichester: Издательство «John Wiley & Sons, Ltd», 2002. 232 p. ISBN 0471-49581-6.

2. Баричев С. Г., Гончаров В. В., Серов Р. Е. Основы современной криптографии. М. : Горячая Линия – Телеком, 2011. 175 с. ISBN 978-5-9912-0182-7.

3. Кукунин Д. С. Анализ эффективности декодирования циклических кодов с использованием двойственного базиса: дис. ... канд. техн. наук: 05.13.01 / Кукунин Дмитрий Сергеевич. СПб., 2009. 197 с.

4. Владимиров С. С. Сетевой программируемый калькулятор Галуа // Инновационные процессы и технологии в современном мире: материалы международной научно-практической конференции, г. Уфа, 29–30 нояб. 2013 г. Уфа: Автономная некоммерческая организация «Исследовательский центр информационно-правовых технологий», 2013. С. 147–150.

5. Клавиатура Arduino Рационально [Электронный ресурс] // Союз топора и паяльника [сайт]. URL: https://sites.google.com/site/elektrouzhas/home/klaviatura-arduino-racionalno (дата обращения: 22.02.2020).

6. Владимиров С. С. Математические основы теории помехоустойчивого кодирования : учеб. пособие. СПб. : СПбГУТ, 2016. 96 с. ISBN 978-5-89160-131-4.

7. Кукунин Д. С. Дискретное логарифмирование в полях Галуа с использованием контрольных точек // Научно-технические ведомости Санкт-Петербургского государственного политехнического университета. Информатика. Телекоммуникации. Управление. 2009. Т. 2. № 76. С. 185–192.

УДК 004.428.2
ГРНТИ 50.41.25

РАЗРАБОТКА ВЕБ-ПРИЛОЖЕНИЯ ДЛЯ УЧЕТА ВЫПОЛНЕНИЯ РАБОТ СТУДЕНТОВ ВУЗА

В. Д. Внучкова, А. Ю. Цветков, М. А. Юрченко

Санкт-Петербургский государственный университет телекоммуникаций им. проф. М. А. Бонч-Бруевича

Многие учебные образовательные организации испытывают недостаток автоматизации учета выполнения лабораторных, практических и курсовых работ и проектов. В наше время все больше возрастает актуальность использования систем электронного документооборота в связи с ростом объемов документов, требующих ручной обработки и следующей из этого необходимостью автоматизации. Рассмотрена возможность внедрения системы учета выполнения работ, выделены основные проблемы

внедрения данной системы в учебный процесс кафедры высшего учебного заведения и показаны возможные способы защиты информации на основе существующих нормативно-правовых документов РФ.

цифровая подпись, системы электронного документооборота, веб, php.

В настоящее время все больше возрастает потребность в автоматизации учебного процесса и ведения документооборота в электронной среде [1]. Однако, автоматизированные системы нуждаются в обеспечении безопасности ввиду своей специфики. Рассмотрим основные механизмы обеспечения безопасности веб-приложений на языке php на примере разработки модуля учета выполнения работ студентов с использованием цифровых подписей для написанной ранее системы автоматизации учебного процесса “LabGen” [2].

Выбор веб-платформы обусловлен высокой кроссплатформенностью и доступностью для студентов и преподавателей практически с любого устройства, а также клиент-серверной архитектурой, обеспечивающей централизованное хранение данных и удобство администрирования.

Веб-платформа на данный момент является одной из самых популярных, а для разработки часто используется язык программирования php для создания динамических сайтов в силу своей распространенности, низкого порога входа для новичков и гибкости. Для разработки системы LabGen был выбран именно этот язык, таким образом, модуль также будет написан на языке php.

Клиент-серверная архитектура, лежащая в основе веб-платформы, поделена на звенья и состоит из N звеньев клиента и связанных серверов. Каждый из промежуточных серверов выступает в роли посредника между клиентом и конечными серверами, разбивая систему на логические части, где каждый отвечает только за свое. Сервера могут как объединять в себе множество функций, так и разбиваться на несколько звеньев для упрощения поддержки, возможного увеличения отказоустойчивости и возможного увеличения читаемости кода.

Разработанный проект основывается на трехзвенной архитектуре и его схема представлена на рис. 1.

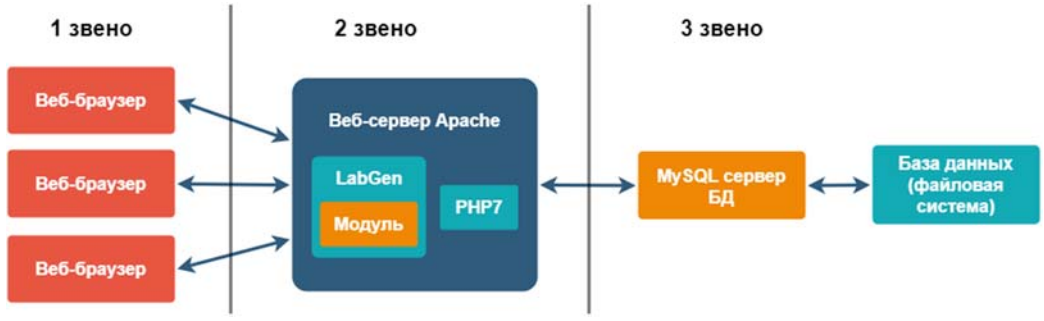


Рис. 1. Схема разработанной системы

Роль клиента в веб-приложениях обычно играет веб-браузер. Для второго звена был выбран веб-сервер Apache, совместимый с интерпретатором языка PHP, а сервер баз данных третьего звена был организован на сервере MySQL, так как MySQL является одно из самых распространенных СУБД.

Клиент-серверные системы подвержены различным типам уязвимостей, перечислим основные:

– Reverse engineering клиентской части приложения, анализ исходного кода и поиск уязвимостей по нему;

– прослушивание и подмена сетевых пакетов между клиентом и сервером атаками спуфинга, “man in the middle” и т. д.;

– несанкционированный доступ к устройствам привилегированных участников системы и получение полных прав, а также социальная инженерия.

В целях обеспечения защиты от этих уязвимостей были реализованы следующие меры:

– обфускация скриптов на языке javascript, затруднение процесса анализа файлов веб-приложения;

– использование протокола TLS для защиты передаваемых данных, независимо от логики приложения, на транспортном уровне [3];

– внедрение модели распределения прав доступа между участниками системы в целях снижения потенциального ущерба от действий злоумышленников с правами кого-либо из администраторов системы.

Устранение уязвимости прослушивания и подмены сетевых пакетов возможно с использованием технологий SSL или TLS. Протокол TLS (англ. *transport layer security* – Протокол защиты транспортного уровня) является усовершенствованной версией протокола SSL (англ. *Secure Sockets Layer* – уровень защищенных сокетов).

Другой, достаточно важной проблемой является возможность злоумышленнику заниматься «обратной разработкой» кода клиентской части приложения. В случае с языком javascript, тексты программ распространяются в исходном виде, благодаря чему нарушитель может анализировать текст программы и искать в нем незакрытые уязвимости, используя их в корыстных целях.

Полностью защититься от данной уязвимости невозможно, однако, можно произвести обфускацию. Обфускация – процесс запутывания кода приложения. В результате данного процесса для злоумышленника значительно усложняется задача анализа кода приложения путем стирания названий всех переменных (превращения в бессмысленные идентификаторы), использования конструкций, сложных для восприятия человеком, шифрования констант и строк в коде программы (с дешифрованием при ее исполнении [4]) и так далее.

Однако, существуют средства частичного обращения обфускации. Они могут раскрывать сложные конструкции в более читаемый вид по распространенным шаблонам сжатия конструкций языка при обфускации, пытаться восстановить идентификаторы объектов скрипта по их смысловому применению в программе, а также пытаться дешифровать строки и константы, если возможно определить механизм их обфускации шифрованием. Пример процесса обфускации приведен на рис. 2.

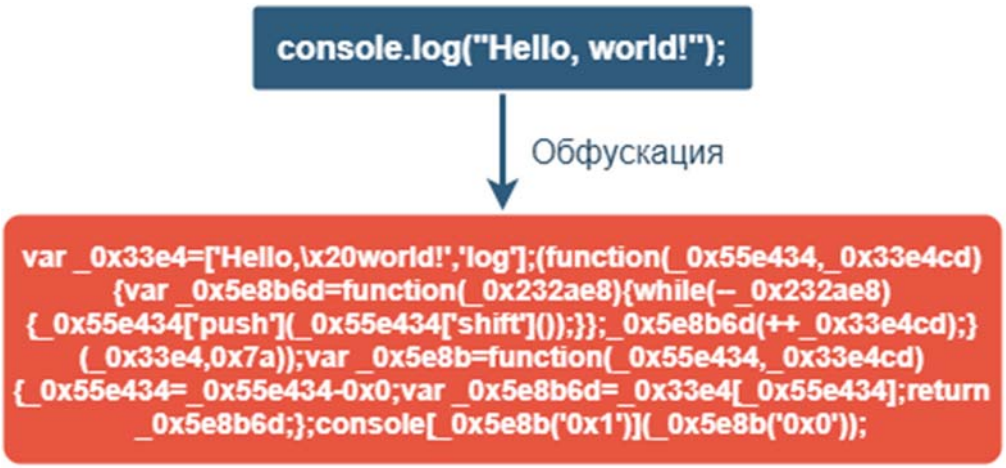


Рис. 2. Процесс обфускации на примере небольшой программы

В целях снижения ущерба от несанкционированного доступа к устройствам администраторов и средств социальной инженерии была введена гибкая ролевая модель безопасности с привязкой прав к определенным учебным дисциплинам, в результате чего злоумышленник с имеющимся аккаунтом администратора не в праве нарушить функциональность всей системы в целом, а только в подвластной ему части.

Поверх административной панели LabGen был разработан модуль данной системы - RepAcc. Система состоит из двух частей: RepAcc от имени преподавателя и от имени студента. Студент может загружать в систему отчеты по выполненным лабораторным работам (только по доступным ему дисциплинам), преподаватель имеет возможность просматривать отчет в браузере, оставлять приватные и публичные комментарии (приватные видны только другим преподавателям на этой же дисциплине) и ставить оценку от 1 до 5 звезд. После проставления оценки вычисляется среднее арифметическое между всеми оценками преподавателей, а преподаватели имеют доступ только к тем отчетам, на дисциплинах которых у них есть необходимые права. Вид системы от имени студента представлен на рис. 3 (см. ниже).

Однако, злоумышленник все еще может получить доступ к аккаунту преподавателя и сделать поддельную оценку. Например, если преподава-

тель случайно оставит свое устройство после занятия [5]. Система и студенты должны удостовериться в том, что комментарий и/или оценку поставил именно сам преподаватель. Для этого была внедрена система цифровой подписи для комментариев и оценок.

Цифровая подпись работает на асимметричных алгоритмах шифрования по обратному принципу. Сообщение шифруется собственным закрытым ключом и полученные зашифрованные данные прикрепляются к самому сообщению. Для проверки достоверности адресаты этого сообщения могут расшифровать подписанную часть с помощью открытого ключа, но не могут подделать подпись, так как не имеют закрытого ключа.

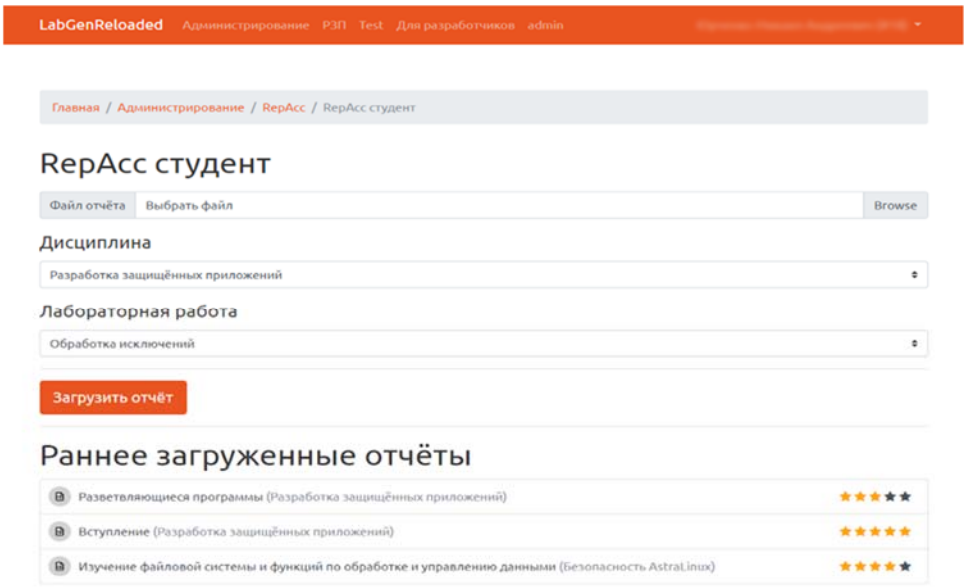


Рис. 3. RepAcc от имени студента

Преподаватель получает свой собственный сертификат и закрытый ключ, устанавливает его в систему и с использованием стороннего плагина для браузера подписывает проставляемые оценки и комментарии. Сервер на php проверяет подпись с помощью открытого ключа преподавателя и принимает решение о выполнении данного действия преподавателя.

Таким образом, для противодействия атакам на данную систему в среде высшего учебного заведения, где злоумышленником может являться любой обучающийся, были реализованы следующие механизмы безопасности:

– обфускация скриптов на языке javascript, затруднение процесса анализа файлов веб-приложения;

– протокол TLS для защиты передаваемых данных независимо от логики приложения, на транспортном уровне;

– модель распределения прав доступа между участниками системы в целях снижения потенциального ущерба от действий злоумышленников с правами кого-либо из администраторов системы;

– удостоверение личности преподавателя при проставлении оценок и комментариев при помощи механизма цифровой подписи.

Они позволят обеспечить необходимый уровень безопасности [5], но при рассмотрении других возможных моделей злоумышленников, могут потребоваться модификации [6, 7, 8].

Список используемых источников

1. Волкогонов В. Н., Гельфанд А. М., Деревянко В. С. Актуальность автоматизированных систем управления // Актуальные проблемы инфотелекоммуникаций в науке и образовании. VIII Международная научно-техническая и научно-методическая конференция : сб. науч. ст. в 4-х т. СПб. : СПбГУТ, 2019. Т. 2. С. 262–266.

2. Цветков А. Ю., Шалаева М. Е., Юрченко М. А. Обеспечение безопасности в клиент-серверном java приложении для учета и автоматической проверки лабораторных работ // Актуальные проблемы инфотелекоммуникаций в науке и образовании. VIII Международная научно-техническая и научно-методическая конференция : сб. науч. ст. в 4-х т. СПб. : СПбГУТ, 2019. Т. 2. С. 756–761.

3. Волкогонов В. Н., Гельфанд А. М., Карамова М. Р. Обеспечение безопасности персональных данных при их обработке в информационных системах персональных данных // Актуальные проблемы инфотелекоммуникаций в науке и образовании. VIII Международная научно-техническая и научно-методическая конференция : сб. науч. ст. в 4-х т. СПб. : СПбГУТ, 2019. Т. 2. С. 266–270.

4. Гельфанд А. М., Пестов И. Е., Катасонов А. И., Рязанцев К. С. Разработка модели распространения самомодифицирующегося кода в защищаемой информационной системе // Современная наука: актуальные проблемы теории и практики. Серия: Естественные и технические науки. 2018. № 8. С. 91–97.

5. Штеренберг С. И., Полтавцева М. А. Распределенная система обнаружения вторжений с защитой от внутреннего нарушителя // Проблемы информационной безопасности. Компьютерные системы. 2018. № 2. С. 59–68.

6. Дубровин Н. Д., Ушаков И. А., Чечулин А. А. Применение технологии больших данных в системах управления информацией и событиями безопасности // Актуальные проблемы инфотелекоммуникаций в науке и образовании. V Международная научно-техническая и научно-методическая конференция : сб. науч. ст. в 4-х т.СПб. : СПбГУТ, 2016. Т. 2. С. 348–353.

7. Гельфанд А. М., Косов Н. А., Красов А. В., Орлов Г. А. Защита для распределенных отказов в обслуживании в облачных вычислениях // Актуальные проблемы инфотелекоммуникаций в науке и образовании. VIII Международная научно-техническая и научно-методическая конференция : сб. науч. ст. в 4-х т. СПб. : СПбГУТ, 2019. Т. 2. С. 329–334.

8. Красов А. В., Штеренберг С. И., Голузина Д. Р. Методика визуализации больших данных в системах защиты информации для формирования отчетов уязвимостей // Электросвязь. 2019. № 11. С. 39–47.

Статья представлена заведующим кафедрой ЗСС СПбГУТ, кандидатом технических наук, доцентом А. В. Красовым.

УДК 519.87
ГРНТИ 10.19.61

ОБОБЩЕННАЯ МОДЕЛЬ ИНФОРМАЦИОННОЙ СИСТЕМЫ ОБРАЗОВАТЕЛЬНОЙ ОРГАНИЗАЦИИ

В. А. Волостных, Ю. В. Гвоздев, П. А. Кононов

Санкт-Петербургский государственный университет телекоммуникаций им. проф. М. А. Бонч-Бруевича

Процесс деятельности образовательной организации высшего образования представляет собой сложную и комплексную систему, охватывающую информационные потоки, протекающие в тесном взаимодействии с внешней средой организации и все внутренние информационные процессы. Информационная система организации представляет собой совокупность информационной инфраструктуры и информационных активов организации. В статье рассматриваются подходы к разработке обобщенной модели информационной системы типовой образовательной организации высшего образования инженерно-технической направленности, функционирующей в условиях угроз информационной безопасности.

информационная система, угрозы информационной безопасности, образовательная организация.

В настоящие время роль информации и информационных процессов играют важное, а где-то и определяющее значение в функционировании и перспективном развитии почти каждой современной организации [1].

Особенности образовательной организации высшего образования связаны с разносторонними формами деятельности, обилием направлений и методов учебной работы, пространственной распределенностью инфраструктуры (колледжи, филиалы), наличием разветвленной структуры вспомогательных подразделений и служб, целесообразностью межведомственного электронного взаимодействия с вышестоящими организациями, периодическим изменением статуса работников и обучающихся [2].

В современном информационном обществе качество работы фактически каждой образовательной организации связаны с оперативным и безопасным доступом к данным и обменом информацией между профессорско-преподавательским составом и обучающимися, руководящим составом организации и педагогическими работниками, между различными структурными подразделениями организации. Только при выполнении данных условий возможно выстроить эффективную работу всей образовательной организации, начиная от отдельных работников и заканчивая структурными подразделениями, без которых работа организации будет затруднительна, а иногда и невозможна. К числу таких подразделений необходимо отнести

учебно-методические и научные подразделения, деканаты и кафедры, отдел бухгалтерии, и административно-кадровый отдел, подразделения информатизации и защиты информации, а также, хозяйственные подразделения.

Особенности структуры информационных потоков в образовательной организации высшего образования связаны с многофункциональностью самой организации. Основным видом деятельности в образовательной организации является процесс обучения, поэтому поток информации между педагогическими работниками и обучающимися назовем первым информационным потоком. Несомненно, данный поток имеет двухсторонний характер, так как обучающиеся в процессе обучения задают вопросы, отвечают на вопросы преподавателей и т. д. Под информационным потоком понимается совокупность сообщений, циркулирующих внутри системы, а также между этой системой и средой, внешней по отношению к ней, которые необходимы для управления и контроля за деятельностью всего учреждения [3].

Следующим (вторым) информационным потоком будем называть поток информации от руководящего состава организации к педагогическим работникам. Этот поток характеризуется структурой управления образовательным процессом и реализуется путем издания приказов, указаний, распоряжений.

Определенные действия с информацией в образовательных организациях можно осуществить благодаря внедрению информационно-образовательной среды.

Информационно-образовательная среда образовательной организации включает совокупность технических, программных средств, комплекс информационных образовательных ресурсов: средства вычислительной техники, мультимедийное оборудование, коммуникационные каналы, иное информационное оборудование; систему современных педагогических технологий, обеспечивающих обучение в современной информационно-образовательной среде.

Это составляющая имеет два направления и включает в себя непосредственно образовательную сферу и вспомогательный контент. Образовательная сфера деятельности подразумевает доведение различных материалов с помощью информационных технологий профессорско-преподавательским составом до обучающихся. А к вспомогательному контенту относится вся документация, которая представлена в электронном виде и сопровождает сам учебный процесс: учебные планы, рабочие программы, образовательные стандарты, графики занятий, ведомости и пр. К данной информации имеют доступ обучающиеся и преподаватели, администрация факультетов, кафедр, ректорат, а также лица, не связанные с образовательным процессом напрямую. Структурные подразделения, обеспечивающие функционирование высшей образовательной организации, такие как отдел

бухгалтерии, отдел кадров, хозяйственный отдел, имеют только ограниченный доступ к образовательному и вспомогательному контенту.

Под информационной безопасностью организации понимается состояние защищенности интересов организации в условиях угроз в информационной сфере. Защищенность достигается обеспечением совокупности свойств информационной безопасности – конфиденциальностью, целостностью, доступностью инфраструктуры организации и информационных активов [3].

Для определения оценки уровня информационной безопасности и выявления уязвимостей информационной системы (ИС) специалисты организаций нередко прибегают к моделированию ИС, функционирующих в условиях воздействия угроз информационной безопасности организаций.

Под информационной системой принято понимать совокупность содержащейся в базах данных информации и обеспечивающих ее обработку информационных технологий и технических средств, а под угрозой ИБ организации понимается совокупность факторов и условий, создающих опасность нарушения информационной безопасности организации, вызывающих или способных вызвать негативные последствия (ущерб/вред) для организации [4, 5].

Авторами проведена классификация информационных ресурсов образовательной организации, которая представлена в таблице.

ТАБЛИЦА. Классификация информационных ресурсов образовательной организации

№ п/п	Наименование ресурса	Необходимость ограничения доступа	Необходимость использования технических средств	По типу носителя	Объем ресурса	Значимость
1.	Приказы, распоряжения	да, нет	да	Бм	М	В
2.	Инструкции, положения, регламенты	да, нет	да	Бм	М	С
3.	Программы, расписания, графики	да, нет	да	Бм, Э	М	В
4.	Методические материалы	нет	да, нет	Бм, Э	С	С
5.	Учебные материалы	нет	да, нет	Бм, Э	Б	В
6.	Научно-технические материалы	да, нет	да	Бм, Э	Б	В
7.	Художественные произведения	нет	нет	Бм	Б	М

Обозначения:

1. Бм – бумажный, Э – электронный;
2. Б – большой, С – средний, М – малый;
3. В – высокая, С – средняя, М-маленькая.

Представленную классификацию информационных ресурсов предлагается уточнять до количественных показателей и применять при анализе безопасности информационных подсистем организации. В качестве уровней информационных потоков в образовательной организации предлагается выделить горизонтальные и вертикальные. Данные названия потоков полностью сопоставимы с направлением движения информации в организации.

На горизонтальном уровне происходит обмен информацией между обучающими и обучающимися в двухстороннем порядке.

На вертикальном уровне происходит обмен информацией между руководящим составом организации и профессорско-преподавательским составом, а также между руководящим составом организации и студентами.

При формировании обобщенной модели информационной системы образовательной организации в данной статье рассмотрение внешних потоков и потоков информации, содержащих государственную тайнувведено в разряд ограничений.

С учетом особенностей информационных потоков, циркулирующих в организации, была разработана обобщенная модель информационной системы образовательной организации, представленная на рис.

Рис. Обобщенная модель информационной системы образовательной организации

Работу ИС можно оценить по нескольким направлениям, используя при этом количественные и качественные критерии. К качественным характеристикам относится бесперебойное функционирование информационной

системы, а также возможность получения доступа к необходимому информационному ресурсу в любой момент времени. Количественные критерии характеризуются следующими показателями: скорость передачи и получения информации, общий объем трафика, максимальное количество пользователей, работающих в данный момент времени, уровни пользователей, количество активных документов в ИС, среднее число добавления/удаления документов за единицу времени.

Данные показатели позволяют оценить и спрогнозировать функционирование системы в условиях угроз безопасности информации и перехода к нестандартной форме ведения образовательного процесса [6].

Выводы

1. Необходимость создания модели информационной системыобразовательной организации связана с необходимостью совершенствования информационной системы на научной основе с учетом возрастающих угроз информационной безопасности и переходом к нестандартным формам функционирования организаций и предприятий.

2. Обобщенная модель информационной системы образовательной организации позволяет выделить существенные для образовательной деятельности информационные потоки и разработать организационно-технические предложения по обеспечению их безопасности.

3. Для разработки научно-технических предложений по обеспечению информационной безопасности образовательной организации необходимо провести декомпозицию обобщенной модели, выделить существенные показатели информационных потоков и уязвимости подсистем информационной системы образовательной организации.

Список используемых источников

1. Доктрина информационной безопасности Российской Федерации, утвержденная указом Президента Российской Федерации от 5 декабря 2016 г. № 646.

2. Федеральный закон от 29.12.2012 N 273-ФЗ «Об образовании в Российской Федерации».

3. ГОСТ Р 53114-2008. Защита информации. Обеспечение информационной безопасности в организации. Основные термины и определения. М. : Изд-во стандартов, 2009.

4. Вентцель Е. С. Исследование операций. М. : Советское радио, 1972. 552 с.

5. Бусленко Н. П. Исследование сложных систем. М. : Наука. 1978.

6. Волостных В. А., Гвоздев Ю. В., Карганов В. В. Моделирование информационных систем организации // Актуальные проблемы инфотелекоммуникаций в науке и образовании. VII Международная научно-техническая и научно-методическая конференция : сб. науч. ст. в 4-х т. СПб.: СПбГУТ, 2019. Т. 1. С. 284–289.

УДК 003.26.09
ГРНТИ 81.93.29

ОБНАРУЖЕНИЕ СТЕГОСИСТЕМЫ С ВЛОЖЕНИЕМ ±1НЗБ НА ОСНОВЕ ИСПОЛЬЗОВАНИЯ NIST-ТЕСТОВ

А. Г. Габуев, В. И. Коржик, З. К. Нгуен

Санкт-Петербургский государственный университет телекоммуникаций им. проф. М. А. Бонч-Бруевича.

Существует множество методов обнаружения стегосистем. В данной статье оценивается эффективность использования нового метода стегоанализа на основе использования NIST-тестов применительно к вложению, известному как ±1НЗБ. Объясняются принципы вложения и извлечения информации при использовании метода ±1НЗБ. Результаты стегоанализа при использовании NIST-тестов сравниваются с результатами стегоанализа на основе ранее известного метода, использующего двумерное преобразование Фурье.

стегосистема, стегоанализ, NIST-тесты, вложение ±1НЗБ.

Для вложения скрытой информации в изображение существует множество различных методов. Одним из таких методов является вложение ±1НЗБ. Суть метода заключается в следующем: исходное изображение преобразуется путем представления его в оттенках серого. Таким образом, каждый пиксель изображения вместо информации о красной, зеленой и синей составляющей будет содержать информацию только об оттенках серого [1]. Количество возможных значений оттенка серого типично равно 256 (от 0 до 255). Таким образом, каждый пиксель содержит 8 бит информации. В этих 8 битах и будет содержаться 1 бит вкладываемой информации.

Процесс вложения информации

Вложение информации в изображение происходит по следующему правилу:

$$C_w(n) = \begin{cases} C(n), \text{ если НЗБ } \big(C(n)\big) = b(n), \\ C(n)+1, \text{ с вероятностью } {}^1\!/_2, \text{ если НЗБ } C(n) \neq b(n), \\ C(n)-1, \text{ с вероятностью } {}^1\!/_2, \text{ если НЗБ } C(n) \neq b(n), \end{cases}$$

где $C_w(n)$ – величина отсчёта $C(n)$ после вложения; $C(n)$ – исходное значение отсчета; $b(n)$ – вкладываемый бит информации.

Как говорилось ранее, 1 пиксель будет содержать 1 бит скрытой информации. Исходя из правила вложения информации в изображение, эта последовательность не будет отличаться от исходной последовательности только в том случае, если НЗБ исходной последовательности равен вкладываемому биту информации. Если же НЗБ исходной последовательности не равен вкладываемому биту информации, то передаваемая последовательность будет изменена – значение оттенка серого пикселя будет увеличено на 1 с вероятностью 50 %, либо же уменьшено на 1, так же с вероятностью 50 % [2]. Однако следует помнить, что крайние возможные значения оттенка 0 и 255, могут быть только увеличены или уменьшены, соответственно.

Процесс извлечения информации

Извлечение информации из изображения происходит по следующему правилу:

$$\tilde{b}(n) = 0, \text{ если } C_w(n) - \text{четное число, т. е. НЗБ } \left(C_w(n)\right) = 0,$$

$$\tilde{b}(n) = 1, \text{ если } C_w(n) - \text{нечетное число, т. е. НЗБ } \left(C_w(n)\right) = 1,$$

где $\tilde{b}(n)$ – бит извлеченной информации; $C_w(n)$ – последовательность отсчета после вложения.

Ниже представлены два изображения: исходное изображение, преобразованное путем представления его в оттенках серого (рис. 1а), и стегоизображение, содержащее в себе скрытую информацию (рис. 1б).

а) б)

Рис. 1. Покрывающее изображение(а); стегоизображение (б)

Визуально кажется, что изображения одинаковые, и поэтому факт вложения не может быть обнаружен путем простого визуального анализа.

Основная идея использования ±1НЗБ вместо обычного НЗБ-замещения состоит в том, что обычное НЗБ обладает некоторой несимметрией. Это, в свою очередь, приводит к появлению характерных статистических признаков, позволяющих сделать процедуру обнаружения более надежной.

Обнаружение СГ-±1НЗБ на основе использования NIST-тестов

NIST-тесты представляют собой 15 статистических тестов, целью которых является определение меры случайности полученных двоичных последовательностей [3].

Анализ изображения содержит несколько этапов: сперва производится извлечение двоичной последовательности по алгоритму извлечения (если он известен или найден) в предположении присутствия СГ. Далее последовательность проверяется для всех 15 NIST-тестов, а результаты тестов заносятся в таблицу – при прохождении теста в соответствующее поле таблицы ставится 1, иначе – 0. Финальным этапом анализа изображения является сравнение прошедших тестов с выбранным порогом. Если число прошедших тестов будет больше порога, то принимается решение о вложении СГ, иначе – решение об отсутствии вложения. Названия используемых NIST-тестов приведены в таблице 1.

ТАБЛИЦА 1. Список названий стандартных NIST-тестов

№ Теста	Название теста
1	The frequency test
2	Frequency test within a block
3	The runs test
4	Tests for the longest-run-of-ones in a block
5	The binary matrix rank test
6	The discrete Fourier transform (spectral) test
7	The non-overlapping template matching test
8	The overlapping template matching test
9	Maurer’s “Universal Statistical” test
10	The linear complexity test
11	The serial test
12	The approximate entropy test
13	The cumulative sums (cusums) test
14	The random excursion test
15	The random excursions variant test

Экспериментальное обнаружение СГ-±1НЗБ

NIST-тесты были выполнены на 10 последовательностях, извлеченных из изображений размером 512×512 [4], не содержащих скрытую информацию. В результате была построена таблица 2. Затем эти же тесты были про-

ведены на 10 последовательностях, полученных из изображений, содержащих скрытую информацию, зашифрованную шифром ГОСТ-28147-89 [5], в результате была построена таблица 3.

ТАБЛИЦА 2. Результаты NIST-тестов для изображений, не содержащих скрытую информацию

Index of sequence	T1	T2	T3	T4	T5	T6	T7	T8	T9	T10	T11	T12	T13	T14	T15	Sum
Image_1	0	0	0	0	1	0	0	0	0	1	0	0	0	0	0	2
Image_2	0	0	0	0	1	1	0	0	0	1	0	0	0	0	0	3
Image_3	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
Image_4	0	0	0	0	1	0	0	0	0	1	0	0	0	0	0	2
Image_5	0	0	0	0	0	0	0	0	0	1	0	0	0	0	0	0
Image_6	1	0	1	0	1	1	0	0	0	1	0	1	0	0	0	6
Image_7	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
Image_8	1	1	1	1	1	1	1	1	1	1	0	1	1	0	0	12
Image_9	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
Im-age_10	1	1	0	0	1	1	0	0	0	1	0	1	0	0	0	6

ТАБЛИЦА 3. Результаты NIST-тестов для изображений, содержащих скрытую информацию

Index of se-quence	T1	T2	T3	T4	T5	T6	T7	T8	T9	T10	T11	T12	T13	T14	T15	Sum
Seq 1	1	1	1	1	1	1	1	1	1	1	1	1	1	0	0	13
Seq 2	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	15
Seq 3	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	15
Seq 4	1	1	1	1	1	1	1	1	1	1	1	1	1	0	0	13
Seq 5	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	15
Seq 6	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	15
Seq 7	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	15
Seq 8	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	15
Seq 9	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	15
Seq 10	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	15

Как видно из сравнения содержимого таблиц 2 и 3, NIST-тесты позволяют обнаружить такое вложение в изображение.

Для выбора оптимального порога, NIST-тесты были выполнены на последовательностях, извлеченных из 1000 изображений [4] с вероятностью вложения информации в каждый пиксель p = 1,0 (табл. 4): P_m – вероятность *необнаружения* (*пропуска*) СГ в случае, когда вложение присутствует; P_{fa} – вероятность *ложного обнаружения* СГ в случае, когда вложение отсутствует; а вероятность обнаружения ошибок СГА $P_e = \frac{1}{2}(P_m + P_{fa})$.

ТАБЛИЦА 4. Зависимость вероятностей ошибок P_m, P_{fa} и P_e (в %) в зависимости от величины порога прохождения NIST-тестов

Порог	0	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15
P_m	0	0	0	0	0	0	0	0	0	0	0	0	0.7	4.1	24.8	39.3
P_m	100	98.8	92.4	79.6	66.0	55.0	43.1	37.0	31.3	27.8	25.5	24.4	21.6	18.9	13.8	8.9
P_e	50	49.4	46.2	39.8	33.0	27.5	21.55	18.5	15.65	13.9	12.75	12.2	11.15	11.5	19.3	24.1

Из таблицы 4 видно, что для минимизации полной вероятности ошибки обнаружения СГ $P_e = 11{,}15\ \%$ целесообразно выбрать пороговое значение 12.

Видно, что при вероятности вложения равной 1, метод работает гораздо лучше метода двумерного преобразования Фурье [6], представленного на рис. 2.

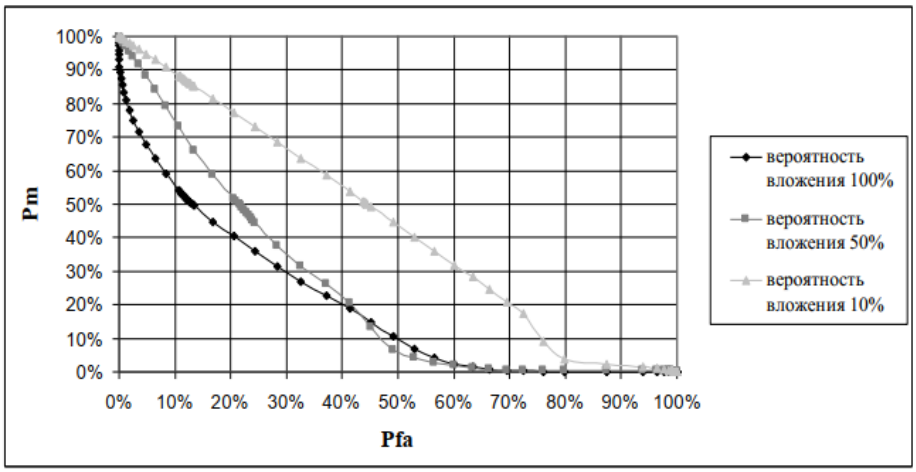


Рис. 2. Результаты метода двумерного преобразования Фурье

Из рис. 2 видно, что в случае полного вложения этот стегоаналитический метод обеспечивает $P_{fa} = 20{,}0\ \%$, $P_m = 40{,}0\ \%$, что значительно хуже, чем $P_{fa} = 0{,}7\ \%$, $P_m = 21{,}6\ \%$, для предложенного выше, стегоаналитического метода на основе использования NIST-тестирования.

Таким образом, можно сделать вывод о том, что NIST-тесты являются очень эффективными для обнаружения стегосистемы с вложением ±1НЗБ.

Список используемых источников

1. Коржик В. И., Небаева К. А., Герлинг Е. Ю., Догиль П. С., Федянин И. А. Цифровая стеганография и цифровые водяные знаки. Часть 1. Цифровая стеганография / Под общ. ред. проф. В. И. Коржика. СПб. : СПбГУТ, 2016. 226 с. ISBN 978-5-89160-125-3.

2. Korzhik V., Fedyanin I., Godlewski A., Morales-Luna G. Steganalysis based on statistical properties of the encrypted messages // International Conference on Mathematical Methods, Models, and Architectures for Computer Network Security. Lecture Notes in Computer Science, vol 10446. Warsaw, Poland, 28–30 August 2017. С. 288–298.

3. Bassham III L. E., Rukhin A. L., Soto J., Nechvatal J. R., Smid M. E., Barker E. B., Leigh S. D., Levenson M., Vangel M., Banks D. L., Heckert N. A., Dray J. F., Vo S. Sp. 800–22 rev. 1a. a statistical test suite for random and pseudorandom number generators for cryptographic applications // National Institute of Standards and Technology. 2010. 131 p. URL: https://www.nist.gov/publications/statistical-test-suite-random-and-pseudorandom-number-generators-cryptographic (дата обращения 26.02.2020).

4. DDE Laboratory in the Binghamton University, BOSSBASE 1.01. URL: http://dde.binghamton.edu (дата обращения 26.02.2020).

5. Schneier B. The GOST encryption algorithm // DR DOBBS JOURNAL. 1995. N 20 (1). PP. 123-124.

6. Ker A. D. Steganalysis of LSB matching in grayscale images // IEEE signal processing letters. 2005. N 12 (6). PP. 441–444.

УДК 004.77
ГРНТИ 81.93.29

АНАЛИЗ ЗАЩИЩЕННОСТИ СОВРЕМЕННЫХ СРЕДСТВ ПЕРЕДАЧИ ИНФОРМАЦИИ ПОСРЕДСТВОМ ПОРТАТИВНОЙ ЛАБОРАТОРИИ НА ОСНОВЕ МИКРОКОМПЬЮТЕРА RASPBERRY PI

А. Г. Габуев, А. В. Красов, Ф. Д. Ощенков, Н. М. Тарасов

Санкт-Петербургский государственный университет телекоммуникаций им. проф. М. А. Бонч-Бруевича

В данной статье рассматривается метод проверки безопасности беспроводных средств передачи информации с помощью портативного инструмента анализа безопасности, основанного на Raspberry. Для анализа защищенности протокола аутентификации WPA2 была использована платформа Raspberry с ОС Linux и установленным ПО, позволяющим произвести проверку безопасности протокола аутентификации Wi-Fi.

Wi-Fi, Linux, информационная безопасность, penetration testing, WPA2, Raspberry, DoS.

Введение

В нынешнее время протоколы аутентификации являются важной частью защиты информационной системы. Существует множество протоколов аутентификации для беспроводных систем обмена информацией. В работе идет речь о безопасности протокола WPA2.

Проведение исследования

Анализ защищённости современных средств передачи информации посредством портативной лаборатории на основе микрокомпьютера Raspberry Pi состоит из следующих этапов:

– подготовка одноплатного микрокомпьютера Raspberry Pi;

– подготовка тестовой платформы, на которой будет проводиться моделирование;

– перехват handshake;

– обработка перехваченных данных.

После проделанных этапов делается заключение о защищенности рассматриваемого протокола.

Определения, используемые в статье:

DoS (аббр. англ. *Denial of Service* «отказ в обслуживании») – хакерская атака на вычислительную систему с целью довести её до отказа [1], то есть создание таких условий, при которых добросовестные пользователи системы не смогут получить доступ к предоставляемым системным ресурсам (серверам), либо этот доступ будет затруднён [2].

Handshake – это обмен информацией между точкой доступа и клиентом в момент подключения клиента к ней.

Этап 1. Подготовка одноплатного микрокомпьютера Raspberry Pi

Для начала устанавливают операционную систему Raspbian. Установочная система взята с сайта производителя (https://www.raspberrypi.org/). Установка производится на SD карту памяти. Вставляют SD карту памяти в Raspberry, периферийные устройства (мышь, клавиатура, монитор) подключают к Raspberry Pi (рис. 1). Проводят первоначальную установку системы и настройку удаленного доступа по SSH. Устанавливают первоначальный пакет программ, необходимый для тестирования безопасности протокола WPA2.

Рис. 2. Платформа Raspberry Pi

Этап 2. Подготовка тестовой платформы, на которой будет проводиться моделирование

Включают маршрутизатор. Осуществляют настройку маршрутизатора, применяя необходимую конфигурацию, а именно, устанавливают протокол шифрования WPA2. Подключают клиентское устройство к беспроводной сети маршрутизатора [3] (рис. 2).

Рис. 3. Тестовая платформа

Этап 3. Перехват handshake

Так как сетевая карта Raspberry Pi не поддерживает режим мониторинга сети, то необходимо подключить внешнюю сетевую карту, которая поддерживает данный режим [4]. Переводят сетевую карту в режим мониторинга (рис. 3).

```
PHY     Interface       Driver          Chipset

phy0    wlan0           brcmfmac        Broadcom 43430
phy1    wlan1           rt2800usb       Ralink Technology, Corp. RT2870/RT3070

                (mac80211 monitor mode vif enabled for [phy1]wlan1 on [phy1]wlan1mon)
                (mac80211 station mode vif disabled for [phy1]wlan1)
```

Рис. 4. Monitor mode

Находят тестируемую сеть. Просматривают подключенных к сети клиентов, и находят подключенное ранее клиентское устройство. Добиваются деаутентификации клиента посредством Dos атаки. При следующем подключении клиента к точке доступа будет перехвачен handshake, который является хешем от пароля [5] (рис. 4).

```
CH  1 ][ Elapsed: 1 min ][ 2019-10-29 23:30 ][ WPA handshake: [redacted]

BSSID              PWR RXQ  Beacons    #Data, #/s  CH  MB   ENC  CIPHER AUTH ESSID

[redacted]         -20 100      675      634   15   1   54  WPA2 CCMP   PSK  ASUS

BSSID              STATION            PWR   Rate    Lost    Frames  Probe

[redacted]         [redacted]          -8    0e- 0e   227      533
```

Рис. 5. Процесс получения handshake

Этап 4. Обработка перехваченных данных

При помощи ранее установленного на Raspberry Pi программного обеспечения осуществляют подбор пароля, сравнивая данные, полученные на прошлом этапе, с данными, полученными при применении алгоритма хеширования, аналогичного алгоритму WPA2, к предполагаемым паролям (рис. 5).

```
[00:02:44] 62666/9822770 keys tested (144.13 k/s)

Time left: 18 hours, 49 minutes, 38 seconds                0.64%

                     KEY FOUND! [ 43334643 ]


Master Key     : 17 73 AA 1D 15 E5 7B A1 70 78 74 FE 65 C3 79 01
                 72 90 6B 38 DB 6E 70 C7 A2 3C 28 F9 A8 21 AA D6

Transient Key  : 65 F9 C2 71 F1 BB 28 F8 62 FB AF 55 51 5F 60 49
                 53 2D 8E 22 D1 B1 75 05 43 B1 59 5D FB EF 31 EC
                 BF B3 5E C7 B4 C0 F4 70 25 8B E8 49 6C 68 48 A6
                 5F 5D 2F 97 36 8C 06 DB 52 DD AD CA CC 84 57 19
```

Рис. 6. Результат подбора пароля

Вывод

На сегодняшний день [6, 7, 8] применение протоколов аутентификации является необходимым условием построения информационной системы. Но многие из этих протоколов остаются достаточно небезопасными из-за наличия разнообразных уязвимостей и, в том числе, человеческого фактора. В данной работе при анализе защищённости протокола WPA2 произведен эксперимент, в котором имеется возможность получения и хранения приватных данных пользователей сети, в следствии чего появляется возможность получения несанкционированного доступа в сеть к пользователю.

Список используемых источников

1. Зобнин Е. Устоять любой ценой. Методы борьбы с DoS/DDoS-атаками // Журнал «Хакер». 2009. URL: https://xakep.ru/2009/10/14/49752/ (дата обращения 29.09.2019).

2. Peng Liu. Denial of Service Attacks. – University Park. 2004. URL: https://s2.ist.psu.edu/paper/DDoS-Chap-Gu-June-07.pdf (дата обращения 29.09.2019).

3. Сахаров Д. В., Штеренберг С. И., Левин М. В., Колесникова Ю. А. Разработка модели обеспечения отказоустойчивости сети передачи данных // Известия высших учебных заведений. Технология легкой промышленности. 2016. Т. 34. № 4. С. 14–20.

4. Лаврова Д. С., Попова Е. А., Штыркина А. А., Штеренберг С. И. Предупреждение Dos-атак путем прогнозирования значений корреляционных параметров сетевого трафика // Проблемы информационной безопасности. Компьютерные системы. 2018. № 3. С. 70–77.

5. Штеренберг С. И., Полтавцева М. А. Распределенная система обнаружения вторжений с защитой от внутреннего нарушителя // Проблемы информационной безопасности. Компьютерные системы. 2018. № 2. С. 59–68.

6. Ковалев Д., Ковцур М. Механизмы аутентификации и управления ключами стандарта IEEE 802.11-2012 // Первая миля. 2014. № 3 (42). С. 72–77.

7. Юркин Д. В., Исаченков П. А., Патрикеев А. И. Улучшение вероятностно-временных характеристик протоколов инкапсуляции 802.11 // Вопросы кибербезопасности. 2016. № 2 (15). С. 46–53.

8. Алейников А. А., Билятдинов К. З., Красов А. В., Левин М. В. Контроль, измерение и интеллектуальное управление трафико: монография. СПб. : ЦНИТ Астерион, 2016. 92 с.

УДК 004.056
ГРНТИ 81.93.29

АЛГОРИТМ АНАЛИЗА МНОГОШАГОВЫХ АТАК ДЛЯ ОЦЕНКИ ЗАЩИЩЕННОСТИ КОМПЬЮТЕРНОЙ СЕТИ

В. А. Гаврилюк, А. А. Чечулин

Санкт-Петербургский государственный университет телекоммуникаций им. проф. М. А. Бонч-Бруевича

В настоящее время компьютерные сети используются практически во всех областях нашей жизни. Поэтому взлом таких сетей может привести к значительным финансовым и репутационным потерям. В данной статье рассмотрен способ анализа защищенности локальной сети, основанный на моделировании действий нарушителя и возможных уязвимостей программно-аппаратного обеспечения элементов этой сети. Кроме того, в статье приведено описание разработанного программного обеспечения, реализующего данный способ, а также результаты экспериментов.

оценка защищенности, графы атак, компьютерная сеть, уязвимость.

Практически все современные корпоративные сети включают в себя большое количество устройств (компьютеры, сетевое оборудование и т. д.), каждое из которых может иметь в себе уязвимости – недостатки ПО, которые могут быть использованы хакером для получения доступа к системе или сети [1]. Обнаружение и исправление всех уязвимостей в сети может потребовать большого количества времени. Поэтому актуальной задачей является разработка программного обеспечения для оценки защищенности корпоративных компьютерных сетей, которая учитывала бы не только отдельные уязвимости, но и последовательность их эксплуатации, а также топологию сети.

Для формирования возможных последовательностей эксплуатаций уязвимостей используется следующий алгоритм:

1. Формирование множества хостов, к которым есть доступ у злоумышленника.

2. Основываясь на указанном программно-аппаратном обеспечении, выполняются запросы в базу данных уязвимостей о наличии в данных системах возможности эскалации прав до администратора.

3. Если таких уязвимостей нет, то идет проверка возможности поднять свои права до уровня пользователя, а затем с уровня пользователя до адми-

нистратора. Если подобные уязвимости найдены, то данные устройства вносятся во множество подконтрольных систем и начинается аналогичная проверка уже их соседей.

4. Если поднять свои права на компьютере жертвы не удалось, но есть уязвимости, позволяющие нанести ущерб конфиденциальности, целостности или доступности системы, то такой компьютер попадает во множество уязвимых, но проверка его соседей не начинается.

5. Построение графа атаки продолжается до тех пор, пока в составляемые нами множества не перестанут поступать новые устройства.

В данной работе будет использоваться стандарт CVE (англ. *Common Vulnerabilities and Exposures*), так как база уязвимостей в этом формате общедоступна, часто обновляется и предоставляет необходимый объем данных. Поддержкой CVE занимается организация MITRE. Полностью с CVE можно ознакомится в Национальной Базе Уязвимостей США (NVD [2]).

Также имеются следующие аналоги [3], тоже представляющие собой описания уязвимостей:

– BID – эта классификация используется исключительно на портале SecurityFocus; классификация, более сжатая чем в CVE, но может дать достаточно наглядную информацию [4].

– Secunia – не имеет особых преимуществ, но именно они предлагают платную подписку на свою базу уязвимостей [5].

– ISS X-Force – помимо стандартных метрик содержит временные метрики [6].

В дальнейшем работу алгоритма можно улучшить за счет объединения информации из различных баз.

Связь уязвимости с программно-аппаратными платформами описывается в формате CPE (*Common Platform Enumeration*). Он представляет собой способ описания всех продуктов, операционных систем и устройств.

Для проверки алгоритма был реализован программный прототип, который основан на языке Python, базе уязвимостей NVD, переведенной в базу данных SQLite, а также на алгоритме поиска в глубину (англ. *Depth-First Search*), с помощью которого скрипт пробегает по созданному графу сети, который строится из передаваемого программе JSON-файлу с описанием хостов и их взаимосвязей, а также записями CPE.

В качестве тестовых данных была взята небольшая сеть, где злоумышленником является администратор одного из компьютеров (рис. 1) это компьютер под номером 0.

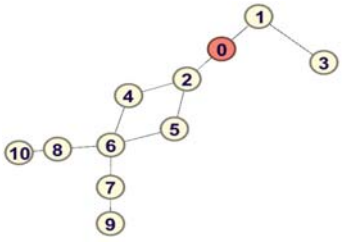


Рис. 1. Топология сети

На всех ПК установлена Windows10 версии 1703 cpe:/o:microsoft:windows_10:1703, которая имеет в себе некоторые уязвимости, но не имеет

уязвимостей, позволяющих произвести эскалацию прав до администраторских, а также в таблице указанно использующееся на компьютерах ПО.

ТАБЛИЦА. Описание хостов в сети

ID	Связи хостов	Уязвимое ПО	CPE-запись
1	0,3	Acrobat reader	cpe:/a:adobe:acrobat_reader:9.3.2
2	0,4,5	Acrobat reader	cpe:/a:adobe:acrobat_reader:9.3.2
3	1	–	–
4	2,6	Adobe flash player, VMware Workstation	cpe:/a:adobe:flash_player:9.0.48.0, cpe:/a:vmware:workstation:6.0.5
5	2,6	–	–
6	4,7,8	Microsoft Edge	cpe:/a:microsoft:edge:-
7	6,9	–	–
8	6,10	–	–
9	7	–	–
10	8	–	–

Как можно видеть на рис. 2, в приведенном примере злоумышленник смог получить контроль (отмечены красным) или нанести ущерб (отмечены желтым) большей части сети. Например, получив полный доступ, благодаря эскалации прав за счет уязвимости в Acrobat reader на компьютерах 1 и 2, а также Microsoft Edge на компьютере 6. Однако, внеся изменения в конфигурацию второго компьютера, избавив его от уязвимого ПО, мы смогли сильно ограничить злоумышленника в продвижении вглубь сети, что можно видеть на рис. 3.

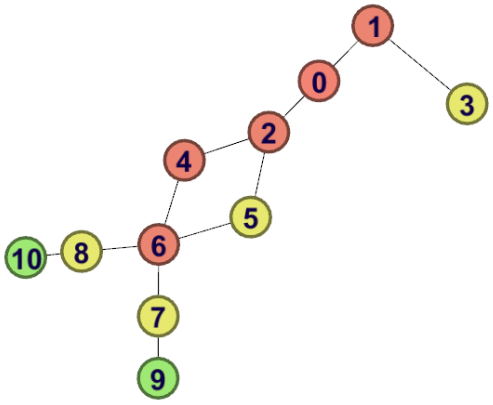


Рис. 2. Результат анализа сети

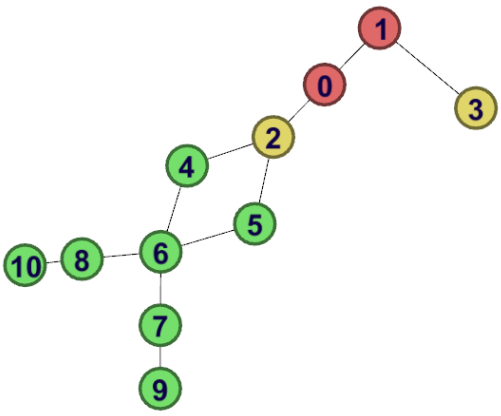


Рис.3. Результат анализа сети после внесения изменений

Таким образом, данный алгоритм позволяет не только оценить защищенность сети, но и решить какие меры стоит принять, чтобы ограничить потенциального хакера наиболее эффективно.

Список используемых источников

1. CVE Terminology [Электронный ресурс]. URL: https://www.cvedetails.com/cve-help.php (дата обращения 31.03.2020).

2. National Vulnerability Database [Электронный ресурс]. URL: https://www.nvd.nist.gov (дата обращения 31.03.2020).

3. Федорченко А. В., Чечулин А. А., Котенко И. В. Исследование открытых баз уязвимостей и оценка возможности их применения в системах анализа защищенности компьютерных сетей // Информационно-управляющие системы. 2014. № 5. С. 74–76.

4. BID [Электронный ресурс]. URL: https://www.securityfocus.com/bid (дата обращения 31.03.2020).

5. Secunia [Электронный ресурс]. URL: https://www.flexera.com/products/operations/software-vulnerability-research/secunia-research.html (дата обращения 31.03.2020).

6. X-Froce [Электронный ресурс]. URL: https://www.ibm.com/ru-ru/security/xforce (дата обращения 31.03.2020).

УДК 004.056
ГРНТИ 49.33.35

АНАЛИЗ СТРУКТУРНО НЕОПРЕДЕЛЕННОЙ ПОЛЕЗНОЙ НАГРУЗКИ СЕТЕВОГО ТРАФИКА ПРОМЫШЛЕННЫХ КИБЕРФИЗИЧЕСКИХ СИСТЕМ

Д. А. Гайфулина

Санкт-Петербургский институт информатики и автоматизации Российской академии наук

Особенностью среды передачи промышленных киберфизических систем является частое применение протоколов с нерегламентированными спецификациями, что может затруднять построение профиля сетевой активности и мониторинг событий безопасности в подобных сетях. Данная работа посвящена исследованию сетевого трафика в условиях неопределенных спецификаций сетевых протоколов киберфизических систем. Предлагается подход к анализу полезной нагрузки сетевого трафика с использованием лексического распознавания условно структурированных бинарных данных на основе частотного анализа возможных последовательностей информационных единиц и их комбинаций. Представлены методика анализа сетевого трафика и результаты экспериментов, подтверждающих применимость предлагаемого подхода. Испытательный стенд имитирует процесс работы промышленной киберфизической системы с использованием протокола MODBUS/TCP. В качестве бинарных данных для анализа принимается полезная нагрузка протокола Modbus.

анализ сетевого трафика, нерегламентированные протоколы, промышленные киберфизические системы, кибербезопасность, обнаружение вторжений.

Какие трудности могут возникнуть при анализе сетевого трафика киберфизических систем (КФС)? Это высокая разнородность источников информации, использование проприетарных (нерегламентированных) протоколов, для которых отсутствуют общеизвестные спецификации. Спецификацией сообщения называется информация о типах данных, синтаксисе и семантике полей его структуры, а также о группировке полей в определенной последовательности. Подобные проблемы могут стать причинами снижения эффективности оценки защищенности для среды передачи данных киберфизических систем.

К примеру, анализ трафика может включать следующие этапы:

1. сбор данных о пакетах сетевого трафика, в том числе информации об используемых протоколах;

2. предобработка, заключающаяся в определении признаков сетевого трафика – параметров сетевых сообщений;

3. анализ полученных признаков для выявления аномальной активности, под которой понимается поведение инфраструктуры, отличающееся от заложенного шаблонного поведения;

4. представление результатов оценки.

На втором этапе исследователь может столкнуться с проблемой, что без наличия спецификаций некоторых протоколов определить их параметры в сетевом трафике затруднительно, что ведет к частичному отсутствию данных в результатах оценки защищенности. Таким образом, возникает необходимость анализа бинарных данных сетевого трафика, позволяющего получить атрибуты нерегламентированных протоколов.

Целью данного исследования является оценка подхода к анализу структурно-неопределенной полезной нагрузки сетевого трафика. Задачами исследования являются:

1) обозначить подход к анализу бинарных данных сетевого трафика;

2) составить план эксперимента по оценке данного подхода для анализа трафика прототипа промышленной киберфизической системы;

3) оценить эффективность разработанного подхода.

Исходными данными для выполнения предлагаемого подхода является последовательность бинарных данных, представляющая запись сообщений. Далее анализ идет по примеру анализа текста на естественном языке: нам необходимо найти определенные слова, а после составить из них «словосочетания» и «предложения». В обычном тексте при этом мы имеем разделители, такие как пробелы и знаки препинания, но в бинарных данных ключевые слова необходимо искать путем поиска повторений байт, а затем

перебором их возможных последовательностей, чтобы получить интересующие нах сочетания. Подробное описание разрабатываемой методики представлены в работах автора [1, 2].

Предлагаемый подход к анализу сетевого трафика в условиях нерегламентированных протоколов был реализован на языке программирования Python и апробирован на различных наборах данных.

Поставленный эксперимент состоит из следующих этапов:

1. определить исходные данные сетевого трафика в различных режимах (нормальный и аномальный) для проведения эксперимента;

2. определить структуру бинарных данных сетевого трафика;

3. вычислить статистические характеристики сетевого трафика и построить профиль сетевой активности КФС для различных режимов;

4. сравнить профили нормальной и аномальной сетевой активности.

Исследуемый набор данных был сгенерирован для сценария автоматизации процессов управления с использованием оборудования MODBUS/TCP [3]. Он состоит из насоса для жидкости, который имитируется электродвигателем и управляется частотно-регулируемым приводом и программируемым логическим контроллером (ПЛК). Скорость двигателя определяется MODBUS устройством, который моделируется с использованием Arduino. Протокол Modbus широко применяется в промышленности для передачи данных между устройствами через последовательные интерфейсы RS-485, RS-422, RS-232 и сети TCP/IP. Тестовый стенд изображен на рис. 1.

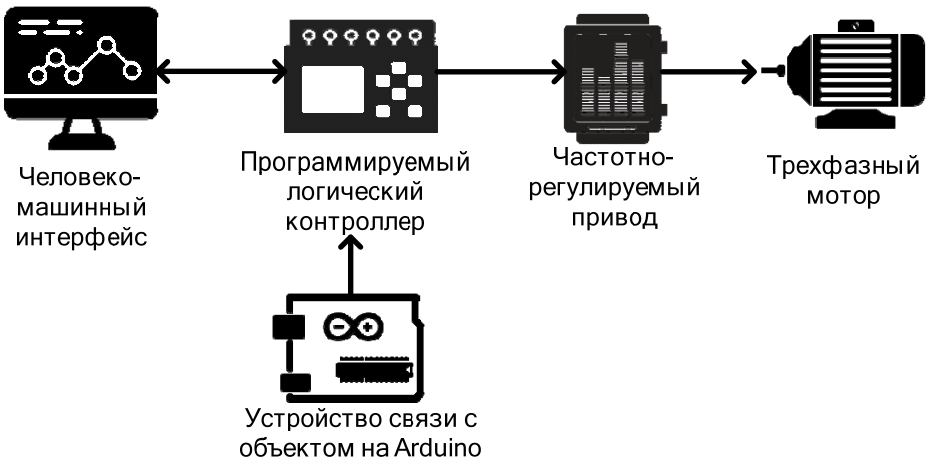


Рис. 1. Схема тестового стенда для сбора сетевого трафика

Для целей анализа на стенде было реализовано подмножество возможных атак, которые были нацелены на ПЛК [4]. Исследуемые наборы данных содержат записи сетевого трафика данной КФС для следующих сценариев:

нормальный (штатный) режим работы КФС; атака «человек посередине» (*Main-in-the-Middle*, MITM); MODBUS Query flooding; ICMP flooding; TCP SYN flooding.

На рис. 2 представлены структуры сообщения протокола, размеченные предложенным подходом.

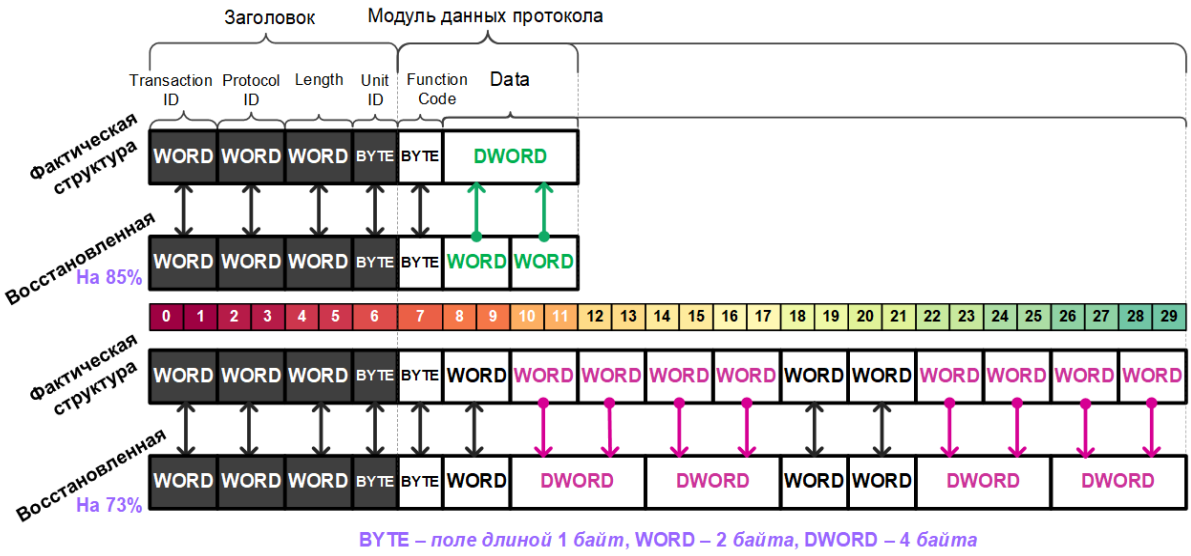


Рис. 2. Анализ полезной нагрузки сообщения протокола Modbus

Сопоставление данных полей отображено в трех видах:

двойная стрелка – полное совпадение полей;

стрелка сверху-вниз – слияние фактических полей сообщения;

стрелка снизу-вверх – дробление фактического поля сообщения.

Полное совпадение полей является наиболее удачным результатом и достигается при наличии достаточного числа дублируемых данных в бинарных данных трафика. В данном примере точность восстановления структуры от 73 % до 85 %. Применение методики анализа бинарных данных позволяет получить больше атрибутов сетевого трафика для построения профиля и выявления аномалий. В среднем, около 20 % прежде неразмеченных данных после внедрения методики пригодно для дальнейшего анализа.

В следующем примере мы используем значения одного из полей восстановленной структуры протокола. Представленные на рис. 3 (см. ниже) графики отображают распределение вероятностей для интенсивности появления различных значений поля протокола Modbus для нормального режима и режима атаки. Данный вид диаграммы позволяет отобразить медиану, квартили, минимальное и максимальное значение выборки и выбросы.

Таким образом, мы можем наблюдать появление большого числа выбросов для некоторых значений при атаке MODBUS Query flooding. Осуществим кластерный анализ для определения участка сетевого трафика, в котором присутствует аномалия. В качестве точек используются значения

интенсивности приема пакетов с исследуемым значением поля Modbus. Результат кластеризации представлен на рис. 4.

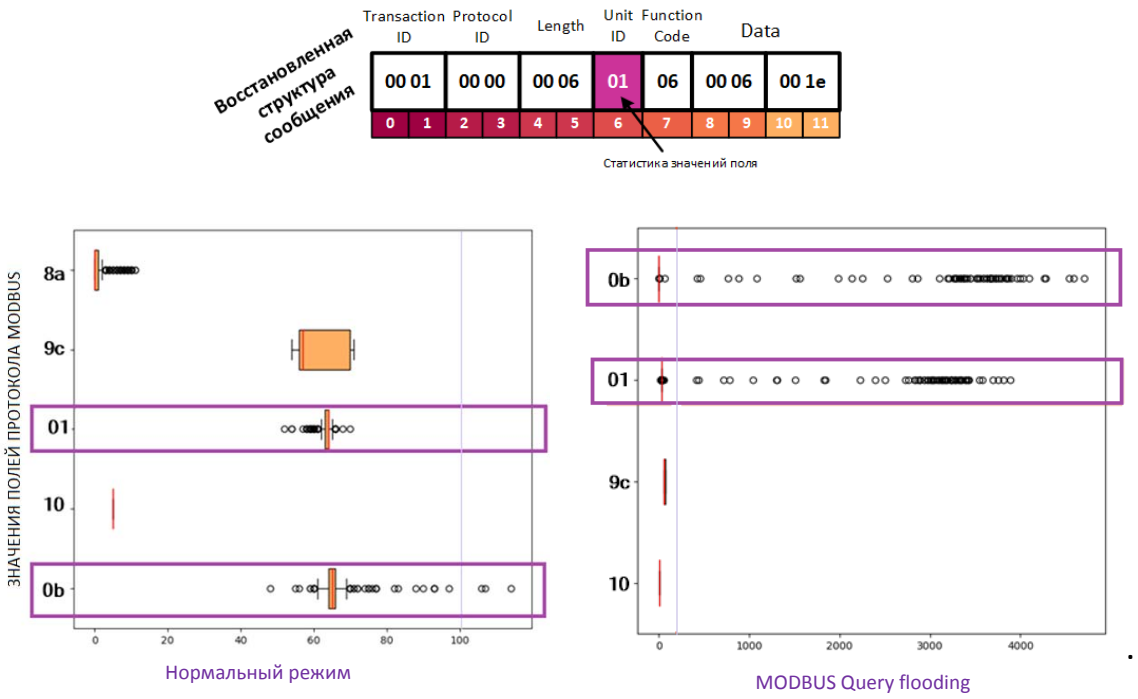


Рис. 3. Распределение интенсивности значений трафика

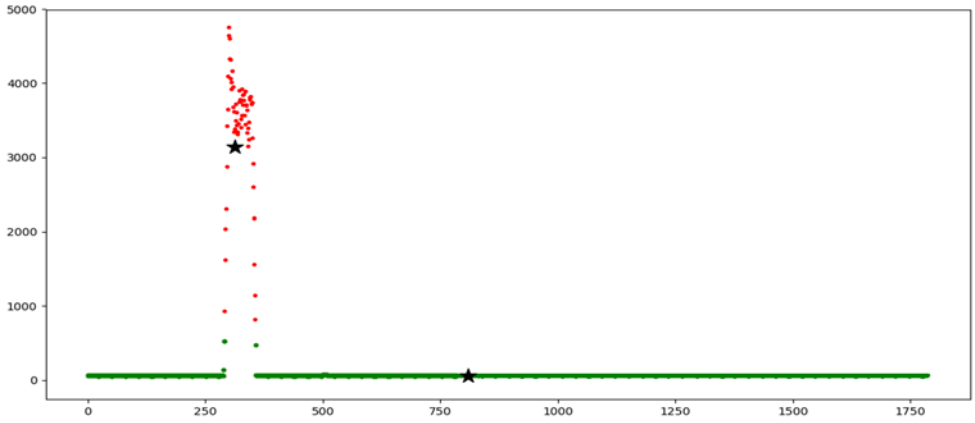


Рис. 4. Представление выявления аномалии в сетевом трафике

Таким образом, можно заключить, что на промежутке сетевого трафика между 300 и 380 секундами присутствует сетевая аномалия. Оценка качества данной кластеризации свидетельствует о высокой точности выявления аномалии в данных сетевого трафика (табл., см. ниже).

Высокие значения гомогенности, полноты и V-меры соответствуют высокой точности кластеризации. Значение силуэта, близкое к нулю, свидетельствует о том, что кластеры пересекаются и накладываются друг на друга. Таким образом, вычисленные оценки демонстрируют высокую точность выявления аномалии в данных сетевого трафика.

ТАБЛИЦА. Метрики оценки качества кластеризации

Метрика	Обозначение	Значение	Границы
Скорректированный рандовый индекс	Схожесть кластеризации	0.662295	[–1; 1]
Скорректированная взаимная информация	Независимость разбиения на кластеры	0.734566	[0; 1]
Гомогенность	Насколько каждый кластер состоит из объектов одного класса	0.83904	[0; 1]
Полнота	Насколько объекты одного класса относятся к одному кластеру	0.852974	[0; 1]
V-мера	Среднее гармоническое гомогенности и полноты	0,84595	[0; 1]
Силуэт	Плотность кластеров	0.14556	[–1; 1]

В результате исследования разработана методика анализа бинарных данных сетевого трафика, которая направлена на преодоление лексической неопределенности протоколов сетевого трафика. Практическая значимость работы заключается в возможности выполнения предварительной обработки данных сетевого трафика для автоматизированного решения задач обнаружения аномалий в условиях неопределенных спецификаций сетевых протоколов.

Работа выполнена при частичной финансовой поддержке бюджетной темы 0073-2019-0002.

Список использованных источников

1. Гайфулина Д. А., Федорченко А. В., Котенко И. В. Лексическая разметка данных сетевого трафика для оценки защищенности // Защита информации. Инсайд. 2019. № 6. С. 56–60.

2. Гайфулина Д. А., Котенко И. В., Федорченко А. В. Методика лексической разметки структурированных бинарных данных сетевого трафика для задач анализа протоколов в условиях неопределенности // Системы управления, связи и безопасности. 2019. № 4. С. 280–299.

3. Frazão I. Abreu P., Cruz T., Araujo H., Simoes P. Cyber-security Modbus ICS dataset [Электронный ресурс] // IEEE Dataport. 2019. URL: http://dx.doi.org/10.21227/pjff-1a03 (дата обращения 26.01.2020).

4. Frazão I. Abreu P., Cruz T., Araujo H., Simoes P. Denial of Service Attacks: Detecting the frailties of machine learning algorithms in the Classification Process // 13th International Conference on Critical Information Infrastructures Security (CRITIS 2018), ed. Springer. 2018. 9 p.

Статья представлена главным научным сотрудником СПИИРАН, доктором технических наук, профессором И. В. Котенко.

УДК 004.056
ГРНТИ 49.33.35

АНАЛИЗ МЕТОДОВ ГЛУБОКОГО ОБУЧЕНИЯ ДЛЯ ЗАДАЧ ОБНАРУЖЕНИЯ ВТОРЖЕНИЙ

Д. А. Гайфулина, И. В. Котенко

Санкт-Петербургский институт информатики и автоматизации Российской академии наук

В настоящее время технологии машинного обучения повсеместно применяются для решения множества задач классификации, прогнозирования и принятия решений в сфере информационной безопасности. Все чаще в основе этих направлений лежит класс методов, называемых глубоким обучением. В данном исследовании проводится анализ методов глубокого обучения, применяемых для задач обнаружения вторжений в информационно-коммуникационных системах. Предлагается общий подход к обнаружению вторжений с использованием глубокого обучения. Подход состоит в реализации четырех основных процессов: анализ исходных данных, извлечение признаков, предварительная обработка и классификация на основе глубокого обучения. Приводится сравнительная характеристика рассмотренных методов глубокого обучения с указанием параметров обучения, конфигурации сети, используемых наборов данных и итогового качества работы по экспериментальным оценкам.

глубокое обучение, глубокие нейронные сети, кибербезопасность, обнаружение вторжений.

Способность алгоритмов машинного обучения извлекать разноуровневые представления из данных делает их привлекательными для решения различных задач информационной безопасности. Для обнаружения вторжений часто применяются методы машинного обучения и вычислительного интеллекта [1]. Концепция глубокого обучения (ГО) возникла из исследований искусственных нейронных сетей. По сравнению с другими формами машинного обучения, глубокое обучение требует намного меньше ограничений и ручного программирования. В то время как эффективность обнаружения вторжений может значительно снижаться из-за высокой гетерогенности данных и несогласованности их форматов [2], алгоритмы на основе ГО позволяют осуществлять автоматический отбор информативных признаков и работать напрямую с необработанными, в том числе большими, данными.

Целью данного исследования является анализ методов глубокого обучения, применяемых для задач обнаружения вторжений в информационно-коммуникационных системах. Задачами исследования являются:

1) провести обзор существующих исследовательских работ;

2) определить общий подход к обнаружению вторжений с использованием глубокого обучения;

3) составить сравнительную характеристику рассмотренных методов глубокого обучения.

Методы обнаружения вторжений с использованием *автокодировщиков* основаны на реконструкции данных, при которой определяется величина различия нормальных и аномальных данных. В статье [3] авторы представили решение AutoIDS, использующее в качестве детекторов два автокодировщика. На этапе тестирования сбой нейронных сетей при обработке пакетов означает, что такой поток не соответствует нормальному трафику. Оценка AutoIDS проводилась на наборе данных NSL-KDD и показала точность 90,17 %. Также системы обнаружения вторжений, управляемые автокодировщиками, представлены в исследованиях [4, 5], а в работе [6] предлагается метод с применением шумоподавляющего автокодировщика для реконструкции входных данных из зашумленной версии ввода. Лучший результат оценивается с точностью 90,32 %.

Аналогично автокодировщикам ограниченная машина Больцмана (*Restricted Boltzmann Machine*, RBM) применяет реконструкцию данных. Исследование [7] посвящено использованию RBM для обнаружения кибератак в мобильной облачной среде. Результаты экспериментов показывают, что предлагаемая структура распознает различные кибератаки с точностью 97,11 %. Работа [8] посвящена определению DDoS-атак с использованием классификатора RBM, а отбор признаков производится с помощью модели оптимизации поиска с произвольной гармонией (*Random Harmony Search*, RHS). Модель RHS-RBM протестирована на основе набора данных KDD-99 и достигает максимальной точности 99,92 %.

Отличительной особенностью рекуррентных нейронных сетей (*Recurrent Neural Network*, RNN) является наличие обратной связи, чт позволяет им анализировать последовательные данные и временные ряды. Анализируя последовательность измерений, сеть обучается предсказывать состояние процесса. Если предсказанное RNN состояние отличается от текущего, регистрируется аномалия. В исследовании [9] RNN применяется для бинарной и мультиклассовой классификации сетевых данных при обнаружении вторжений. Самая высокая точность обнаружения составила 83,2 8% для двоичной классификации и 81,29 % для мультиклассовой. Недостатком стандартных RNN являются проблемы с нехваткой памяти для информации прошлого времени. В работе [10] предлагается метод обнаружения вторжений, основанный на долговременной кратковременной памяти (*Long Short-Term Memory*, LSTM), который улучшает проблемы недостаточной временной памяти. В статье [11] используется RNN с управляемым рекуррентным блоком (*Gated Recurrent Units*, GRU). Эффективность GRU сопоставима с LSTM, но GRU обладает меньшим числом параметров,

что облегчает их обучение нейронной сети. Описанный подход продемонстрировал точность обнаружения 99,91 %.

Помимо рекуррентных нейронных сетей для анализа и прогнозирования временных рядов могут применяться сверточные нейронные сети (*Convolutional Neural Network*, CNN). Они используют операцию свертки, что также позволяет использовать их для выявления аномалий. В работе [12] представлен метод классификации вредоносного сетевого трафика на основе CNN и RNN для решения проблем в программно-определяемых сетях (*Software Defined Networking*, SDN). Оценка подхода проводилась на наборах данных, один из которых сгенерирован в симуляторе SDN, а второй является набором данных CTU-13. Наилучшая точность модели может достигать 99,86 % для CTU-13 и 99,84 % для сгенерированных данных.

Одним из подходов к обнаружению вторжений является использование генеративно-состязательных сетей (*Generative Adversarial Networks*, GAN) для генерации поддельных сетевых данных с целью повышения производительности исходной модели обнаружения. Так в работе [13] данная модель применима для выявления бот-сетей. Авторы провели экспериментальные исследования набора данных ботнетов ISCX, продемонстрировавшие точность обнаружения в 71,17 %. В исследовании [14] модель на основе двунаправленной GAN используется для обнаружения вторжений. Подобная модель была протестирована на наборе данных KDD-99 и показала точность обнаружения в 93,24 %.

На основе проведенного обзора, можно составить схему общего подхода к обнаружению вторжений с использованием методов глубокого обучения (рис.). Данный подход состоит в реализации четырех основных процессов: анализ исходных данных, извлечение признаков, предварительная обработка и классификация на основе глубокого обучения.

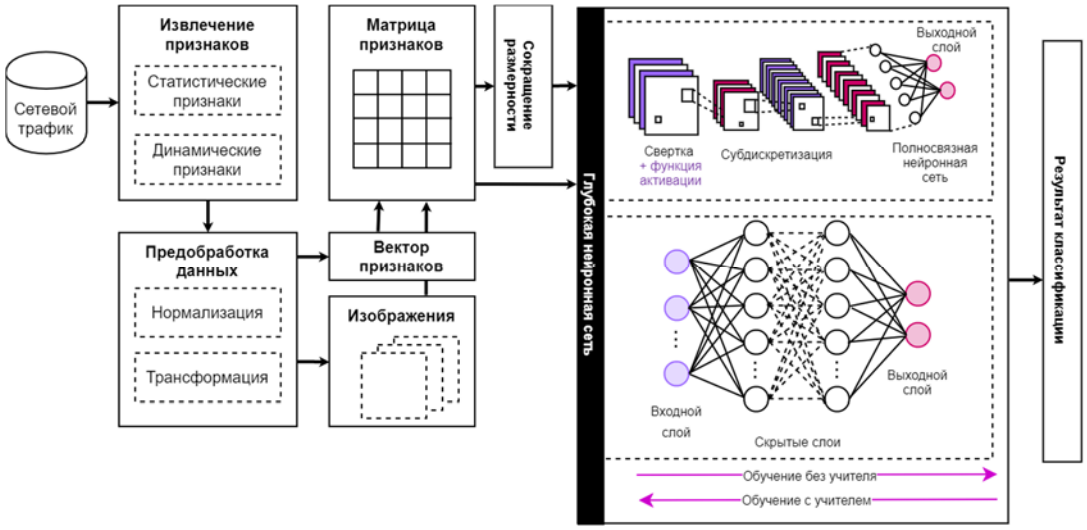


Рис. Подход к обнаружению вторжений с использованием глубокого обучения

В таблице показаны следующие характеристики используемых методов глубокого обучения: архитектура сети – количество слоев и нейронов в каждом из них (*x* – входной слой, *y* – выходной слой, *h* – скрытый слой, *p* – субдискретизирующий слой, *c* – сверточный слой, *n* – полносвязный слой), функция активации (*sigm* – сигмоида, *htang* – гиперболический тангенс), используемые наборы данных, точность обнаружения для предложенного подхода (метрика аккуратности).

ТАБЛИЦА. Значения времени передачи кадра при различных соотношениях параметров

Статья	Метод	Архитектура сети (число нейронов)	Функция активации	Набор данных	Точность метода, %
[3]	SAE+AE	*h*(140)–*h*(80)	ReLu, sigm	NSL-KDD	90,17
[4]	AE	*x*(102)–*h*(50)–*y*(102)	softmax	NSL-KDD	87
[5]	AE	*h*(32)–*h*(32)–*h*(32)–*h*(32)	sigm	KDD-99	94,71
[6]	DAE	*x*(122)–*h*(8)–*y*(122)	ReLu	NSL-KDD	90,32
[7]	RBM	2*h*(1000)	sigm	NSL-KDD, KDD-99, UNSW-NB15	97,11
[8]	RHS+RBM	9*h*(1000)	sigm	KDD-99	99,92,
[9]	RNN	*h*(80)	sigm	NSL-KDD	83,28
[10]	RNN-LSTM	*h*(256)	L2	CICIDS2017	91
[11]	RNN-GRU	*h*(?)	dropout	KDD-99	99,91
[12]	CNN+RNN	CNN(4*c*–4*p*–4*n*)– –RNN(*h*(300))	L2	Собственный, CTU-13	99,86
[13]	GAN	LSTM(*x*(120)-*h*(80)– –*y*(122))+DNN(*h*(122)– –*h*(80)–*h*(20)–*y*(3))	softmax	ISCX botnet dataset	71,17
[14]	GAN	discriminator, encoder and generator	L1	KDD-99	93,24

Можно сделать вывод, что большинство подходов дают хорошие результаты для обнаружения вторжений. Подход [13], вероятно, показал низкое качество из-за использования малого количества признаков. Подходы [4, 9] имеют меньшее качество по сравнению с остальными, что можно связать с использованием недостаточно глубоких архитектур. Для обнаружения вторжений лучшие результаты показывают глубокие сети доверия с большим количеством нейронов [8] и методы обучения с использованием реккурентных нейронных сетей [11, 12].

С увеличением числа слоев в глубоких нейронных сетях ошибка обучения возрастает, а производительность сети ухудшается. В соответствии

с этим выводом, в качестве основного направления будущего развития глубоких нейронных сетей можно отметить увеличение размера сетей, то есть количества нейронов на каждом слое, и глубины сетей. При этом данный аспект требует мощных вычислительных ресурсов и может привести к риску переобучения. Еще одним направлением развития является использование информации из разных источников и комбинация разных типов признаков, как статистических, так и динамических.

Работа выполнена при частичной финансовой поддержке бюджетной темы 0073-2019-0002.

Список используемых источников

1. Браницкий А., Котенко И. Анализ и классификация методов обнаружения сетевых атак // Труды СПИИРАН. 2016. № 4. С. 207–244.

2. Гайфулина Д. А., Котенко И. В., Федорченко А. В. Методика лексической разметки структурированных бинарных данных сетевого трафика для задач анализа протоколов в условиях неопределенности // Системы управления, связи и безопасности. 2019. № 4. С. 280–299.

3. Gharib M., Mohammadi B., Dastgerdi S. H., Sabokrou M. AutoIDS: Auto-encoder Based Method for Intrusion Detection System // arXiv preprint arXiv: 1911.03306, 2019. PP. 1–9.

4. Ieracitano C., Adeel A., Morabito F. C., Hussain A. A Novel Statistical Analysis and Autoencoder Driven Intelligent Intrusion Detection Approach // Neurocomputing. 2019. PP. 1–12.

5. Farahnakian F., Heikkonen J. A deep auto-encoder based approach for intrusion detection system // 2018 20th International Conference on Advanced Communication Technology (ICACT), IEEE, 2018. PP. 178–183.

6. Mohamed S., Ejbali R., Zaied M. Denoising Autoencoder with Dropout based Network Anomaly Detection // The Fourteenth International Conference on Software Engineering Advances (ICSEA 2019), 2019. PP. 98–104.

7. Nguyen K. K., Hoang D. T., Niyato D., Wang P., Nguyen D., Dutkiewicz E. Cyberattack detection in mobile cloud computing: A deep learning approach // 2018 IEEE Wireless Communications and Networking Conference (WCNC). IEEE, 2018. PP. 1–6.

8. Mayuranathan M., Murugan M., Dhanakoti V. Best features based intrusion detection system by RBM model for detecting DDoS in cloud environment // Journal of Ambient Intelligence and Humanized Computing. 2019. PP. 1–11.

9. Yin C., Zhu Y., Fei J., He X. A deep learning approach for intrusion detection using recurrent neural networks // IEEE Access. 2017. Vol. 5. PP. 21954–21961.

10. Zhu M., Ye K., Wang Y., Xu C. Z. A deep learning approach for network anomaly detection based on AMF-LSTM // IFIP International Conference on Network and Parallel Computing Springer, Cham, 2018. PP. 137–141.

11. Manavi M., Zhang Y. A new intrusion detection system based on gated recurrent unit (GRU) and genetic algorithm // International Conference on Security, Privacy and Anonymity in Computation, Communication and Storage, Springer, Cham, 2019. PP. 368–383.

12. Qin Y., Wei J., Yang W. Deep Learning Based Anomaly Detection Scheme in Software-Defined Networking // 2019 20th Asia-Pacific Network Operations and Management Symposium (APNOMS), IEEE, 2019. PP. 1–4.

13. Yin C., Zhu Y., Liu S., Fei J., Zhang H. An enhancing framework for botnet detection using generative adversarial networks // 2018 International Conference on Artificial Intelligence and Big Data (ICAIBD). IEEE, 2018. PP. 228–234.

14. Chen H., Jiang L. GAN-based method for cyber-intrusion detection // arXiv preprint arXiv: 1904.02426. 2019. PP. 1–6.

УДК 004.42
ГРНТИ 50.41.25

РАЗРАБОТКА МОБИЛЬНОГО ПРИЛОЖЕНИЯ, РЕАЛИЗУЮЩЕГО ФУНКЦИИ ПРЕЗЕНТЕРА ДЛЯ УНИВЕРСАЛЬНОГО ФОРМАТА ПРЕЗЕНТАЦИЙ

М. А. Галактионов, Д. В. Окунева

Санкт-Петербургский государственный университет телекоммуникаций им. проф. М. А. Бонч-Бруевича

В данной статье рассматриваются подходы и процесс разработки программного обеспечения для дистанционного управления презентацией. Цель разработки заключается в создании ПО, позволяющего управлять презентацией без презентера, с помощью мобильного устройства (смартфона), а также использовать универсальный формат презентаций PDF без электронных накопителей.

программное обеспечение, презентер, клиент-серверная архитектура, слайд, Android, java, python.

Одним из наиболее важных аспектов публичного выступления является презентация. Именно видеоряд или слайды помогают выступающему проиллюстрировать свою речь. На сегодняшний день презентации присутствуют в выступлениях, затрагивающих самые разнообразные сферы жизни, например, деловые выступления, бизнес-презентации, научные доклады и многое другое.

Успех выступления очень часто зависит от его эффектности. Это значит, что выступающий должен постоянно держать контакт с аудиторией, но, если при этом он также вынужден прерывать выступление для того, чтобы подойти к компьютеру и переключить слайд, то выступление получается сбивчивым и теряет целостность. Во избежание этого было разработано устройство под названием кликер (от англ. *click*) или презентер (от англ. *present*). Данное устройство позволяет переключать слайды презентации дистанционно, что в свою очередь позволяет оратору не отвлекаться от выступления.

Часто проблему могут вызвать несовпадающие форматы презентаций, например, презентацию, подготовленную с помощью онлайн-сервиса Prezi, нельзя открыть и воспроизвести с помощью очень распространенного программного обеспечения PowerPoint. Также не стоит забывать о человеческом факторе, очень часто бывает так, что из-за забытого флеш-накопителя срывается важная презентация.

Решить все вышеперечисленные проблемы можно за счет программного обеспечения, которое позволит дистанционно управлять презентацией, избавит от необходимости использования разного рода накопителей и универсализирует формат презентаций.

Анализ рынка существующих мобильных приложений для дистанционного управления презентациями, результаты которого приведены в таблице, показал, что приложение, которое бы удовлетворяло вышеперечисленным требованиям, пока отсутствует.

ТАБЛИЦА. Таблица сравнительных характеристик существующих решений

Название продукта	Регистрация	Соединение с облаком	Доп. ПО	Способ трансляции	Время отклика	Кол-во условных шагов
Presentor mobile	Да	Да	Да	Нет данных	Нет данных	БОЛЕЕ 10
Presenter wear free	Нет	Нет	Да	Запрос	Менее 1 сек	8
Display link presenter	Да	Нет	Да	Контент	~1 сек	БОЛЕЕ 10
Mouse kit	Нет	Нет	Да	Запрос	Менее 1 сек	10
Пульт для презентаций	Нет	Нет	Да	Запрос	Менее 1 сек	12

В связи с этим, было решено разработать приложение с клиент-серверной архитектурой, и это обусловлено рядом факторов, речь о которых пойдет далее [1].

Подобный подход диктуется тем, что позволяет снизить аппаратные требования к терминалам конечных пользователей, кроме того, данная архитектура необходима, т.к. помимо мобильного клиента нужен еще и веб-клиент.

Клиентское приложение разрабатывалось на Java [2] для устройств под управлением операционной системы Android [3]. Java это не только язык программирования, но и платформа, которая включает в себя встроенную среду выполнения, а также огромное количество готовых классов, которые сильно облегчают разработку.

Компонента веб приложения разработана на JavaScript с использованием библиотеки React. Все современные браузеры имеют поддержку JavaScript, что очень важно, так как разрабатываемое веб-приложение должно работать во всех современных браузерах.

Серверная компонента написана на языке Python [4, 5]. Python вобрал в себя современные тенденции в программировании «с нуля». Кроме того, он динамично развивается: процесс включения новых конструкций в язык хорошо отлажен, и он продолжает впитывать в себя приемы функционального программирования, аспектно-ориентированного программирования и прочего, оставаясь при этом обратно-совместимым и внутренне непротиворечивым.

Причинами выбора данной связки является ее простота и распространенность. Любой программный продукт после первого релиза нужно обслуживать и совершенствовать, в случае с Python и JavaScript это достаточно легко.

Мобильное приложение состоит из семи подсистем: отрисовки страницы PDF; асинхронной отправки номера страницы; асинхронной отправки кода авторизации; асинхронной загрузки файла; авторизации VK Docs; авторизации Google drive; отображения списка доступных документов.

В состав веб-клиента входит подсистема авторизации на сервере, серверное приложение обеспечивает синхронизацию и взаимодействия между компонентами мобильного и веб-клиентов.

Подводя итоги, можно сказать, что в результате было разработано программное решение, позволяющее: управлять презентацией с мобильного устройства (смартфона), взаимодействовать с облачными хранилищами и использовать универсальный формат презентаций, как PDF-файлы.

Список используемых источников

1. Роджерс Р., Ломбардо Д. Android. Разработка приложений. М. : ЭКОМ Паблишерз, 2010. 400 с. ISBN 978-5-9790-0113-5.

2. Герберт Шилдт. Java. Полное руководство, 10-е издание. Java. The Complete Reference, 10th Edition. М. : Диалектика, 2018. 1488 с. ISBN 978-5-6040043-6-4.

3. Донн Фелкер. Android: разработка приложений Android Application Development for Dummies. М. : Диалектика, 2011. 336 с. ISBN 978-5-8459-1748-5.

4. Марк Лутц. Программирование на Python ; пер. с англ. 4-е изд. СПб. : Символ-Плюс, 2011. Т. 1. 992 с. ISBN 978-5-93286-210-0.

5. Марк Лутц. Изучаем Python; пер. с англ. 4-е изд. СПб. : Символ-Плюс, 2010. 1280 с. ISBN 978-5-93286-159-2

УДК 004.056
ГРНТИ 81.93.29

ОЦЕНКА РИСКОВ И УГРОЗ БЕЗОПАСНОСТИ В СРЕДЕ «УМНЫЙ ДОМ»

А. М. Гельфанд, А. А. Казанцев, А. В. Красов, Г. А. Орлов

Санкт-Петербургский государственный университет телекоммуникаций им. проф. М. А. Бонч-Бруевича

В среде «умного дома» системы и устройства автоматически управляются и взаимодействуют друг с другом, чтобы обеспечить удобство и эффективность для жителей дома, повышая качество их жизни. Тем не менее, концепция умной домашней среды и тот факт, что она всегда связана с внешним миром через Интернет, могут вызвать много проблем. Основными целями исследования являются выявление различного рода уязвимостей безопасности «умного дома» и представление рисков для жителей.

IoT, Internet of Thing, Интернет вещей.

Интернет вещей – формирующаяся парадигма, обусловленная широким развитием информационных и коммуникационных технологий. Инфраструктура IoT включает в себя сеть устройств и объектов, подключенных к контроллеру управления и удаленному серверу.

Хотя существует несколько определений «умного дома», с технической точки зрения, общая концепция заключается в подключении датчиков, бытовой техники и интеллектуальных устройств через Интернет для достижения удаленного мониторинга, удаленного доступа и дистанционного управления жилой средой. При проектировании любой среды «умного дома» основное внимание фокусируется на автоматизации и контроле экологических услуг, таких как освещение, отопление, вентиляция и кондиционирование воздуха, мониторинг и контроль, безопасность, а также экономии энергии. Поскольку среда интеллектуального дома будет содержать важную и конфиденциальную информацию, такие дома требуют нового уровня требований к защите. В случае взлома системы или устройства, злоумышленник может вторгнуться в частную жизнь пользователя, украсть личную информацию и контролировать пользователей в среде «умного дома».

В этой статье рассматривается проблема угроз безопасности «умного дома» на основе Интернета вещей, как на кибер-, так и на физические риски безопасности в домене, и предлагаются способы снижения угрозы.

Определение угроз

В таблице показаны информационные активы, которые были идентифицированы и использованы в процессе оценки рисков, связанные с ними угрозы, а также последствия или потенциальные последствия в виде конкретных рисков и оценок рисков. При угрозе кражи личности законного пользователя, как показано в таблице в разделе 1, противник пытается действовать от имени законного пользователя. Доступ к учетным данным пользователя в таком случае может быть осуществлен с помощью социальной инженерии или путем перехвата простых данных, которые обеспечивают доступ к ресурсам Интернета вещей [1, 2].

ТАБЛИЦА. Угрозы безопасности на информационные активы и возможные риски

№	Информационные ресурсы	Возможные угрозы безопасности	Возможные последствия (риски)
1	Учетные данные пользователя	Подмена личности пользователя и кража учетных данных	Несанкционированный доступ к основной системе «умный дом». Потеря контроля над системой «умный дом»
2	Мобильные персональные данные и приложения	Введение вредоносного кода в приложения, установленные на телефоне	Злоумышленник может удаленно управлять смартфоном: делать фотографии, отслеживать местоположение, получать доступ к микрофону телефона и камере, совершать звонки
3	Информация, собираемая устройствами. Информация о состоянии «умного дома»	Изменение информации. Атака типа «отказ в обслуживании» (DoS). Компрометация устройства или датчика. Раскрытие информации	Манипуляция измерениями для проникновения в домашнюю систему. Получение информации отслеживания присутствия для осуществления ограбления. Финансовые потери
4	Информация о структуре «умного дома»	Поиск конкретного устройства с известными уязвимостями для атаки на «умные дома»	Злоумышленник идентифицирует самое слабое устройство с известными уязвимостями. Злоумышленник берет под свой контроль системы «умного дома». Финансовые потери
5	Журнальная информация	Сбор полезной информации для осуществления атаки на систему «умного дома» [3]	Злоумышленник находит способ получить доступ к основной системе. Злоумышленник изменяет конфигурацию системы и добавляет backdoor. Финансовые потери

№	Информационные ресурсы	Возможные угрозы безопасности	Возможные последствия (риски)
6	Информация, передаваемая через шлюз	Кража информации из пакетов, передаваемых через шлюз	Системные ресурсы исчерпываются за счет постоянной саморепликации. Возможность вывести систему из строя, сделав ее в конечном счете непригодной для использования. Возможность внедрения в систему. новых уязвимостей системы безопасности
7	Информация о настройке «интеллектуального дома»	Изменение информации	Несанкционированный доступ к основной системе «умный дом». Потеря контроля над системой «умный дом». Финансовые потери
8	Видео камер наблюдения	Контроль камер для мониторинга и слежки за пользователями	Нарушение конфиденциальности пользователей. Финансовые потери. Ущерб репутации
9	Информация об отслеживании местоположения	Наблюдение за трафиком данных о местоположении пользователя	Нарушение конфиденциальности пользователей. Осуществление ограбления
10	Информационные ресурсы (например, фотографии, документы и музыка)	Кража частной информации. Порча носителя из-за сбоя оборудования	Нарушение конфиденциальности пользователей. Потеря информации. Ущерб репутации

Угрозы для устройства, описанные в таблице 1 в разделе 3, могут привести к возникновению ситуаций, когда датчики перестают отправлять сигнал при обнаружении физических рисков, таких как пожар, наводнение или любое странное движение в доме, либо посылают ложные сигналы. Кроме того, перехватив информацию, собранную установленными датчиками, как указано в разделе под номером 6, злоумышленник может внедрить вредоносный код, вирус или червя в сетевой трафик, а затем выпустить его в системе или мобильных приложениях [4]. Интенсивное использование ресурсов системы путем постоянной саморепликации приводит к тому, что система не может выполнить соответствующую работу и выводит систему из строя. Получив доступ к данным о местоположении с мобильных устройств или устройств с поддержкой GPS, как указано в разделе 9, злоумышленник может сделать вывод, что пользователь находится вне дома, что может привести к серьезным последствиям, таким как финансовые потери из-за ограбления дома.

Риски и подходы к смягчению последствий в действии

Архитектура интеллектуального дома на основе интернета вещей делится на три уровня: уровень устройства, сетевой уровень и уровень приложений. Риски безопасности могут пересекать более одного уровня Интернета вещей. Например, риск несанкционированного доступа можно обнаружить в доступе к основным системным конфигурациям, доступе к IoT-шлюзу и при входе в приложения «умного дома». Поэтому во всех этих точках должен быть реализован надежный метод многофакторной аутентификации.

IoT-устройства, такие как датчики, не обладают высокой вычислительной мощностью и большим объемом памяти. Поэтому внедрение интенсивных решений по обеспечению безопасности может оказаться недоступным вариантом. Чтобы обеспечить безопасное соединение между устройствами Интернета вещей и шлюзом внутри среды «умного дома», следует принять во внимание распределенный механизм шифрования или энергоэффективный подход к шифрованию данных [5]. Шлюз Интернета вещей восприимчив к различным эксплойтам безопасности, таким как атака «человек посередине» для сбора данных с устройств Интернета вещей. Таким образом, безопасность шлюза является необходимостью для защиты потока данных внутри и за пределами среды «интеллектуального дома». Безопасный шлюз может быть построен путем реализации эффективных алгоритмов безопасности, таких как криптография эллиптических кривых (ECC) и использование надежных подходов аутентификации пользователей [5, 6].

Для достижения высокого уровня безопасности на всем пути передачи данных, от устройства Интернета вещей до домашнего пользователя на удаленной стороне, сетевое соединение с интернет-провайдером должно быть защищено. Общие механизмы сетевой безопасности, такие как виртуальные частные сети (VPN), должны быть реализованы для обеспечения зашифрованной связи с провайдером. Необходимо развернуть распределенную систему обнаружения вторжений (IDS) для сетей Интернета вещей. Кроме того, сбор и мониторинг трафика с использованием сертифицированного оборудования и программного обеспечения может быть развернут для построения системы раннего обнаружения любого аномального поведения в сетевом трафике [6, 7].

«Умные дома» на базе Интернета вещей очень уязвимы для внешних атак. Если вся домашняя система или устройство будут скомпрометированы, противник сможет вторгнуться в частную жизнь жителей, украсть личную или конфиденциальную информацию, контролировать систему умного дома и даже контролировать жителей внутри среды. Физические риски для аппаратного обеспечения связаны с кражей, дефектами, манипуляциями и саботажем различных устройств внутри или вне «умной» домашней среды. Самая высокая оценка риска связана с кибер-или информационными

активами, такими как учетные данные пользователей, мобильные персональные данные и приложения пользователей. В рамках сетевой коммуникации основные риски связаны со слабыми механизмами аутентификации, отсутствием безопасных каналов связи и отсутствием соответствующих механизмов шифрования данных.

Надежные методы аутентификации пользователей, такие как биометрия, должны быть рассмотрены и применены к «интеллектуальным домам» на базе Интернета вещей. Биометрическая защита направлена на достижение идентификации или верификации человека на основе его физиологических или поведенческих характеристик.

Заключение

Применение технологии Интернета Вещей к «умным домам» дает как возможности, так и риски для безопасности. Такие дома очень уязвимы к различным угрозам безопасности как внутри, так и снаружи дома. Если безопасность системы или устройства будет нарушена, то под угрозой окажется конфиденциальность пользователя, его личная информация и безопасность. Поэтому необходимо принять соответствующие меры, чтобы сделать «умные дома» более безопасными и пригодными для проживания. Тщательная оценка рисков безопасности должна предшествовать любой реализации мер безопасности, чтобы гарантировать, что все соответствующие проблемы будут обнаружены первыми. В данной статье была успешно проведена комплексная оценка рисков безопасности и определены 10 критических кибер- и физических активов.

Результаты оценки рисков показывают, что человеческие факторы являются самыми большими причинами рисков, поскольку пользователи с различной степенью технической осведомленности живут в «умных домах». Таким образом, программа повышения осведомленности о безопасности является обязательной во всех случаях, чтобы уменьшить количество рисков безопасности и величину ожидаемого ущерба.

Список используемых источников

1. Пестов И. Е., Сахаров Д. В., Сергеева И. Ю., Чернобородов И. С. Выявление угроз безопасности информационных систем // Актуальные проблемы инфотелекоммуникаций в науке и образовании. VI Международная научно-техническая и научно-методическая конференция: сб. науч. ст. в 4-х т. СПб. : СПбГУТ, 2017. С. 525–527.

2. Ушаков И. А., Котенко И. В. Модель обнаружения внутренних нарушителей на основе использования технологий больших данных // Региональная информатика и информационная безопасность 2017. С. 253–254.

3. Кобзев С. А., Кулешов А. А., Ушаков И. А. Проектирование и реализация прототипа системы централизованного сбора, хранения и обработки системных журналов // Актуальные проблемы инфотелекоммуникаций в науке и образовании. VI Международная научно-техническая и научно-методическая конференция: сб. науч. ст. в 4-х т. СПб. : СПбГУТ, 2017. С. 410–416.

4. Штеренберг С. И., Красов А. В., Цветков А. Ю. Компьютерные вирусы: учеб. пособие. СПб., 2015. Т. 1.

5. Котенко И. В., Левшун Д. С., Чечулин А. А., Ушаков И. А., Красов А. В. Комплексный подход к обеспечению безопасности киберфизических систем на основе микроконтроллеров // Вопросы кибербезопасности. 2018. № 3 (27). С. 29–38.

6. Виткова Л. А., Денисов Е. И., Сахаров Д. В., Ушаков И. А. Вопросы формирования безопасной информационной системы на основе технологии децентрализованных сетей // Актуальные проблемы инфотелекоммуникаций в науке и образовании. VII Международная научно-техническая и научно-методическая конференция: сб. науч. ст. в 4-х т. СПб. : СПбГУТ, 2018. С. 174–179.

7. Котенко И. В., Ушаков И. А. Технологии больших данных для мониторинга компьютерной безопасности // Защита информации. Инсайд. 2017. № 3 (75). С. 23–33.

УДК 004.056.5
ГРНТИ 81.93.29

ИССЛЕДОВАНИЕ РАСПРЕДЕЛЕННОГО МЕХАНИЗМА БЕЗОПАСНОСТИ ДЛЯ УСТРОЙСТВ ИНТЕРНЕТА ВЕЩЕЙ С ОГРАНИЧЕННЫМИ РЕСУРСАМИ

А. М. Гельфанд, А. А. Казанцев, А. В. Красов, Г. А. Орлов

Санкт-Петербургский государственный университет телекоммуникаций им. проф. М. А. Бонч-Бруевича

С развитием и распространением Интернета вещей все большее количество устройств подключаются к Интернету и передают личные и конфиденциальные данные. В данной статье рассмотрен распределенный механизм для обеспечения безопасной передачи данных в среде IoT с устройствами класса 0, имеющими ограниченные ресурсы для выполнения вычислений, необходимых при шифровании. Целью исследование является изучение всего пути передачи данных в двух сегментах устройство-контроллер и контроллер-сервер.

IoT, Интернет вещей.

В последнее время Интернет вещей, придуманный как таковой в 1999 году, стал эволюционирующей парадигмой в области беспроводной связи. Общая инфраструктура IoT – это сеть устройств и объектов, таких как встроенные компьютеры, управляемые и интеллектуальные автоматизированные устройства, и датчики, подключенные к шлюзу Интернета вещей и удаленному серверу [1].

Ограниченные устройства Интернета вещей (IoT-устройства класса 0) – это устройства с ограниченными ресурсами в отношении вычислительной мощности процессора, ПЗУ, оперативной памяти и времени автономной

работы. Такие устройства часто имеют небольшие размеры и ограниченные функции, к ним относятся датчики и интеллектуальные устройства, управляющие электрическими приборами или услугами. Они способны собирать и передавать данные, например, показания датчиков, через Интернет для хранения и анализа. Такие данные могут быть личными или конфиденциальными и не должны попасть в руки злоумышленника. В некоторых областях применения IoT, например, здравоохранение, утечка таких данных может угрожать жизни людей.

В данной статье рассмотрен распределенный механизм безопасности, который подходит для устройств Интернета вещей класса 0. Философия рассматриваемого решения заключается в том, что легкое ресурсоемкое объектное шифрование реализуется на стороне IoT-устройства, где обработка объектов и протоколов, сильно потребляющая ресурсы, делегируется шлюзу, который выступает в качестве посредника между устройством Интернета вещей и Интернетом.

Распределенный механизм безопасности

Механизм охватывает три компонента систем Интернета вещей: IoT-устройство, шлюз IoT и удаленный веб-сервер. Каждый компонент подробно обсуждается вместе с описанием того, как передаются данные. Конструкция рассмотренного механизма обеспечения безопасности направлена на достижение требований к устройствам класса 0:

1. Обеспечение безопасности данных между устройством класса 0 и шлюзом Интернета вещей.
2. Обеспечение безопасности данных между шлюзом Интернета вещей и интернетом.
3. Эффективная работа с потреблением минимальных ресурсов.

Безопасность от устройства к шлюзу

С точки зрения связи, другой уровень безопасности между IoT-устройством и шлюзом может быть достигнут с помощью аппаратного симметричного шифрования уровня канала передачи данных (DLL) как части беспроводного протокола (например, IEEE 802.15.4, IEEE 802.11 n). Беспроводная передача может быть обеспечена с помощью модуля IEEE 802.15.4, такого как интерфейс ZigBee или Low power Wireless Personal Area Network (6LoWPAN). При подключении к сети устройства защищаются с помощью PSK, который устанавливается на каждом авторизованном устройстве и необходим для инициализации связи между шлюзом и устройствами в сети. Любые несанкционированные устройства, контролирующие трафик, не смогут расшифровать данные без правильного PSK [2].

Конфиденциальность обеспечивается между IoT-устройством и местом назначения путем шифрования данных на уровне объекта. Безопасность

объектного уровня существует на прикладном уровне внутри полезной нагрузки пакета передачи. Формат пакета и шифрование данных показаны на рис. 1. Этот уровень шифрования используется в качестве основного уровня защиты, и может быть объединен с предлагаемой беспроводной безопасностью для более надежной защиты между IoT-устройством и шлюзом Интернета вещей.

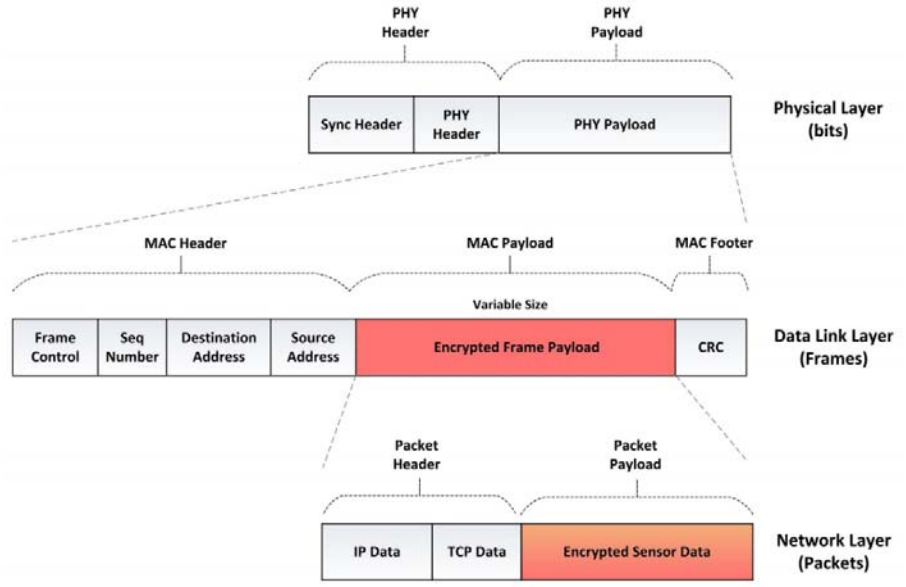


Рис. 1. Форматы передаваемых пакетов на физическом, канальном и сетевом уровнях

Безопасность на уровне шлюза Интернета вещей

Шлюзы интернета вещей – это вычислительные устройства с достаточным количеством ресурсов для запуска операционных систем и протоколов, необходимых для безопасной передачи трафика через Интернет, которые недоступны устройствам класса 0.

Объект JSON, полученный от устройства, не читается шлюзом или любой другой промежуточной сущностью, кроме предполагаемого назначения. Аналогично, если сервер отправляет команду обратно на устройство, объект данных шифруется с помощью предварительно разделенного симметричного ключа и пересылается на устройство для расшифровки. Безопасность применяется на канальном уровне передачи данных в виде аппаратного шифрования AES, защищенного с помощью PSK. Только авторизованные устройства должны находиться во владении PSK. Второй уровень безопасности применяется только к содержимому объекта данных. Объект данных шифруется с помощью симметричного ключа, который был совместно использован только с сервером, так, что никакие посредники не смогут расшифровать данные [3, 4].

Как только данные поступают в шлюз, они обрабатываются в HTTPS и подготавливаются для передачи на удаленный сервер.

Безопасность на уровне веб-сервера

Сообщения, передаваемые на сервер, шифруются открытым ключом сервера, который устанавливается в шлюзе. Закрытый ключ находится на сервере и не используется совместно с другими устройствами. Подробная блок-схема обеспечения безопасности со всеми последовательными процессами, которые сопоставляются с тремя компонентами системы Интернета вещей, показана на рис. 2.

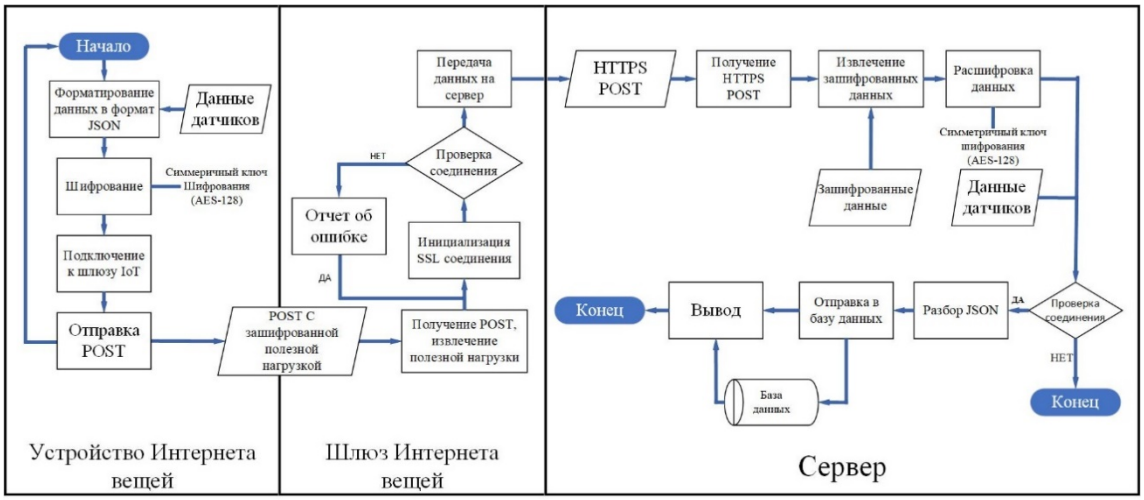


Рис. 2. Полная блок-схема обеспечения безопасности для всех компонентов IoT системы Интернета вещей

Как только HTTPS пакеты поступают на сервер, они расшифровываются с помощью закрытого ключа. Зашифрованный объект данных затем может быть расшифрован с помощью симметричного секретного ключа от исходного устройства, в данном случае IoT-устройства класса 0. Если ключ присутствует только на одном устройстве и сервере, его можно использовать для проверки подлинности данных, полученных от любой из сторон. Если ключ используется совместно с несколькими устройствами, они проходят проверку подлинности как часть группы. Этот сценарий сохраняет конфиденциальность данных всякий раз, когда они проходят через общедоступную сеть [5, 6].

Расширенный стандарт шифрования

Расширенный стандарт шифрования (AES) является одним из симметричных стандартов, который работает на высоких скоростях и требует меньше ресурсов, чем DTLS, что делает его очень подходящим для устройств класса 0. AES может быть легко реализован и оптимизирован на аппаратном обеспечении. AES вводит данные в виде 16-байтовых (128-битных) блоков, которые затем шифруются с помощью криптографического ключа размером 128 бит, 192 бита или 256 бит. Чем больше размер ключа,

тем выше требования к безопасности и ресурсам устройства для шифрования и дешифрования [3, 7]. Симметричное шифрование может применяться на различных уровнях стека связи, таких как уровень канала передачи данных (например, беспроводные передачи), и к конкретным объектам данных в сообщении, таким как показания датчиков.

Симметричная криптография предполагает шифрование данных с помощью одного ключа шифрования, который совместно используется несколькими устройствами. Любое устройство, обладающее этим ключом, может расшифровать данные, зашифрованные тем же ключом. Когда ключ используется совместно с другими устройствами, существует более высокий риск того, что он может попасть в чужие руки, и поэтому его необходимо хранить в безопасности.

Симметричный ключ является статическим и устанавливается только на устройстве интернета вещей и сервере. Таким образом, шлюз не в состоянии расшифровать полезную нагрузку пакета. Сообщения, передаваемые от шлюза на сервер, шифруются открытым ключом сервера, который устанавливается в шлюзе. Только сервер может расшифровывать сообщения, используя свой соответствующий закрытый ключ. Закрытый ключ находится на сервере и не используется совместно с каким-либо другим устройством. Асимметричный подход к криптографии ключей используется между шлюзом и сервером из-за множества вычислительных возможностей.

Оценка эффективности

Реализованная многоуровневая безопасность обеспечивает надежную защиту от любых внешних атак на систему Интернета вещей. Злоумышленник сначала должен получить доступ к сети либо через прямой доступ к шлюзу, либо с помощью PSK, чтобы сеть могла захватить данные. При дополнительном шифровании, применяемом к объектам данных, даже если злоумышленник имеет доступ к сети или шлюзу, он не сможет считывать данные без ключа шифрования.

На шлюзе данные обрабатываются в HTTPS с использованием RSA 2048-битного и сеансового ключа и надежно пересылаются на веб-сервер. Шифрование обеспечивает защиту от несанкционированных пользователей, перехватывающих трафик.

Выводы

В этом исследовании был рассмотрен распределенный механизм безопасности для ограниченных устройств Интернета вещей класса 0. Принцип проектирования, лежащий в основе решения, заключается в делегировании низкоресурсоемких операций устройству Интернета вещей и сохранении высокоресурсоемких процессов на стороне шлюза. В дополнение к собственной беспроводной безопасности, представлена многоуровневая схема

защиты путем выполнения асимметричного шифрования объектов данных на уровне устройства. Реализация механизма распределенной безопасности включает в себя устройство Интернета вещей, шлюз Интернета вещей и серверную часть.

Список используемых источников

1. Höller, J., Tsiatsis, V., Mulligan, C., Karnouskos, S., Avesand, S., Boyle, D. From Machine-to-Machine to the Internet of Things: Introduction to a New Age of Intelligence // Elsevier, 1st edn. (2014).

2. Дешевых Е. А., Конюхов В. М., Крылов К. Ю., Ушаков И. А. Исследование методов защиты от инсайдерских атак // Актуальные проблемы инфотелекоммуникаций в науке и образовании. IV Международная научно-техническая и научно-методическая конференция : сб. науч. ст. в 2-х т. СПб. : СПбГУТ, 2015. С. 310–313.

3. Котенко И. В., Левшун Д. С., Чечулин А. А., Ушаков И. А., Красов А. В. Комплексный подход к обеспечению безопасности киберфизических систем на основе микроконтроллеров // Вопросы кибербезопасности. 2018. № 3 (27). С. 29–38.

4. Алейников А. А., Билятдинов К. З., Красов А. В., Кривчун Е. А., Крысанов А. В. Технические аспекты управления с использованием сети интернет : монография. СПб : Астерон, 2016. 305 с. ISBN 978-5-00045-408.

5. Красов А. В., Левин М. В., Цветков А. Ю. Метод управления трафиком в гибридной программно-определяемой сети // Информационные технологии и телекоммуникации. 2016. Т. 4. № 2. С. 53–63.

6. Василишин Н. С., Ушаков И. А., Котенко И. В. Исследование алгоритмов анализа сетевого трафика с использованием технологий больших данных для обнаружения компьютерных атак // Аллея науки. 2018. Т. 3. № 6 (22). С. 1012–1021.

7. Коржик В. И., Яковлев В. А. Основы криптографии : учеб. пособие. СПб. : ИЦ Интермедия, 2016. 296 с. ISBN 978-5-89160-097-3.

УДК 004.056.5
ГРНТИ 81.93.29

ОБЕСПЕЧЕНИЕ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ ПРИ РАЗРАБОТКЕ WEB-ПРИЛОЖЕНИЙ

Е. Ю. Герлинг, С. Е. Горлов, Д. И. Кириллов

Санкт-Петербургский государственный университет телекоммуникаций им. проф. М. А. Бонч-Бруевича

Web-сервисы, которые предоставляются пользователям, охватывают большую сферу потребностей человека и по этой причине являются столь желанными для хакеров. При регистрации на таких сервисах, люди, вводя свои личные данные, могут не осознавать, что эта информация может попасть к злоумышленникам. Эксплуатация уязвимостей, таких как SQL- и PHP-инъекций и др., позволяет получить полный контроль над данными пользователей. Обеспечение защиты этой информации, а также защиты

самих web-приложений, является одной из основных задач, которая ставится в процессе разработки.

SQL-инъекции, атаки на web-приложения, хакинг, защита web-приложений.

Каждый день web-приложения подвергаются атакам. Взломанные сайты используются в различных целях – для распространения вредоносного ПО, кражи информации, размещения несанкционированной рекламы или запрещенной информации, мошенничества, проникновения во внутреннюю сеть компании [1, 2].

Чаще всего злоумышленники атакуют инфраструктуру и web-ресурсы компаний: это 49 и 26 % атак соответственно. Доля атак на банкоматы и POS-терминалы за год сократилась с 3 до 1 % (рис. 1) [2].

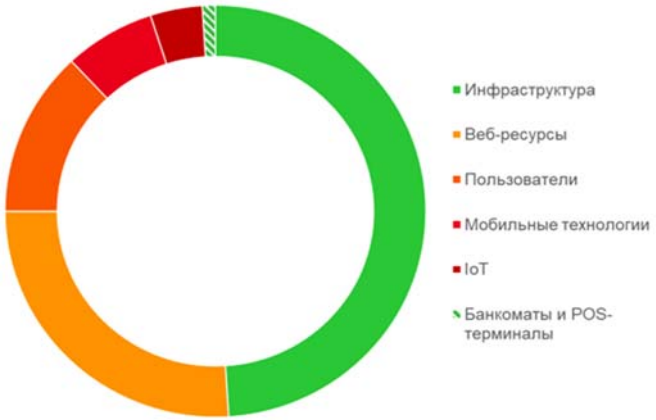


Рис. 7. Объекты атак

Тройка наиболее распространенных атак на web-сайты не меняется год от года: это «Внедрение SQL-кода» (*SQL Injection*), «Выход за пределы каталога» (*Path Traversal*) и «Межсайтовое выполнение сценариев» (*Cross-Site Scripting*, XSS) (рис. 2) [1].

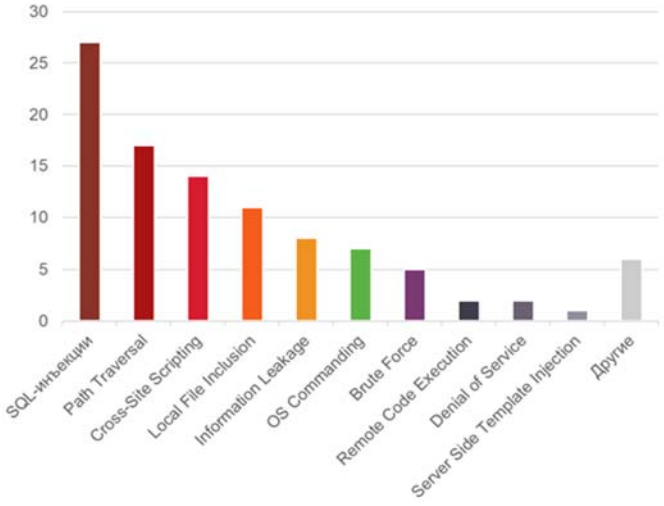


Рис. 8. Методы атак

Суммарно они составляют более половины всех выявляемых кибератак на web-ресурсы компаний. С одной стороны, это можно объяснить высокой эффективностью подобных атак. С другой стороны, подобные атаки просты в реализации и могут осуществляться низкоквалифицированными хакерами, в том числе, автоматизировано, с использованием общедоступного ПО [1].

Действия хакеров становятся все более хитроумными: атаки все чаще проходят в несколько этапов, в рамках которых применяются разные методы. Вредоносное ПО используется более чем в половине атак, возросла роль социальной инженерии: к ней хакеры прибегают в каждой третьей атаке (рис. 3) [2, 3].

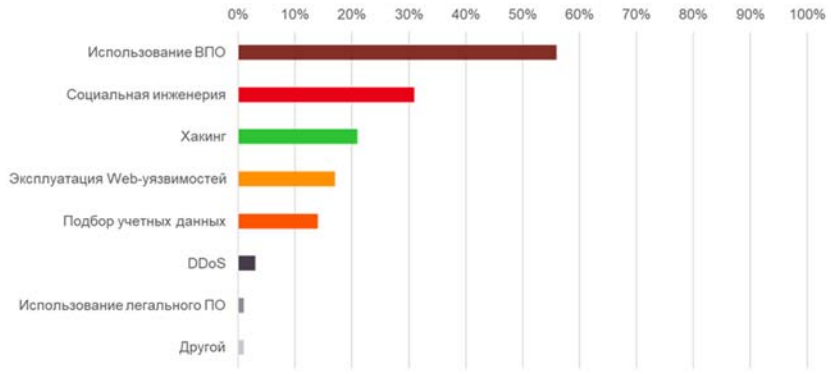


Рис. 9. Основные угрозы

Модель нарушителя представляет собой некие действия злоумышленников, которые способны реализовать угрозы информационной безопасности web-приложения. Под нарушителем рассматривается лицо или группа лиц. Всех нарушителей можно разделить на два типа [4]:

Внешние нарушители – лица, у которых нет прав доступа в контролируемую зону web-приложения, где размещается оборудование;

Внутренние нарушители – лица, у которых есть права доступа в контролируемую зону, на которой размещается оборудование web-приложения.

Возможности злоумышленника зависят от его должности и прав доступа к оборудованию.

Цель нарушителя – кража конфиденциальных данных, нарушение целостности web-приложения или остановка процессов web-приложения, что приводит его в неработоспособное состояние.

Члены Web Application Security Consortium унифицировали стандартную технологию описания угроз безопасности web-приложений [5]. Они разделил атаки на классы:

1. Атаки, направленные на аутентификацию – атаки, направленные на обход или эксплуатацию уязвимостей в механизмах реализации аутентификации web-серверов.

2. Атаки, направленные на авторизацию – атаки, благодаря которым злоумышленник может повысить свои привилегии и получить доступ к защищенным ресурсам.

3. Атаки, направленные на пользователей. Пользователь ожидает, что сайт предоставит ему легитимное содержимое. Злоумышленник, пользуясь этим доверием, может использовать различные методы для проведения атак на клиентов сервера.

4. Атаки, направленные на выполнение кода на web-сервере. Злоумышленник получает возможность модифицировать исполняемые команды в следствии низкой безопасности.

5. Атаки направлены на получение дополнительной информации о web-приложении. Используя эти уязвимости, злоумышленник может определить всю нужную ему информацию. Чем большими знаниями о приложении будет располагать злоумышленник, тем легче ему будет скомпрометировать систему.

6. Атаки направлены на эксплуатацию функций приложения или логики его функционирования. Злоумышленник может обойти или использовать эти механизмы в своих целях.

Чтобы убедиться, что web-приложение является безопасным, необходимо определить все проблемы безопасности и уязвимости в самом web-приложении, прежде чем их обнаружит нарушитель и сможет использовать [6]. Процесс обнаружения уязвимостей web-приложения нужно выполнять на протяжении всего жизненного цикла разработки программного обеспечения (SDLC), а не только в процессе эксплуатации. Тестирование на ранних стадиях разработки имеет первостепенное значение, поскольку в дальнейшем может быть очень сложно или вовсе невозможно обеспечить безопасность приложения, не переписав его [7]. Чем раньше безопасность web-приложения будет включена в проект, тем более безопасным будет web-приложение и тем дешевле и проще будет устранить выявленные проблемы на более позднем этапе [8].

Существует несколько технологий обнаружения уязвимостей в web-приложениях [9, 10]:

– автоматическое сканирование по принципу белого ящика (*white box*): предполагает тестирование с известной внутренней структурой работы программы;

– проверка исходного кода вручную: исходный код проверяется на наличие ошибок программистами;

– тест на проникновение (*penetration test*): используя программные средства, находятся уязвимости в программе;

– автоматическое сканирование по принципу черного ящика (*black box*): предполагает тестирование, при прохождении которого внутреннее устройство программы недоступно.

К средствам защиты web-сайтов можно отнести следующие [11, 12]:

– Web Application Firewall (WAF) – Imperva.

– Средства анализа web-сайтов на наличие вирусов – VirusTotal.

– Балансировщики нагрузки на web-приложения – Google Cloud Load Balancer.

– Средства защиты от DDoS – StormWall.

– Сканеры защищенности web-приложений (WASS) – Rapid7 Metasploit.

Атаки, совершаемые хакерами, очень эффективны и просты в исполнении. Их методы совершенствуются, меняются, поэтому важно обезопасить свое приложение. Используя указанные способы тестирования, а также приложения для защиты web-сайтов, будет обеспечиваться необходимая безопасность web-приложения.

Список используемых источников

1. Атаки на web-приложения: итоги 2018 года [Электронный ресурс]. URL: https://www.ptsecurity.com/ru-ru/research/analytics/web-application-attacks-2019 (дата обращения 25.03.2020).

2. Актуальные киберугрозы – 2018. Тренды и прогнозы [Электронный ресурс]. URL: https://www.ptsecurity.com/ru-ru/research/analytics/cybersecurity-threatscape-2018 (дата обращения 25.03.2020).

3. Ковцур М. М., Луеке П. Э. Разработка систем учета посещаемости студентов // Актуальные проблемы инфотелекоммуникаций в науке и образовании. VIII Международная научно-техническая и научно-методическая конференция : сб. науч. ст. в 4-х т. СПб. : СПбГУТ, 2019. С. 532–537.

4. Модель угроз и нарушителя безопасности персональных данных, обрабатываемых в специальных информационных системах персональных данных отрасли: отчет о НИР. Москва: 2010.

5. Классификация угроз безопасности Web-приложений [Электронный ресурс]. URL: http://www.infosecurity.ru/iprotect/websec/classification (дата обращения 27.03.2020).

6. Котенко И. В., Ушаков И. А Технологии Больших данных для мониторинга компьютерной безопасности // Защита информации. Инсайд. 2017. № 3 (75). С. 23–33.

7. Акимова А. И., Ковцур М. М. Разработка программного модуля защиты от ложных вызовов для IP-АТС ELASTIX // Актуальные проблемы инфотелекоммуникаций в науке и образовании. VII Международная научно-техническая и научно-методическая конференция : сб науч. ст. в 4-х т. СПб. : СПбГУТ, 2018. Т. 1. С. 33–37.

8. Shterenberg, S. I., Krasov, A. V., Ushakov, I.A. Analysis of using equivalent instructions at the hidden embedding of information into the executable files // (2015) Journal of Theoretical and Applied Information Technology, 80 (1), pp. 28–34.

9. Защита веб-приложений: мифы и реальность [Электронный ресурс]. URL: https://www.anti-malware.ru/analytics/Technology_Analysis/web-security-myths-and-reality (дата обращения 27.03.2020).

10. Израилов К. Е. Система критериев оценки способов поиска уязвимостей и метрика понятности представления программного кода // Информатизация и связь. 2017. № 3. С. 111–118.

11. Сахаров Д. В., Ковцур М. М., Бахтин Д. В. Модель защиты от эксплойтов и руткитов с последующим анализом и оценкой инцедентов // Наукоемкие технологии в космических исследованиях Земли. 2019. Т. 11. № 5. С. 22–31.

12. Десницкий В. А., Сахаров Д. В., Чечулин А. А., Ушаков И. А., Захарова Т. Е. Защита информации в центрах обработки данных : учебное пособие; Федеральное агентство связи. Санкт-Петербургский государственный университет телекоммуникаций им. М. А. Бонч-Бруевича. СПб. : СПбГУТ, 2019. 91 с.

УДК 4.056
ГРНТИ 81.93.29

К ВОПРОСАМ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ SS7 В СОВРЕМЕННОМ МИРЕ

М. Д. Глуховский, Д. В. Сахаров

Санкт-Петербургский государственный университет телекоммуникаций им. проф. М. А. Бонч-Бруевича

Система сигнализации № 7 – это нервная система телекоммуникационных сетей, основанная на технологиях 2G и 3G. Ранее SS7 была обособлена и защищена, теперь же стала более уязвима с переходом отрасли на технологию IP. Злоумышленники используют сетевые коммуникации для отслеживания абонентов, перехвата вызовов, отказа в обслуживании и для совершения мошеннических операций. В статье представлен обзор угроз и уязвимостей SS7.

SS7, SIGTRAN, протоколы сигнализации, телекоммуникационная безопасность, CN, MAP, SCTP.

Система сигнализации №7 (SS7) – это семейство протоколов сигнализации, первоначально использовавшихся в телефонной сети общего пользования (PSTN). Стандартизованный Сектором стандартизации электросвязи Международного союза электросвязи (МСЭ-Т, ITU-T) в 1988 году, она используется между элементами в PSTN для обмена информацией, в первую очередь, для настройки и разрыва телефонных звонков, но также используется для выставления счетов, службы коротких сообщений (SMS), маршрутизации и общего обмена информацией между элементами в GSM и базовой сети UMTS (CN).

С переходом отрасли на технологию IP SS7 претерпела изменения. SIGTRAN – это дополнение к протоколам SS7, разработанным Инженерной рабочей группой по Интернету Internet Engineering Task Force (IETF). SIGTRAN позволяет передавать SS7 по IP-сетям, заключая протоколы сигнализации в дополнительные уровни. SIGTRAN использует те же верхние

прикладные уровни, что и исходный стек SS7, но добавляет дополнительные функциональные возможности на нижних уровнях, что позволяет передавать части приложения по IP-сетям. Протокол управления потоком Stream Control Transmission Protocol (SCTP) используется, потому что он имеет несколько преимуществ по сравнению с более часто используемыми протоколами TCP и UDP для передачи сигналов по IP. Базовая функциональность SIGTRAN включает несколько узлов в сети, которые переводят пакеты в исходные протоколы SS7 и наоборот. Для передачи сигналов по IP SIGTRAN использует протоколы, такие как пользовательский уровень адаптации MTP3 MTP3 User Adaption Layer (M3UA) и пользовательский уровень адаптации MTP2 MTP2 User Adaption Layer (M2UA), для надежной передачи сигналов в сетях IP с использованием SCTP [1].

Для определения угроз необходимым является рассмотреть архитектуру сети мобильной связи. В сетях мобильной связи GSM и UMTS (2G и 3G соответственно) базовая сеть Core Network (CN) предоставляет функциональные возможности и услуги, необходимые для обслуживания мобильных абонентов, подключенных к сети (рис.). В CN есть несколько сетевых элементов, имеющих решающее значение для его работы. При роуминге в сети мобильная станция Mobile Station (MS) будет подключена к подсистеме базовой станции Base Station Subsystem (BSS), содержащей базовую приемопередающую станцию Base Transceiver Station (BTS) и совмещенный контроллер базовой станции Base Station Controller (BSC). BSS обрабатывает соединение с и от MS и дополнительно отправляет, и принимает информацию к CN. Различные элементы в CN выполняют разные задачи по предоставлению услуг абонентам. Данная структура существовала долгое время без применения технологии IP.

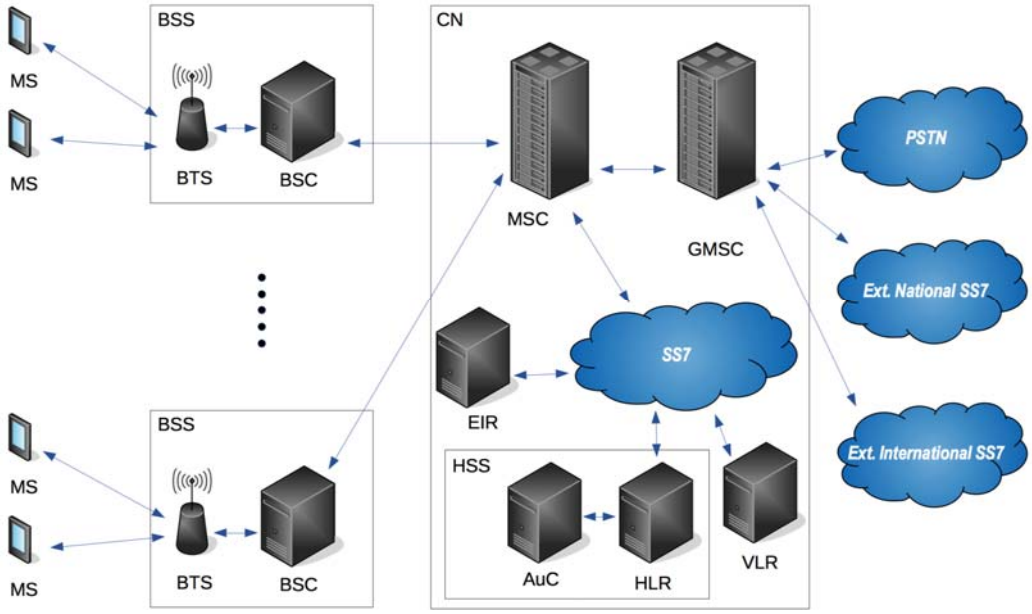


Рис. 1. Схема Core Network SS7

После внедрения технологии IP и расширения тем самым возможностей SS7, а также осуществления либерализации рынка SS7 стала более уязвима, чем когда-либо [2, 3, 4, 5]. SS7 непосредственно влияет на безопасность и конфиденциальность абонентов, подключенных к мобильным сетям, а также на честность операторов, желающих предоставлять своим абонентам лучший сервис. Было обнаружено несколько атак, позволяющих использовать уязвимости сетей SS7. Все эти атаки основаны на одних и тех же условиях:

1. Все сообщения в сети являются легальными.
2. Не требуется сложное оборудование.
3. Эскалация атак возможна с помощью простых шагов.

Одной из более серьезных проблем безопасности сети SS7 является увеличение площади атаки. Сети ранее полагались на обособленность, а это означает, что всем взаимосвязанным операторам доверяли – это уже не так. Сейчас есть множество операторов, имеющих доступ к SS7. Потенциально, с помощью некрупных операторов, могут производится атаки.

В основном используют протокол SS7 MAP для получения промежуточной информации и выполнения атак [6, 7]. Атаки могут включать возможное отслеживание мобильных пользователей вплоть до региона или до уровня домов и улиц, отказ в обслуживании, перехват вызовов и SMS, и мошенничество, чтобы избежать выставления счетов и получения финансовых выгод. Сообщения отправляются соответствующим элементам CN для успешного выполнения атак. Чтобы использовать выявленные уязвимости SS7, злоумышленник должен обладать определенными возможностями, а именно:

1. Каким-либо образом подключаться к сети SS7.
2. Иметь возможность генерировать произвольные сообщения SS7 по желанию.
3. Иметь возможность имитировать узел в сети SS7, предоставляя возможности SS7.

Возможно, одной из наиболее важных способностей атакующего является получение доступа к закрытым сетям SS7. Существуют несколько подходов, которые злоумышленник может использовать для подключения к сети SS7. Тем не менее, SS7 не является общедоступной сетью, и она жестко контролируется мировыми операторами связи. В целом, с точки зрения того, как SS7 развивалась за эти годы, увеличилось количество операторов и услуг, которые они предоставляют с использованием данного набора сигнальных протоколов. Это, в свою очередь, увеличило нагрузку на безопасность, так как количество узлов, подключенных к SS7, увеличилось.

Оказавшись внутри CN, злоумышленник должен иметь возможность сопоставить инфраструктуру, чтобы иметь возможность успешно начинать

атаки. Существуют несколько подходов, которые могут быть использованы злоумышленником для получения обзора сети и связанных с ней элементов. Используя стек протоколов SIGTRAN, в котором используется протокол SCTP, злоумышленник может использовать несколько доступных инструментов и методов для получения информации, необходимой на этапе подготовки атак [8].

Чтобы помочь операторам справиться с некоторыми из уязвимостей SS7, сообщения MAP, используемые во всех раскрытых атаках SS7, могут быть классифицированы на основе их потребности во внешних сетях. Эта классификация выполняется в трех классах с помощью сообщений, и имеет следующий вид:

1. Нет необходимости во внешнем воздействии.

2. Нет необходимости подвергаться внешнему воздействию для собственных абонентов оператора, но могут приниматься для абонентов роуминга другого оператора.

3. Легальная необходимость внешнего воздействия.

Злоумышленник получает данные карты CN путем:

– сканирования на открытые порты;

– создания произвольных пакетов SCTP.

Типы атак на SS7:

1. Перехват.

2. Перехват звонков путем расшифровки радио трафика.

3. Перехват исходящих звонков.

4. Перехват входящих звонков.

5. Перехват sms.

6. Мошенничество.

7. Перевод средств с использованием USSD.

8. Переадресация звонков на премиум номера.

9. Разблокировать украденные устройства.

10. Отказ в обслуживании (изменение данных абонента).

11. Отслеживание местоположения.

Есть несколько методов, которые были рекомендованы для уменьшения уязвимостей SS7 [9]. Эти методы не предназначены специально для прекращения атак, но они обеспечивают еще один уровень безопасности. Это лучшие рекомендации, которые затрудняют атакующему раскрытые атаки, но не препятствуют им. По сути, рекомендуемые подходы сводятся к мониторингу и пониманию сетевого трафика SS7. Операторам рекомендуется анализировать сетевые ссылки SS7 на предмет подозрительного поведения. На основании классификации сообщений, используемых в атаках SS7, существует несколько вариантов того, как можно работать с категорированными сообщениями.

Сообщения категории 1 могут быть отфильтрованы относительно простыми методами на границе сети. Это можно сделать, посмотрев тип сообщения и оценив, было ли сообщение отправлено из внешней сети SS7. Сообщения категории 2 не могут быть просто отфильтрованы на границе сети. Оператор должен сопоставить состояния абонента и проверить, находится ли абонент в роуминге в сети оператора, прежде чем потенциальное сообщение может быть заблокировано. К сожалению, это не защищает абонентов роуминга. Для обнаружения атак с использованием сообщений категории 3 необходимо использовать более сложные подходы [10]. Это сообщения, которые имеют легальное использование в сети и не могут быть просто отфильтрованы. Система защиты должна анализировать поток сетевых сообщений и иметь возможность искать изменения в поведении сетевых элементов и абонентов. Например, просматривая предыдущее местоположение абонента.

Список используемых источников

1. Dryburgh, L. & Hewett, J. Signaling System No. 7 (SS7/C7): Protocol, Architecture, and Services. M. : Cisco Press, 2004. 744 p.

2. Langlois P. Getting in the SS7 kingdom: hard technology and disturbingly easy hacks to get entry points in the walled garden: материал конференции Hackito Ergo Sum, Париж, 8–10 april. 2010. M. : P1 Security, 2010. PP. 1–44. [Online]. URL: http://www.hackitoergosum.org/2010/HES2010-planglois-Attacking-SS7.pdf.

3. Hemant Sengar; Ram Dantu; Duminda Wijesekera; Sushil Jajodia. SS7 over IP: Signaling interworking vulnerabilities // IEEE Network. IEEE, 2006. V. 20. Iss. 6. PP. 32–41.

4. T. Moore; T. Kosloff; J. Keller; G. Manes; S. Shenoi. Signaling system 7 (SS7) network security // The 45th Midwest Symposium on Circuits and Systems (MWSCAS), Талса, 4-7 августа. 2002 г. М.: IEEE, 2003. PP. 32–41.

5. Siddharth Prakash Rao; Silke Holtmanns; Ian Oliver; Tuomas Aura. Unblocking Stolen Mobile Devices Using SS7-MAP Vulnerabilities: Exploiting the Relationship between IMEI and IMSI for EIR Access // 2015 IEEE Trustcom/BigDataSE/ISPA, Хельсинки, 20–22 августа. 2015 г. М.: IEEE, 2015. PP. 1171–1176.

6. ETSI TS 129 002 V10.2.0. 3GPP TS 29.002, Mobile Application Part (MAP) specification (3GPP TS 29.002 version 10.2.0 Release 10). M.: 3GPP, 2011. 954 p.

7. Гойхман В. Ю., Гольдштейн Б. С., Сибирякова Н. Г. Протоколы стека ОКС7: подсистема МАР. Серия «Телекоммуникационные протоколы». Книга 10. СПб. : БХВ-Петербург, 2014. 200 с.: ил.

8. Костырин А. С., Красов А. В. Реализация метода канальной стеганографии с использованием протокола ICMP // Межвуз. сб. науч. тр. региональная информатика и информационная безопасность: Изд-во Санкт-Петербургское общество информатики, вычислительной техники, систем связи и управления, 2017. Вып. 3. С. 312–316.

9. Hank M. Kluepfel. Securing a global village and its resources: baseline security for interconnected signaling system #7 telecommunications networks // 1993 Proceedings of IEEE International Carnahan Conference on Security Technology, Оттава, 13–15 октября. 1993 г. М.: IEEE, 2002. С. 195–212.

10. Гольдштейн Б. С., Гончарок М. Х., Крюков Ю. С. Системный подход к реализации информационной безопасности узлов коммутации // Электросвязь. 2003. № 4. С. 28–32.

УДК 004.056
ГРНТИ 81.93.29

ОБЕСПЕЧЕНИЕ ЗАЩИТЫ ИНФОРМАЦИИ В ПРОЦЕССЕ ИСПОЛЬЗОВАНИЯ ОБЪЕКТОВ АВТОРСКОГО ПРАВА

Ю. А. Головлёва, А. И. Пешков

Санкт-Петербургский государственный университет телекоммуникаций им. проф. М. А. Бонч-Бруевича

В данной статье рассматриваются понятия интеллектуальной собственности и авторского права, вопросы защиты объектов авторского права в современном информационном пространстве, киберугрозы информационной безопасности в отношении объектов прав интеллектуальной собственности, а также технические средства защиты авторских прав и их недостатки.

авторское право, защита информации, защита объектов авторского права.

В нынешних условиях информационного общества и проникновения информационных технологий во многие сферы жизни людей важное значение имеет соблюдение интеллектуального права, которое связано с сохранением секретной и конфиденциальной информации, защитой служебной тайны и соблюдением корпоративных интересов, а также соблюдением авторских прав личности на результаты собственного творческого труда. В настоящий период защита интеллектуальных прав по-прежнему остается актуальной задачей из-за непродолжительного периода существования правового института интеллектуальной собственности, а также интенсивным развитием науки и технологий.

В тоже время институт права интеллектуальной собственности получил достаточно широкое распространение в современном мире. Он закреплен нормами как внутригосударственными нормативно-правовыми актами, так и нормами международного права. Значение интеллектуальной собственности особенно подчеркивается тем, что в конституциях многих государств не оставили без внимания эту существенную область человеческих отношений. Общественное признание интеллектуальной собственности и необходимости ее защиты явилось актом крупного конституционного, научного и практического значения [1].

Мировой тенденцией современности также являются многочисленные угрозы информационной безопасности. Понятия информационный терроризм, информационная война, информационное пиратство, промышленный шпионаж уже прочно закреплены в нынешней новостной повестке дня.

Нарушение исключительных прав на результаты интеллектуальной деятельности, недобросовестная конкуренция являются продолжением этого ряда угроз.

По этой причине актуальность изучения путей решения вопроса обеспечения информационной безопасности в отношении объектов авторского права является крайне высокой.

Киберугрозы нарушения прав интеллектуальной собственности в сфере цифрового пространства Интернет имеют свою специфику.

Достаточно показательным является тот факт, что технологии, которые сделали возможной информационно-цифровую революцию, сами стали представлять значительные угрозы, в том числе для защиты авторских прав. Новейшие достижения в области технологии, повышение мобильности, глобализация и анонимная природа сети Интернет создают растущие проблемы в области защиты авторских прав [2].

Задачи повышения эффективности защиты авторских прав от новых киберугроз связаны с расширением разнообразия самих объектов авторских прав. Цифровые технологии, несомненно, упрощают «пиратство» и затрудняют использование традиционных способов защиты авторского права и смежных прав. Проблемы защиты авторского права влекут за собой необходимость совершенствования механизма защиты в киберпространстве.

К техническим средствам защиты авторских прав (далее – ТСЗАП) относят любые технические устройства или их компоненты, а также технологии, аппаратные или программные средства, контролирующие доступ к произведению, ограничивающие либо предотвращающие действия, направленные на нарушение авторских прав в отношении произведения. Законодательством РФ не допускается устранение ограничений ТСЗАП, а также средств, направленных на устранение ограничений ТСЗАП, что закреплено в ст.1299 ГК РФ [3].

В России доказательством правомерности использования произведения, защищаемого авторским правом, является лицензионный договор. Лицензионным при этом является не само произведение, а использование его копии.

Тем не менее существующие, широко используемые ТСЗАП не могут однозначно отличить нелицензионное копирование от лицензионного. Поэтому ТСЗАП блокируют любое копирование, разрешая лишь то, которое расценено как лицензионное по некой подтверждающей информации, например, по предположительному наличию лицензионного диска в дисководе.

Однако подтверждающая информация от устройства воспроизведения также может быть скопирована вовне и распространена другим пользователям.

Пока не преодолённое противоречие заключается в том, что ТСЗАП должны одновременно и передать оконечному устройству некий «ключ», чтобы дать возможность лицензионного использования, и передачу, чтобы не дать возможность неправомерного копирования.

ТСЗАП обеспечивает не криптография как таковая, а способ изоляции ключа. Поэтому ТСЗАП будут эффективно работать только при повсеместном исключительном использовании закрытых информационных систем, то есть с закрытым доступом к внутренней служебной информации. Однако невозможно создать абсолютно закрытую информационную систему и полностью контролировать производство и эксплуатацию аппаратных и программных средств.

Более того, фактическая распространённость огромного числа аппаратных и программных средств, а также средств поиска и обмена информацией свидетельствует о проблемах с эффективностью данного способа защиты авторских прав популярных произведений. Отдельные уникальные и условно криптостойкие ко взлому ТСЗАП будут эффективной защитой от копирования лишь до того момента, пока они или произведения не станут популярными и не будут вскрыты энтузиастами.

В отношении аудио, видео контента и ряда иных произведений действует дополнительный фактор, существенно снижающий эффективность ТСЗАП, так как информация, составляющая произведение, должна быть передана пользователю-лицензиату в аналоговом виде [4].

Исходя из того, что она доступна для восприятия органами чувств человека, то значит и может быть скопирована, записана без ТСЗАП и свободно распространена. В некоторых случаях нелегальность копии будет подтверждена с помощью стеганографической технологии «цифровых водяных знаков». Тем не менее, цифровой водяной знак, будучи обнаружен, всегда может быть извлечён без существенного влияния на защищаемое произведение.

ТСЗАП развиваются по пути усиления защиты. Однако практика показывает, что усиление и развитие защитных характеристик ТСЗАП затрудняет использование преимущественно легальным пользователям, нелегальные же используют готовые варианты взлома и зачастую не испытывают достаточно серьёзных затруднений.

Исходя из сформулированных рисков и угроз, а также возможных их решений имеющимися современными техническими средствами можно предположить, что необходимо создание информационной системы, способной относительно просто, автоматически, но при этом надёжно регистрировать факт авторского права.

Целью информационной системы является эффективное обеспечение защиты объектов авторских прав в процессе их использования в ответ на современные угрозы информационной безопасности.

Список используемых источников

1. Сидорова В. И. Интеллектуальная собственность: основные термины и понятия // Динамика систем, механизмов и машин. 2014. № 5. С. 229.

2. Гайсин Ф. Ф. Проблема защиты авторских прав // Вестник Марийского государственного университета. Серия «Исторические науки. Юридические науки». 2017. Т. 3. С. 74.

3. Гражданский кодекс Российской Федерации часть 4. Принят Государственной Думой 24 ноября 2006 года. Одобрен Советом Федерации 8 декабря 2006 года.

4. Курамагомедов Р. Ш. Основные сферы применения технических средств защиты авторских и смежных прав // Системные технологии. 2014. № 10. С. 2–4.

УДК 004.415.538
ГРНТИ 50.01.81

ИСПОЛЬЗОВАНИЕ РЕЗУЛЬТАТОВ ФУНКЦИОНАЛЬНЫХ АВТОТЕСТОВ ДЛЯ АНАЛИЗА ПРОИЗВОДИТЕЛЬНОСТИ ПРИЛОЖЕНИЯ

А. Б. Гольдштейн, Д. А. Терентьев

Санкт-Петербургский государственный университет телекоммуникаций им. проф. М. А. Бонч-Бруевича

С целью ускорения процесса верификации и построения инфраструктуры для разработки ПО, основанной на практике непрерывной интеграции, пишется большое количество функциональных автотестов. В статье предлагается использовать данные, собранные дополнительно при их прохождении для анализа производительности разрабатываемого приложения. Это позволит намного быстрее организовать мониторинг производительности программы без дополнительных затрат на написание специальных тестов. Приведен пример использования этой идеи на практике для решения реальной инженерной задачи. Он демонстрирует перспективность дальнейшего анализа способов математической обработки данных производительности, полученных таким способом. В этом докладе будут рассмотрены основные аспекты применения такого подхода, проблемы и возможные способы их решения.

QA, performance testing, анализ результатов прохождения тестов.

Крайне важно, чтобы ПО работало быстро. Это может стать одним из факторов, выделяющих продукт на рынке. Поэтому необходимо уделять время тестированию производительности программного обеспечения, в том числе проверке скорости его работы. Написание «специальных» тестов для данной цели эффективно, но очень трудозатратно и является непростой инженерной задачей. Вместе с этим для любого проекта разрабатывается большое количество функциональных автоматических тестов. Почему

бы не использовать их? Для этого придется решить ряд задач, которые позволят сразу получить большое количество данных производительности приложения:

1. Выбрать метрики, характеризующие производительность приложения, которые будут собираться при прохождении функциональных тестов (время прохождения тестов, количество сборок мусора GC, загрузка CPU).

2. Выбрать математические методы для борьбы с хаотичными внешними воздействиями и шумами, позволяющие сократить погрешность.

3. Выбрать математические методы анализа собранных данных (в том числе автоматического) для вынесения решения о результате теста производительности.

Применим ли этот подход на практике. Необходимо решить задачу обоснования необходимости перехода, тестируемого web-приложения с контейнера сервлетов Apache Tomcat 6 на Apache Tomcat 8. Таким образом, целью исследования становится сравнение быстродействия приложения в двух этих конфигурациях окружения.

Для организации процесса непрерывной интеграции, как практики разработки ПО, для данного приложения разрабатывается проект автоматических тестов UI. Они реализуются с использованием Java, Selenium (в качестве инструмента автоматизированного управления браузерами) и Selenoid, который является реализацией Selenium hub с использованием Docker (программное обеспечение для автоматизации развёртывания и управления приложениями в средах с поддержкой контейнеризации) для запуска браузеров. Упрощенно тестовый стенд можно представить в виде схемы (рис. 1).

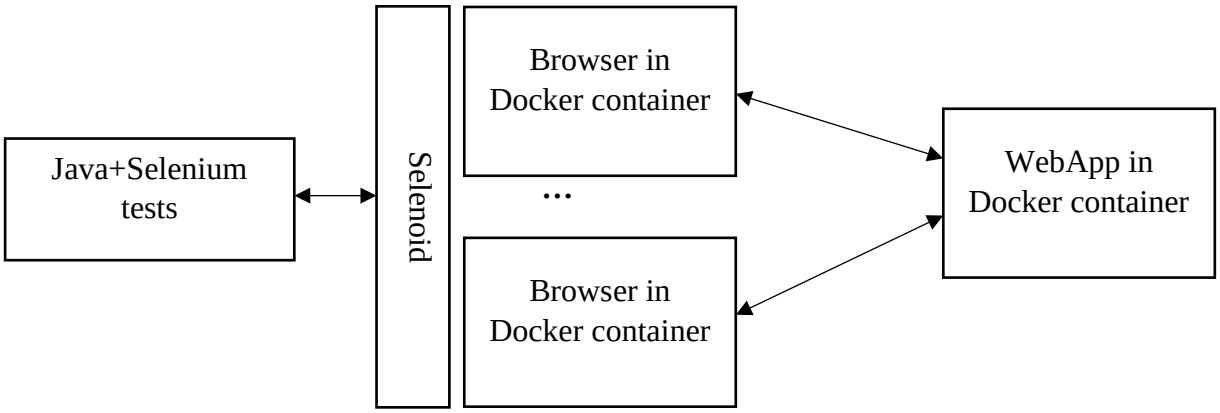


Рис. 1. Схема стенда для автоматического функционального тестирования

Для создания нагрузки используются уже разработанные тесты. Из них был сформирован один, осуществляющий переход по ряду страниц приложения. Для оценки времени загрузки страницы в тест включены методы ожидания появления элементов страницы в DOM (*Document Object Model*).

В качестве метрики, характеризующей производительность, выбрано время прохождения теста. Обработка данных осуществляется простыми методами математической статистики.

Исходя из цели исследования, необходимо убедиться в том, что скорость работы приложения на одной из версий Tomcat больше другой с учетом погрешности при прочих равных условиях. Для этого необходимо обеспечить равное воздействие внешних факторов на тестируемое приложение и тестовое окружение, с помощью которого это тестирование проводилось [1]. Следует убедиться, что причиной полученного результата сравнения двух конфигураций приложения не является погрешность и попытаться определить ее источник, и уменьшить ее. Данным этапом не стоит пренебрегать при тестировании производительности.

Тесты и приложение в контейнере запускаются на выделенной машине. Это позволяет легко обеспечить отсутствие дополнительных воздействий, затрачивающих вычислительные мощности, таких как запуск сторонних программ. Основным источником погрешности будет использование Selenoid для запуска браузеров в контейнерах, в которых и будет проводится тестирование. Данный инструмент запущен на отдельном сервере, используемом и для других задач. Поэтому в процессе проведения измерений могут наблюдаться значительные временные падения производительности. Равномерность влияния этого внешнего фактора обеспечивается проведением измерений примерно в одно время, чередуя версии Tomcat. Это позволит снизить вероятность такого воздействия только на одну исследуемую версию. Таким образом, получены 3 серии экспериментов для каждой версии контейнера сервлетов.

Также для сбора большего количества статистики, необходимой в том числе для учета погрешности и уменьшения ее влияния, проведено тестирование одновременно в 4 потока по 19 тестам. Каждый поток рассматривается как отдельный эксперимент. Таким образом, каждая серия состоит из 4 экспериментов, проводимых параллельно.

Для обработки отчетов Robot Framework, использованного при написании тестов, применен инструмент статистического анализа, разработанного для этой цели и являющегося прототипом системы ретроспективного анализа результатов прохождения автоматических тестов.

Сначала оценивается общее среднее время прохождения теста. После сортировки по возрастанию среднего времени прохождения тестов формируется таблица (табл.) для Tomcat8 и Tomcat6.

ТАБЛИЦА. Сравнение времени прохождения тестов при использовании разных контейнеров сервлетов

Контейнер сервлетов	Tomcat8	Tomcat8	Tomcat6	Tomcat8	Tomcat8	Tomcat6	Tomcat6	Tomcat6
$\overline{T}$, с	15,9389	16,0303	16,2624	16,3310	16,3559	16,4212	16,5592	16,6378

Далее необходимо проверить плотность распределения вероятности для того, чтобы исключить наличие статистических аномалий (например, двух максимумов функции плотности распределения вероятности) и убедиться в возможности использования среднего значения в качестве метрики для сравнения. Для всех экспериментов плотность распределения близка к экспоненциальному закону и является унимодальной [1]. Поэтому использование среднего значения вполне оправдано. Приведены примеры гистограммы времени прохождения тестов одного из экспериментов (рис. 2) и диаграммы времени прохождения тестов (рис. 3). Все графики получены с помощью вышеупомянутого инструмента.

Следующим шагом необходимо оценить погрешность и выяснить ее основной источник. Для этого требуется проанализировать временные характеристики keywords – отдельных подпрограмм, из которых состоят тесты при использовании Robot Framework.

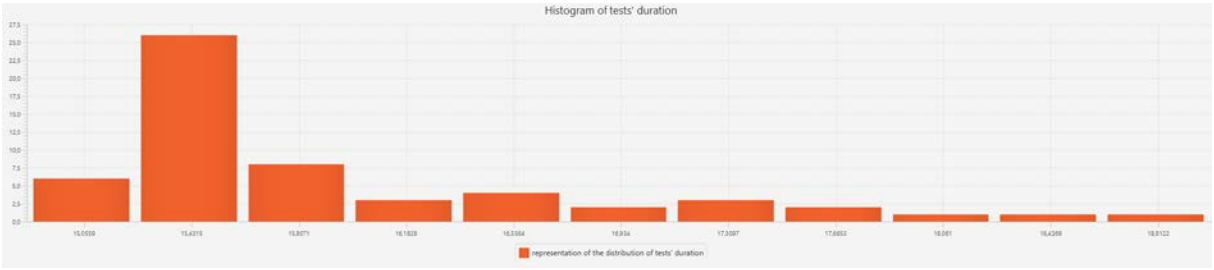


Рис. 2. Гистограмма времени прохождения тестов для 1-го эксперимента (Tomcat8, $t_{ср}$ = 15,9389)

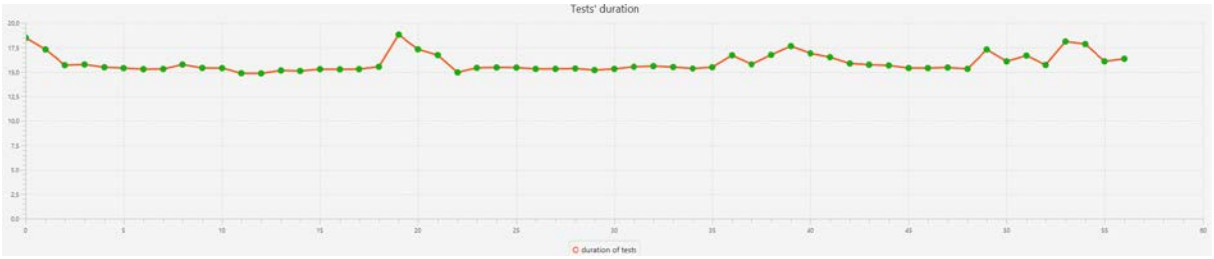


Рис. 3. Диаграмма времени прохождения тестов для 1-го эксперимента (Tomcat8, $t_{ср}$ = 15,9389)

Как и предполагалось ранее, наибольшей дисперсией обладает время запуска браузера в контейнере с помощью Selenoid для прохождения тестов,

т. к. сервер, на котором он расположен используется для ряда других задач (рис. 4).

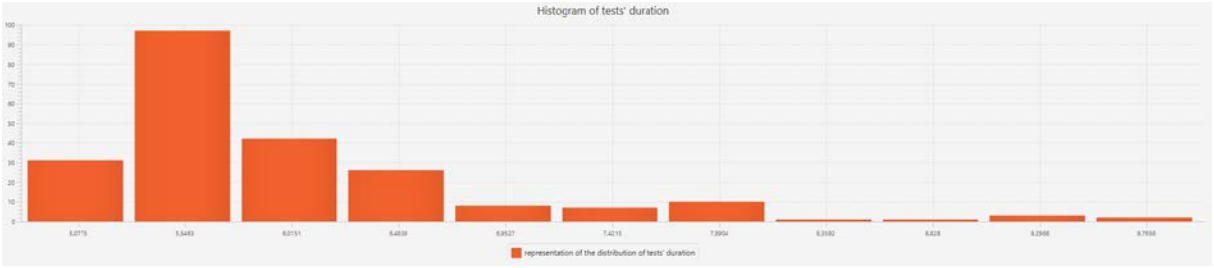


Рис. 4. Гистограмма времени запуска контейнера с браузером

Дисперсия для времени прохождения этого процесса составила 0,9517.

Далее будет продолжено рассмотрение непосредственно keyword – Load, отвечающего за нагрузку на исследуемое приложение. Это позволит исключить основной источник погрешности. Дисперсия Load составила 0,101 для Tomcat 6 и 0,281 для Tomcat 8.

При использовании Tomcat 6 тесты идут лишь на 0,1 с дольше, как видно по гистограмме времени прохождения Load (рис. 5, 6).

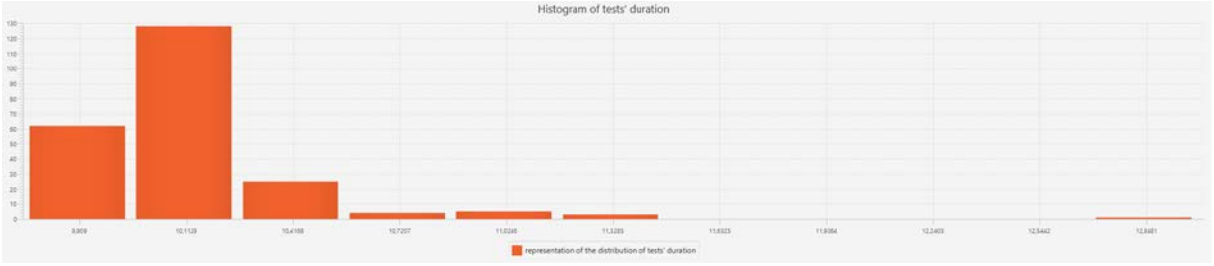


Рис. 5. Гистограмма времени прохождения keyword – Load Tomcat 6

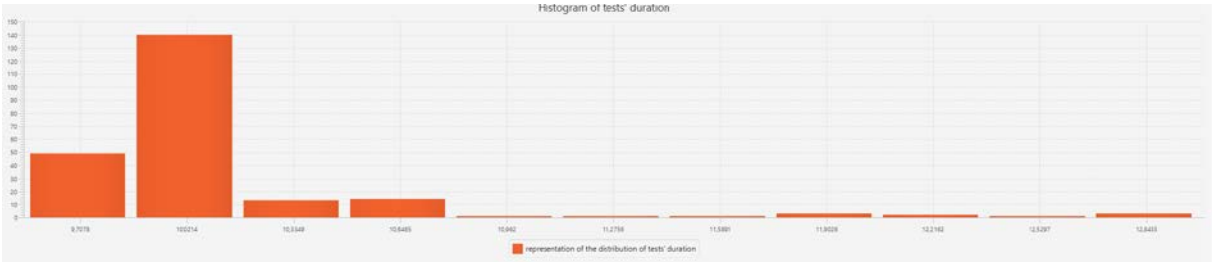


Рис. 6. Гистограмма времени прохождения keyword – Load Tomcat8

Доверительный интервал реального среднего значения для обоих наборов данных может быть рассчитан по формуле:

$$\left[\bar{x} - t\frac{s}{\sqrt{n}}; \bar{x} + t\frac{s}{\sqrt{n}}\right],$$

где s – среднеквадратичное отклонение от среднего значения, n – количество экспериментов (в нашем случае 228), t – критическое значение доверительного интервала (1,282 при точности 80 %). Таким образом, получены два интервала [9,971; 10,071] – Tomcat8, [10,092; 10,132] – Tomcat6.

Учитывая одинаковую форму функций распределения вероятности и отсутствие пересечений доверительных интервалов средних значений времени прохождения тестов, можно сделать выбор в пользу Tomcat8 без применения дополнительных методов сравнения функций плотности распределения вероятности.

Таким образом, данное применение на практике идей использования функциональных тестов для проведения performance тестирования показало эффективность такого подхода, а именно: позволило сократить время подготовки исследования, дало интерпретируемые результаты, подтверждающие ожидания. Дальнейшее исследование будет направлено на внедрение более сложного математического аппарата для получения большей информации из уже имеющейся тестовой инфраструктуры для борьбы с хаотичным внешним воздействием и для сравнения функций плотности распределения вероятности анализируемых процессов.

Список используемых источников

1. Andrey Akinshin, Pro .NET Benchmarking: Apress, 2019. P. 197–202.

УДК 004.722
ГРНТИ 49.33.29

О ВИРТУАЛЬНЫХ ОПЕРАТОРАХ MVNO НА СОВРЕМЕННОМ ЭТАПЕ

Б. С. Гольдштейн, С. М. Елисеев

Санкт-Петербургский государственный университет телекоммуникаций им. проф. М. А. Бонч-Бруевича

MVNO является одним из современных трендов на насыщенном телекоммуникационном рынке с высокой конкуренцией. Доля MVNO в российском сегменте телекоммуникационных услуг составляет порядка 4 %. Клиентская база виртуальных операторов России растет опережающими темпами: по итогам 2019 года зафиксировано ее увеличение на 40 %, в то время как прирост абонентской базы всего мобильного рынка составляет менее 1 %.

MVNO, MNO, MVNE, MVNA, DCN, Private LTE.

Концепция виртуального оператора

MVNO (*Mobile Virtual Network Operator*) – виртуальные мобильные операторы, использующие радиосеть и другие элементы инфраструктуры традиционных мобильных операторов (*Mobile Network Operator*, MNO) и продающие услуги под собственным брендом. В партнерстве с операторами сотовой связи MVNO создают банки, ритейлеры, транспортные компании, промышленные предприятия, социальные сети.

Сетевая архитектура традиционного мобильного оператора состоит из трех уровней:

– Сеть радиодоступа.

– Ядро голосовой и пакетной сетей.

– Подсистема бизнес-приложений OSS/BSS (управление качеством услуг, технический учет, биллинг и т. д.).

Наиболее дорогостоящей частью операторской инфраструктуры является сеть радиодоступа. Виртуальный оператор арендует готовую радиосеть у действующего MNO [1].

Интерес сотрудничества традиционного мобильного оператора с MVNO определяется следующими факторами [2]:

- Увеличение проникновения в конкретные сегменты рынка.
- Повышение лояльности абонентов.
- Уменьшение затрат на привлечение и обслуживание клиентов.
- Получение дополнительного дохода от аренды инфраструктуры.

В свою очередь, виртуальный оператор владеет конкурентными преимуществами на рынке телекоммуникационных услуг:

- Уникальные и выгодные предложения, например, бесплатную мобильную связь для владельцев определенных категорий банковских карт.
- Более удобное и гибкое использование услуг для абонентов.
- Экономия на сервисах информирования (SMS, *e-mail*).
- Возможность собирать больше информации о клиентах с целью дальнейшей обработки и монетизации.
- Дополнительные программы лояльности.

Модели MVNO

Модель MVNO определяет характер деятельности виртуального оператора, оказывает значительное влияние на спектр его возможностей, формирует капитальные затраты, риски и потенциальную прибыль.

На сегодняшний день определены следующие типы виртуальных операторов связи (рис. 1):

- Branded reseller. MVNO, осуществляющий продажу и маркетинг услуг базового оператора под собственным брендом. Вся сетевая инфраструктура арендуется у MNO целиком. Операторы в рамках данной модели

не имеют возможности регулировать ценовую политику. Все подключаемые абоненты фактически принадлежат базовому оператору.

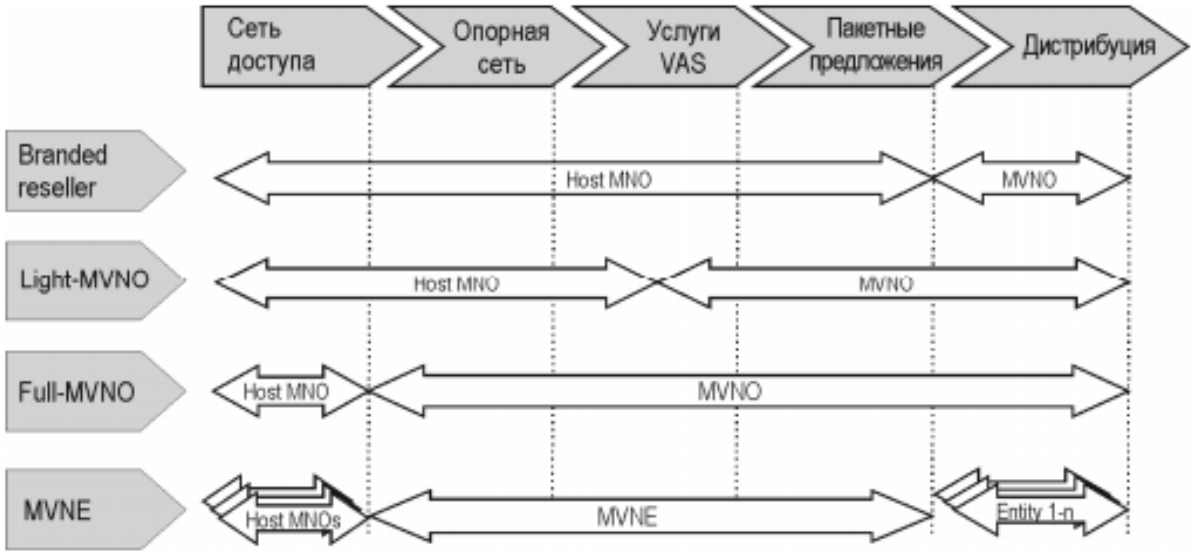


Рис. 1. Модели MVNO [1]

– Light-MVNO. Модель, при которой сетевая инфраструктура также арендуется у MNO, однако есть возможность управлять бизнес-приложениями. Это позволяет регулировать тарифы, биллинг и другие сервисы [2].

– Full-MVNO. Операторы данной модели обладают своим ядром сети и бизнес-приложениями. Арендуется только радиодоступ. При таком режиме работы MVNO не ограничен тарифами базового оператора.

– MVNE. Создание и поддержка собственной инфраструктуры для виртуального оператора является сложной технической задачей. Для решения этой задачи существуют посредники между MVNO и базовым оператором – MVNE (*Mobile Virtual Network Enabler*), которые предоставляют готовые технические решения, помогают сократить время и расходы на внедрение и эксплуатацию MVNO, позволяют ему сконцентрироваться только на продажах и маркетинге.

– Агрегатор MVNA. Модель, позволяющая агрегировать несколько небольших операторов MVNO и взаимодействовать с MNO как единый крупный виртуальный оператор. Таким образом, MVNA (*Mobile Virtual Network Aggregator*) поддерживает целые группы виртуальных операторов, производит подключение их всех к базовому оператору, избавляет от непрофильных задач.

– Концепция DCN. В Rel’13 3GPP введена концепция выделенного ядра сети сотовой связи DCN (*Dedicated Core Network*) для сетей 4G, где уже начали обращать внимание на принципиальные различия в ресурсах, необходимых для обработки разнородных типов трафика. Рост количе-

ства и популярности устройств M2M означает резкое увеличение количества и разнообразия терминалов, зарегистрированных в сети. При этом характеристики трафика, генерируемого этими устройствами, могут кардинальным образом отличаться. Концепция DCN предусматривает возможность сосуществования нескольких ядер сети, подключенных к одной и той же сети радиодоступа. Такое разделение обеспечивает большую гибкость и оптимальное сетевое управление. Кроме того, использование выделенных ядер сети позволяет существенно оптимизировать затраты на построение сетей, так как можно проектировать сети с учетом уровня обслуживания и пропускной способности, необходимых для данного вида и объема трафика [1].

– Технология Private LTE. Private LTE представляет собой концепцию частных сетей LTE. Четвертая промышленная революция предполагает возрастающий объем M2M-коммуникаций. Наиболее эффективно такие задачи решаются при использовании сетевых беспроводных технологий нового поколения, которые обеспечивают масштабируемое управление и высокую надежность. В таких условиях наличие собственной мобильной сети позволяет компаниям и корпорациям оптимальным образом адаптировать инфраструктуру к своим задачам по сравнению с традиционным использованием стандартной сети оператора связи. Преимущества LTE по сравнению с сетями Wi-Fi заключается в лучшем масштабировании, возможности управления качеством обслуживания, мобильности и безопасности [1].

MVNO в России

Область виртуальных мобильных операторов переживает бурный рост. Относительно недавно на нее обратили свое внимание компании финансового сектора. Отчасти на это повлияла борьба за платежи абонентов, развернувшаяся между операторами и банками. В MVNO банки явно увидели для себя интересные возможности по оптимизации текущих расходов на коммуникацию со своими клиентами и возможности дополнительного роста собственной клиентской базы, а также дополнительного источника дохода от телекоммуникационных услуг [3]. К концу 2019 года доля банковского сектора составила 15 процентов абонентов MVNO.

Крупнейшими MVNO России остаются операторские проекты, на которые приходится 75 % рынка. По данным «ТМТ Консалтинг», по итогам 2019 года общее число MVNO абонентов в России достигло 9,3 млн, что составляет почти 4 % всех мобильных абонентов страны [4].

Большая часть абонентов MVNO – частные пользователи (физические лица). На рис. 2 представлена структура рынка MVNO на начало 2020 года.

На рис. 3 отображена общая динамика роста абонентской базы MVNO.

Рис. 2. Структура рынка MVNO России (2019) [4]

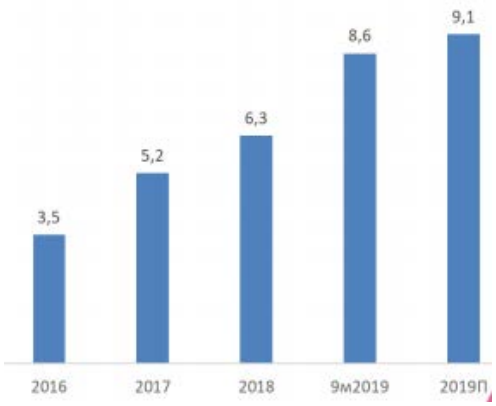


Рис. 3. Динамика абонентской базы MVNO России [4]

В ближайшие годы можно ожидать сохранения тенденции роста российского сегмента MVNO, при этом он по-прежнему будет формироваться, в первую очередь, текущими лидерами отрасли: операторами связи и крупнейшими банками.

Список используемых источников

1. Гольдштейн Б. С. Инфокоммуникационные сети и системы. СПб.: БХВ-Петербург, 2019. 208 с.

2. J. Lehikoinen, P. Pont, Y. Sent: Virtually mobile: What drives MVNO success. McKinsey & Company, 2014. pp. 5–6.

3. Фрейнкман В. MVNO для банковского сектора 2019 [Электронный ресурс] / Режим доступа: https://protei.ru/sites/default/files/media/2019-09Bank_MVNO.pdf (дата обращения 26.03.2020).

4. «ТМТ Консалтинг»: Российский рынок MVNO: Предварительные итоги 2019 года. Режим доступа: http://tmt-consulting.ru/wp-content/uploads/2019/12/TMT-MVNO-2019.pdf (дата обращения 20.03.2020).

УДК 004.413.5
ГРНТИ 50.43.19

ПРИМЕНЕНИЕ МАШИННОГО ОБУЧЕНИЯ И ИСКУССТВЕННОГО ИНТЕЛЛЕКТА В ТЕСТИРОВАНИИ ПРОГРАММНОГО ОБЕСПЕЧЕНИЯ

Б. С. Гольдштейн, В. А. Качалов

Санкт-Петербургский государственный университет телекоммуникаций им. проф. М. А. Бонч-Бруевича

Прогресс не стоит на месте. Вместо пишущих машинок применяются персональные компьютеры. Технологии все чаще находят место в жизни людей. На этом фоне разработка и поддержка программных продуктов становится все более прибыльным бизнесом. Одним из важных пунктов жизненного цикла программного обеспечения является тестирование. Одним из веяний моды в среде тестирования является машинное обучение и искусственный интеллект.

программное обеспечение, автоматизированное тестирование, искусственный интеллект.

С каждым днем прогресс идет все дальше и дальше вперед. Меняются возможности и потребности человечества. Технологии поглощают все больше сфер жизни. Человек становится более зависим от интернета и гаджетов [1]. К примеру, сейчас мы уже не представляем жизнь без онлайн- служб, вроде заказа еды или вызова такси. В больницах и разных общественных местах появилась возможность удаленно записаться и получить номерок в виртуальной очереди. И с каждым днем количество подобных сервисов растет.

Вместе с количеством растет и сложность программного обеспечения (далее ПО): больше строк кода, больше функционал. Это может неблагоприятно сказаться на качестве итогового продукта. Для предотвращения ошибок во время релиза, программная часть должна быть протестирована. При небольшом объеме и количестве приложений целесообразно применять ручное функциональное тестирование. Но что же делать, если объем тестов большой, релизы частые, а команда тестировщиков работает на пределе?

Тогда необходимо тесты автоматизировать. Гораздо проще использовать стандартизированный тестовый сценарий, заставляя алгоритмы работать за вас. Это возможно с использованием специализированных фреймворков, таких как: Selenium, Robot Framework, Katalon Studio. Но у данного метода имеются и свои недостатки. Требуется постоянный контроль над актуальностью тестового сценария. А что, если новый функционал появляется очень быстро и тестировщики перестают справляться? Можно нанять

больше людей, но есть и другой вариант. Использовать искусственный интеллект (далее ИИ) и машинное обучение (далее МО).

Несмотря на то, что применение искусственного интеллекта и машинного обучения может сделать жизнь тестировщика проще, это не является панацеей. Искусственный интеллект прошел долгий путь от научной фантастики до становления реальностью. Применение технологии не ограничивается парой десятков сфер, область его применения очень обширна: от здравоохранения до фермерского хозяйства, финансов и прочего [1].

Использование технологий нашло свое место и в тестировании ПО.

Использование технологий искусственного интеллекта и машинного обучения позволяет не только ускорить процесс создания автотрестов, но также снизить стоимость тестирования и даже самостоятельно генерировать новые тестовые сценарии.

Но применять данные технологии в тестировании не так просто, как составлять модели, нажимая пару клавиш и позволяя «железному мозгу» выполнять работу. Но есть множество вещей, которые не могут быть сделаны «роботами», а также много способов помочь так, как вы и не могли даже предположить. В этой статье будет рассмотрено для чего же лучше использовать машинное обучение и искусственный интеллект в тестировании программного обеспечения, а для чего лучше не использовать. Постановка возможности реализации – первый и важнейший шаг на пути к внедрению МО и ИИ в тестировании.

Не совершайте ошибки, думая, что искусственный интеллект и машинное обучение могут взять все задачи по тестированию на себя. Это не так, тестирование не должно быть полностью автономным. Алгоритмы машинного обучения должны лишь усиливать тестировщиков. Они не могут заменить работу QA-специалиста (от англ. Quality assurance – обеспечение качества), так как не способны самостоятельно определить сценарий работы программного обеспечения. Но, в то же время, эти алгоритмы могут быть мощным инструментом, способным заполнить пропуски и недостатки, затрудняющие процесс тестирования [2].

Автоматизация, помимо решения проблем ручного тестирования привносит и свои. К счастью, часть этих проблем можно решить с помощью внедрения искусственного интеллекта.

Ниже приведены некоторые проблемы, с которыми можно справиться:

– Время: чтобы автотесты удовлетворяли постоянно меняющемуся функционалу, QA-специалистам необходимо изменять тестовые сценарии, что усложняется накоплением изменений с течением времени. В связи с этим начинают накапливаться пробелы [2].

– Пропуск ошибок при добавлении нового функционала: автоматически выполняемые сценарии могут проходить успешно, при этом будут упущены ошибки в только что добавленном функционале. Часто это решается

проведением ручного теста, что не всегда возможно в условиях коротких сроков.

– Долгосрочные тест-кейсы (от англ: *test case* – тестовый случай): при редком обновлении тестовых сценариев возможно накопление упущений в покрытии функционала тестом [2].

– Навыки тестировщика: автоматизация тестирования требует наличия определенных навыков и знаний, а значит, что поиск специалиста может занимать длительное время.

Сложно автоматизировать тестирование пользовательских интерфейсов: обязательно требуется человеческое участие и оценка.

Роль ИИ и МО в тестировании, основные сценарии применения:

Кратко – приведенные технологии обрабатывают данные, идентифицируют схемы, создают и применяют тестовые сценарии без помощи человека. Это стало возможным благодаря применению нейросетей и методов глубокого обучения, когда система самообучается на данных, предоставленных ей, либо данных, извлеченных из внешних источников, в т. ч. и всемирной паутине [3].

Существует два основных сценария применения технологий:

1. Обучить ИИ создавать сценарии автоматизированного тестирования.

2. Обучить ИИ планировать тесты, самостоятельно решая, что необходимо запустить, а что починить.

Ожидается, что в ближайшем будущем технологии смогут научиться:

– находить любые изменения в ПО и определять, является ли это ошибкой, либо же это новый функционал, который должен быть протестирован.

– обновлять тестовые сценарии сразу же, после введения нового функционала.

– сравнивая результаты выполнения тестового сценария с лог файлами приложения, фиксировать изменения в работе ПО.

– оценивать покрытие тестовых задач сценарием, анализируя программный код приложения.

– объединять статистику тестирования в виртуальные рабочие столы и предоставлять удобный доступ к информации.

В любом случае, ожидания от внедрения ИИ и МО велики, но есть и подводные камни.

Во-первых, компании, стремящиеся внедрить эти технологии, не до конца осознают, как нужно использовать их.

Во-вторых, необходимо оценить эффективность новых технологий, в сравнении с традиционными методами тестирования.

В-третьих, применение МО и ИИ для тестирования требует изменений в культуре работы и рабочих процессах. Данные изменения на первых парах потребуют дополнительных расходов.

По этим причинам команды тестирования должны быть осторожны в желании приручить искусственный интеллект в своих целях. Первым делом, необходимо получить представление о пользе внедрения данных технологий, как их применение повлияет на бизнес.

Заключение

Подходы в тестировании ПО эволюционируют день ото дня, чтобы успеть за темпом разработки приложений, становясь более полноценными и сложными. В результате, быстро растущим разработчикам все чаще необходимо изменять свои тестовые конфигурации.

Приняв решение о внедрении искусственного интеллекта и машинного обучения для тестирования, компания должна будет правильно организовать рабочую деятельность и выделить время и финансы на обуздание новых технологий.

Список используемых источников

1. Домингос П. Верховный алгоритм. Как машинное обучение изменит наш мир: пер. с англ. М.: Манн, Иванов и Фербер, 2016. 336 с. ISBN 978-5-00100-172-0.

2. Майерс Г, Баджетт Т, Сандлер К. Искусство тестирования программ. СПб.: Вильямс, 2016, 272 с. ISBN 978-5-8459-1974-8.

3. Yaser S. Abu-Mostafa. Learning From Data: AMLBook, 2012, 213 с. ISBN-10 1600490069.

УДК 004.72
ГРНТИ 49.34.01

ОБЗОР СЛАЙСИНГА ДАННЫХ И АЛГОРИТМА СЕГМЕНТИРОВАНИЯ ТРАФИКА

А. А. Гребенщикова, В. С. Елагин

Санкт-Петербургский государственный университет телекоммуникаций им. проф. М. А. Бонч-Бруевича

Для повышения эффективности использования радиоресурсов 5G для межмашинного типа связи M2M, в работе рассматривается модель агрегации трафика данных типа M2M, а также модель сегментирования услуг пятого поколения 5G. Ожидается, что радиоресурсы 5G будут использоваться путем объединения данных нескольких устройств типа M2M для каждого слайса в отдельности. Каждый сегмент является изолированным от других и использует ресурсы в устройствах межмашинного типа для повышения спектральной производительности системы.

Используя данную работу, можно предсказать эффективность применения сегментирования данных в сетях пятого поколения с помощью методов имитационного моделирования и математических инструментов.

сетевое сегментирование, межмашинное взаимодействие M2M, агрегация трафика, приоритетная очередь, ретрансляционный узел RN, радиоресурсы, трафик пятого поколения 5G.

Введение

Из-за значительного увеличения трафика межмашинного типа связи M2M, снижается производительность обработки мобильного трафика в современных сотовых сетях [1, 2]. Устройства межмашинного типа связи передают как небольшие, так и огромные по размеру данные с различными требованиями по качеству обслуживания QoS.

Основные функции систем пятого поколения 5G включают агрегацию несущих (*Carrier Aggregation*, CA), технологию расширенного множественного входа и выхода (*Enhanced Multiple Input Multiple Output*, MIMO), координированную многоточечную связь (*Coordinated Multi-Point*, CoMP) и ретрансляционный узел (*Relay Node*, RN) [3].

Новая технология слайсинга позволяет сетевым операторам разделять одну физическую сеть среди других таких же, т. е. виртуальных, сквозных. Каждая такая сеть изолирована счетным устройством, сетью доступа, транспортной и базовой сетями. Следующим этапом сетевого сегментирования является выделение отдельного слайса и ресурсов для широкого спектра услуг с различными функциями и требованиями по качеству обслуживания QoS.

Системные модели

При детальном рассмотрении двух моделей трафика межмашинного типа M2M по восходящей линии связи в сетях пятого поколения 5G, стоит обратить внимание на несколько важных пунктов. Во-первых, модель трафика данных, базирующаяся на слайсинге. В данном механизме весь упор делается на классификации и соответствии требованиям по качеству обслуживания QoS. Стоит отметить трафик данных приложений межмашинного типа M2M, таких как смартфоны, интеллектуальная система здравоохранения и интеллектуальный мониторинг трафика. Во-вторых, т. к. приложения типа M2M обладают такими характеристиками, как трафик и разнообразный размер пакетов, становится актуальным рассмотрение модели объединения данных в ретрансляционном узле RN. По итогу, ожидается получение максимального уровня соответствия по качеству обслуживания QoS для радиоресурсов в сетях пятого поколения 5G. Также следует отметить три классификации трафика данных между релейным узлом RN и макростанцией

DeNB (донорская базовая станция, *Donor eNB*) на основе подхода с приоритетной очередью (*Priority Queue*, PQ).

Из-за разнообразия связи типа M2M сообщения межмашинного типа варьируются от потребления полосы пропускания на уровне битов (например, смартфоны) до приложений потребления полосы пропускания на уровне байтов (например, умная система здравоохранения). Согласно стандартизации сотовой сети, каждому устройству предоставляется наименьший ресурс для передачи данных – блок физических ресурсов (*Physical Resource Block*, PRB). Один блок PRB способен передавать несколько сотен байтов.

Данные модели могут быть реализованы для ретрансляционного узла RN в мобильной сети 5G. Подводя короткий итог, устройство межмашинного типа M2M рассматривается как устройство агрегирования ретрансляционного узла RN, в котором данные от нескольких устройств M2M агрегируются в данные одного устройства.

Модель агрегации данных межмашинного типа M2M

Модель, изображённая на рис. 1 (см. ниже), основана на агрегировании данных от нескольких устройств межмашинного взаимодействия M2M на уровне протокола конвергенции пакетных данных (*the Packet Data Convergence Protocol*, PDCP) в релейном узле RN.

Данные от всех устройств межмашинного взаимодействия M2M буферизируются в ретрансляционном узле RN. Алгоритм обновляет значение tMax, если RN принимает пакеты от устройства, которое имеет более высокий приоритет, чем приоритеты всех других устройств в очереди узла. Отдельные заголовки IP всех устройств M2M сохраняются целыми. Пакеты данных буферизуются до тех пор, пока задержка не достигнет tMax. Чтобы сравнить производительность модели агрегирования данных в узкополосных и широкополосных сценариях применения M2M, масштаб агрегации для устройств M2M оставляют равным 1 (не агрегированным), 5, 10, 15 и 20 в обоих случаях.

Модель слайсинга и алгоритм сегментирования трафика

В данной модели стоит обратить внимание на ассоциацию спредыдущей моделью агрегации, которая улучшала качество обслуживания QoS за счет эффективного использования радиоресурсов 5G для M2M и принципиальной идеи подхода приоритетной очереди. Эти интеллектуальные устройства имеют различные приоритеты очередей, которые зависят от приоритета пакетов, т. е. сначала самый высокий приоритет передается на выходной порт, а затем пакеты с более низким приоритетом, и так далее, как показано в алгоритме слайсинга трафика данных на рис. 2 (см. ниже) [4]. Возможным недостатком этого механизма планирования является то, что

трафик более низкого уровня не может обслуживаться в течение длительного времени, пока присутствует более высокий приоритет [5]. Следовательно, у низшего класса возникнут проблемы с обработкой, которая приведет к значительному отказу от пакетов. Ниже приведена среда интеллектуальных систем с тремя уровнями приоритетов: высокий (слайс № 1), средний (слайс № 2) и низкий (слайс № 3), опираясь на типы трафика данных следующим образом:

– интеллектуальная система здравоохранения – чувствительные данные с высоким приоритетом (1 мс);

– умная транспортная система – массивные данные со средним приоритетом (5 мс);

– смартфоны – популярные данные с низким приоритетом (10 мс).

Этот трафик данных будет работать в форме сегментирования по мобильной сети 5G на восходящей линии связи между релейным узлом RN и макросотой DeNB на основе интерфейса плоскости пользователя, как показано на рис. 3.

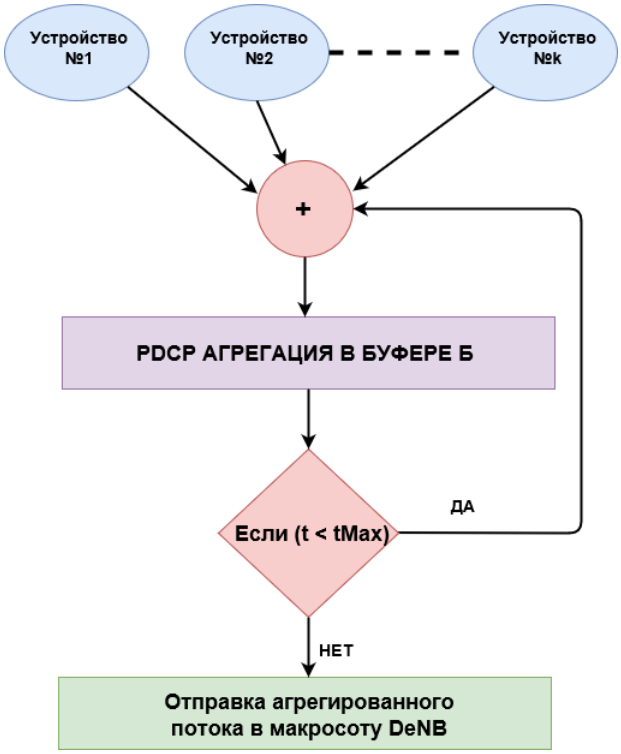


Рис. 1. Алгоритм агрегации данных межмашинного типа M2M

На основе модели, изображённой на рис. 3 (см. ниже), можно смоделировать систему сегментирования данных в программной среде AnyLogic. С помощью имитационного моделирования стоит рассмотреть разные случаи нагрузки отдельных слайсов, т. е. при определённом процентном соотношении рассмотренных типов трафика в модели, будет показана производительность системы и способность выдержать максимальную нагрузку.

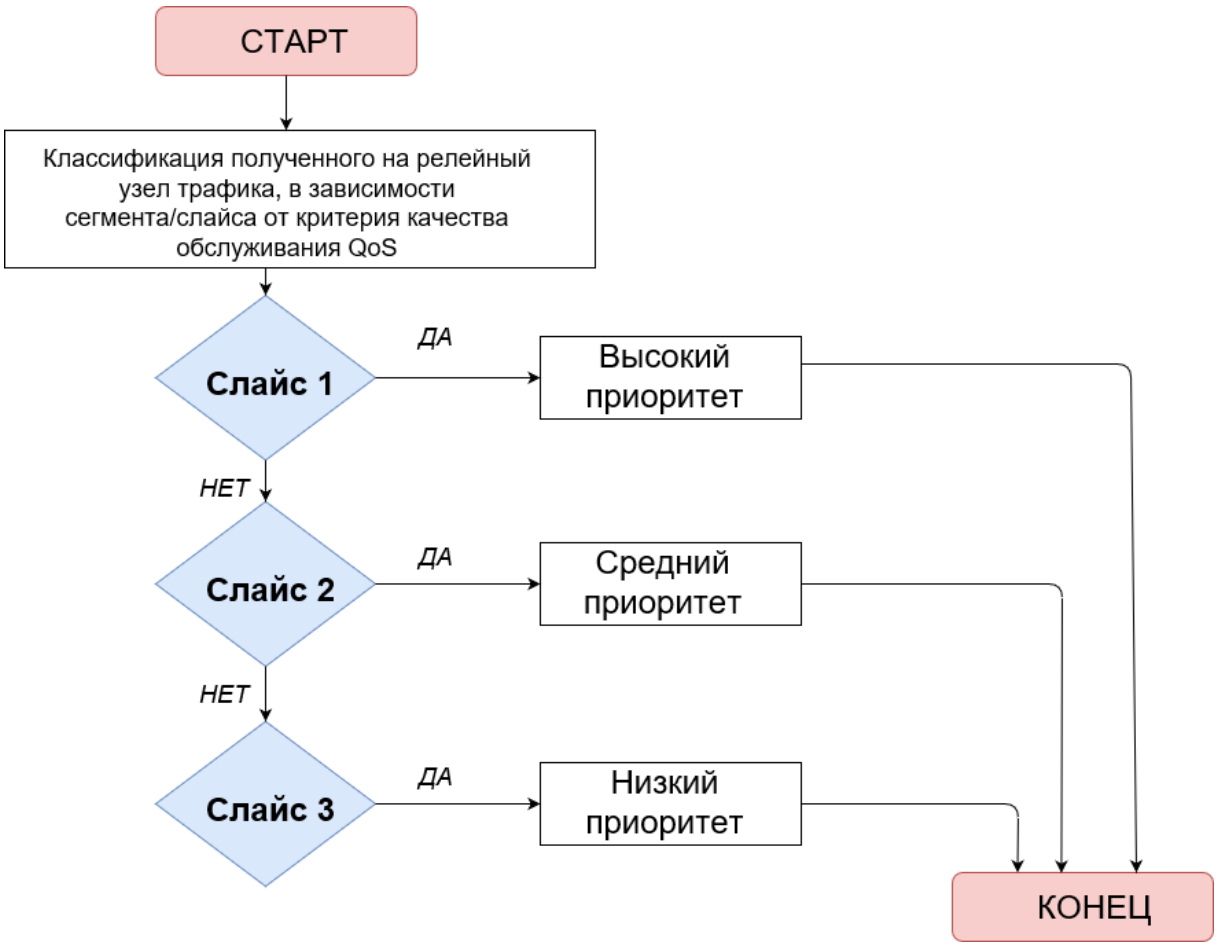


Рис. 2. Алгоритм сегментирования трафика данных

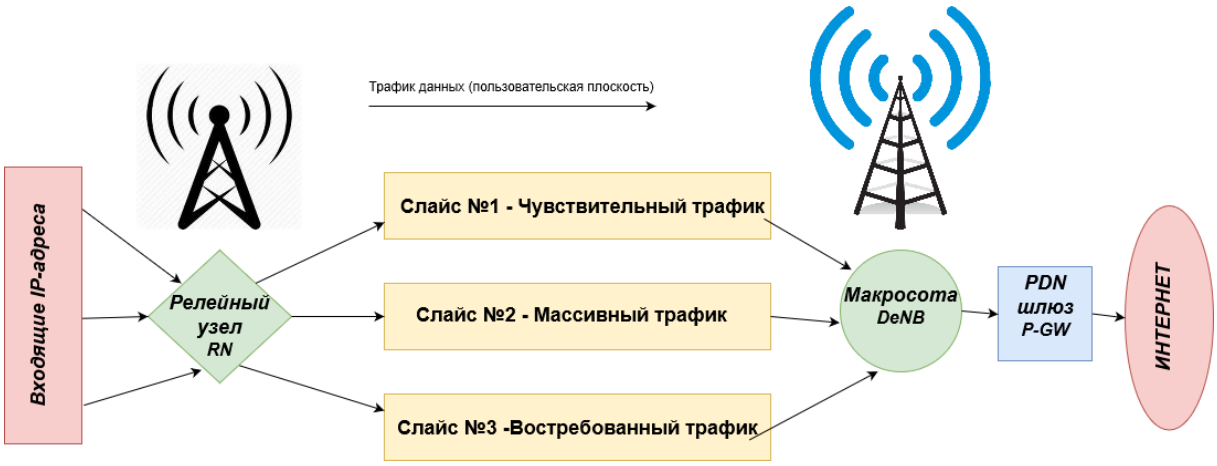


Рис. 3. Модель сегментирования данных

Заключение

Рассмотрено проектирование и разработка модели агрегации трафика данных для радиоресурсов 5G, основанной на эффективном использовании

небольшого по размерам блока физических ресурсов PRB, путем объединения данных с нескольких устройств типа M2M. Кроме того, новая модель сегментирования сети 5G опирается на интеллектуальные системы, что необходимо для умного города. Слайсы сети будут дифференцировать трафик данных интеллектуальных систем с точки зрения требований по качеству услуг QoS в каждом сегменте, таких как смартфоны, умная транспортная система и интеллектуальная система здравоохранения. Моделируемые классы трафика данных 5G содержат протокол передачи файлов (FTP), передачи голоса (VoIP) и видео. Сценарии делятся на три части M2M-связи на основе трафика данных, включая востребованный, чувствительный и массивный. Таким образом, ретрансляционный узел RN используется для улучшения покрытия и агрегирования трафика данных типа M2M восходящей линии связи для каждого сегмента в отдельности.

Список используемых источников

1. Choi Y., Park N. Slice architecture for 5G core network [Электронный ресурс] // Ninth International Conference on Ubiquitous and Future Networks (ICUFN) 2017. URL: https://www.researchgate.net/publication/318737842_Slice_architecture_for_5G_core_network (дата обращения 10.01.2020).

2. Dighriri M., Alfoudi A. S. D., Lee G. M., Baker T. Data Traffic Model in Machine to Machine Communications over 5G Network Slicing [Электронный ресурс] // 2016 9th International Conference on Developments in eSystems Engineering. URL: https://www.researchgate.net/publication/317071782_Data_Traffic_Model_in_Machine_to_Machine_Communications_over_5G_Network_Slicing (дата обращения 20.12.2019).

3. Abdalla I., Venkatesan S. Remote subscription management of M2M terminals in 4G cellular wireless networks // Local Computer Networks Workshops (LCN Workshops), 2012 IEEE 37th Conference on, October 2012: pp. 877–885.

4. Zirong G., Huaxin Z. Simulation and analysis of weighted fair queueing algorithms in OPNET // International Conference on Computer Modeling and Simulation, ICCMS 2009: pp. 114–118.

5. Zhang Y., Li Z., Mei S., Xiao L., Wang M. A new approach for accelerating IPSes communication. // 1-st International Conference on Multimedia Information Networking and Security, MINES 2009: vol. 2, pp. 482–485.

УДК 004.042
ГРНТИ 20.53.19

АНАЛИЗ BIG DATA ФРЕЙМВОРКОВ ДЛЯ РАСПРЕДЕЛЕННЫХ ПОТОКОВЫХ ВЫЧИСЛЕНИЙ

В. П. Гребенюк, В. С. Елагин

Санкт-Петербургский государственный университет телекоммуникаций им. проф. М. А. Бонч-Бруевича

В июле 2016 года в России были приняты два законопроекта, вносящие поправки, в федеральное законодательство: № 374-ФЗ и № 375-ФЗ. Относительно темы данной работы интерес представляют изменения в области регулирования хранения трафика пользователей и правил его предоставления федеральным службам. Законопроект обязывает операторов связи хранить звонки и сообщения абонентов за период, определяемый Правительством Российской Федерации (но не более, чем за 6 месяцев) в соответствии с 64-й статьей федерального закона «О связи», а информацию о фактах приема, передачи, доставки и обработки сообщений и звонков – 3 года. Основной проблемой по реализации 374-ФЗ является большой объем данных, которые необходимо хранить и обрабатывать на сети оператора. Учитывая это, стандартные подходы к работе с ними как со статично хранящимися в электронных таблицах или реляционных базах данных мало применимы.

Сохранение информации о трафике и самого трафика – это динамичный, безостановочный процесс. Исходя из этого, для работы с таким непрерывно поступающим объемом информации могут использоваться подходы технологии Big Data. В данной работе рассмотрены возможные варианты использования Big Data фреймворков для распределенных потоковых вычислений для задач оператора связи. В результате написания работы были изучены различные схемы хранения и обработки данных, возможные точки отказа, а также набор возможностей, предоставляемых программными комплексами обработки и хранения данных.

большие данные (BigData), распределенные вычисления, Apache Spark, хранение и обработка данных, Apache Storm, оператор связи, Apache Flink, Apache Samza.

Введение

Под потоковой обработкой данных (англ. *stream processing*) подразумевается обработка данных любого типа как потока. Потоковая обработка имеет дело с непрерывными данными и является основным инструментом по превращению больших данных в «быстрые» данные. Для этого необходимо, чтобы исходные данные оперативно подавались в аналитический инструмент – небольшими партиями или в режиме реального времени.

Потоковая обработка имеет достаточно богатую и насыщенную историю, которая начиналась с «активных» баз данных. Под активной БД понимается база данных, архитектура которой позволяет управлять событиями –

реагировать на условия как внутри, так и вне базы данных. Они обеспечивали условные запросы к данным, хранящимся в БД.

Одним из первых фреймворков для обработки потоков данных был TelegraphCQ, построенный на базе свободной СУБД с открытым кодом PostgreSQL. В дальнейшем стали создаваться другие фреймворки для потоковой обработки данных. Они позволяли пользователям создавать граф запросов на базе программного кода и запускать его одновременно на множестве машин (серверов).

Подобные архитектурные решения обработки потоков ориентированы на масштабируемость системы. Примерами таких решений стали Aurora, PIPES, Borealis. Однако ни один из них так и не обрел успешного коммерческого развития [1].

Под фреймворком здесь и дальше подразумеваются программные продукты, предназначенные для потоковой обработки данных. Технически они представляют из себя набор программных библиотек, которые решают фундаментальные вопросы взаимодействия и помогают разработчикам писать код для обработки потоковых данных, не имея дело с потоковой механикой более низкого уровня.

Прием и обработка потоковых данных

Фреймворки для потоковой обработки данных являются основой, для полноценного использования которой необходимо объединить её с прикладным ПО пользователя и системой хранения данных [2]. В данной статье рассматриваются свободные фреймворки с открытым исходным кодом из фонда Apache Software Foundation (ASF). Обобщенная схема потоковой обработки данных представлена на рис.

Первоочередной задачей потоковой обработки является прием и упорядочивание сообщений от источников данных. Задачей брокера является принятие сообщений и их гарантированная доставка потребителям. Данная задача может быть выполнена как самим фреймворком, так и сторонним инструментом. Наиболее популярный программный продукт, использующийся в качестве брокера сообщений – Apache Kafka.

Процесс доставки сообщений достаточно прост – входящие данные помещаются в очередь, сообщения которой дополнительно могут быть сохранены во внутреннюю базу данных. Это позволяет гарантировать потребителям, которые были отключены или недоступны в момент поступления данных, получение пропущенных сообщений, после включения в работу.

Потоковый фреймворк для обработки данных подключается к Kafka как потребитель и получает события для обработки из одной или нескольких очередей. Потоковые обработчики определяют операции, которые будут выполняться над каждым элементом данных при прохождении через систему.

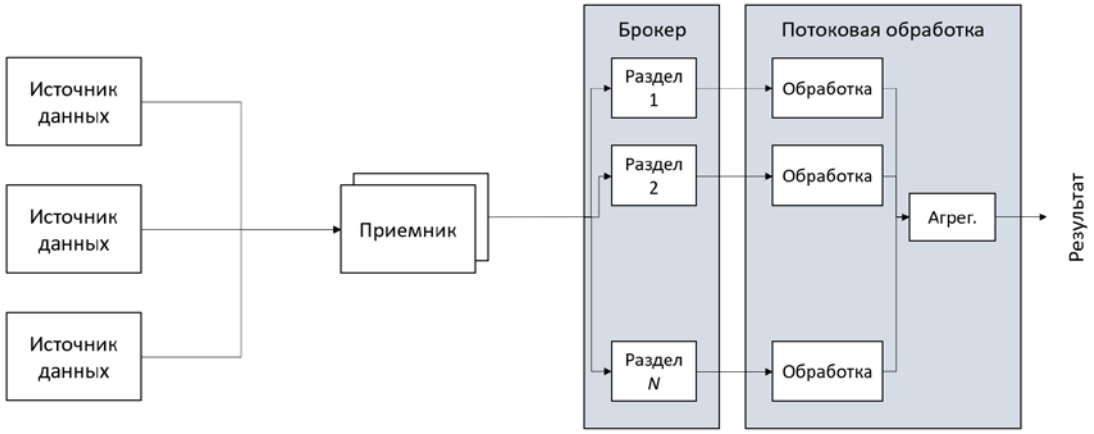


Рис. Обобщенная схема получения и обработки сообщений

Основные различия потоковых фреймворков

Основные различия заключаются в подходе к обработке данных и используемой модели программирования [3].

Относительно модели обработки данных, обычно рассматривают два типа систем:

1. Последовательной потоковой обработки.
2. Пакетной потоковой обработки.

В первом случае входящие данные обрабатываются в строгой последовательности. Среди продуктов Apache на данном принципе устроена работа фреймворков Flink, Storm и Samza.

В случае пакетной модели перед обработкой данные разбиваются по пакетам. Представителями данного подхода являются Apache Spark и Apache Storm.

Модель программирования также бывает двух типов: композиционная и декларативная.

Для композиционной модели характерно создание элементов обработки путем объединения источников и элементарных операторов. С дальнейшим соединением их входов и выходов. По такому принципу работают фреймворки Apache Flume и Apache Storm.

Такое название модель получила потому, что на момент выполнения программного кода формируется схема обработки проходящего через систему сообщения, однако не происходит непосредственной обработки данных. Такая особенность позволяет создавать описание модели на любом языке программирования. Однако должно соблюдаться условие – класс должен соответствовать основному интерфейсу, а также должны быть вызваны соответствующие методы класса, которые воссоздают логический план обработки.

Сравнительный анализ

Исходя из описанного выше, был произведен сравнительный анализ спецификаций следующих продуктов Apache: Spark, Flink, Storm и Samza (табл., см. ниже). Все они являются надежными, отказоустойчивыми, масштабируемыми и распределенными решениями с кластерной архитектурой, и предназначены специально для обработки потоков больших данных «на лету», распределяя вычисления по направленной графовой модели потоковых обработчиков, называемой DAG-топологией (*Directed Acyclic Graph* – направленный ациклический граф) [4, 5].

В качестве критериев были выбраны две категории параметров:

1. Функциональные:
- задержка обработки данных (*latency*);
- семантика доставки сообщений;
- управление состоянием *(stateful* / *stateless*);
- избирательная обработка данных;
- источники и приемники информации.

2. Архитектурные:
- потоковые и вычислительные примитивы;
- поддерживаемые подходы к обработке данных;
- инструменты отказоустойчивости;
- поддерживаемые ЯП, API и коннекторы.

ТАБЛИЦА. Сравнительный анализ Big Data фреймворков

Критерий / Фреймворк	Apache Spark	Apache Flink	Apache Storm	Apache Samza
Обработка данных	Микро-пакетная	Потоковая и пакетная	Потоковая и пакетная	Потоковая
Задержка обработки	> 1 с	< 1 мс	< 1 мс	< 1 мс
Потоковый примитив	Микропакет из нескольких наборов данных	Поток данных	Поток данных в виде наборов пар ключ-значение	Сообщение потокового раздела
Вычислительный примитив	Задача	Задача	Потоковый обработчик	Задача
Семантика доставки сообщений	Однократно	Однократно	Однократно или минимум однократно	Минимум однократно
Сохранение состояния приложений	Внешняя распределенная файловая система	Локальное хранилище, внешнее хранилище	Нет	Встроенные хранилища

Источники и приемники данных	Kafka, Cassandra, HDFS, OpenStack Swift, Cassandra, Amazon S3, Kudu	Kafka, Cassandra, Amazon Kinesis, HBase, HDFS, Google CP	Kafka, Kestrel, Amazon Kinesis, HBase, Cassandra, RabbitMQ, JMS	Kafka
Отказо-устойчивость	Контрольные точки	Контрольные точки	Автоматический перезапуск фоновых задач на узле кластера	Транзакцион-ность сообщений
Избирательная обработка данных	Временные окна	Временные окна	Нет	Нет
Поддерживае-мые языки	Scala, Java, R, Python	Только JVM-языки	Любые	Только JVM-языки

В настоящее время существует достаточно много различных потоковых фреймворков. Разработчики данных продуктов позиционируют их как универсальные и пригодные для всех случаев жизни, однако крупные компании предпочитают создавать узко специализированные фреймворки для удовлетворения своих потребностей [6]. Ни один из этих вариантов не является идеальным, поскольку имеет свои достоинства и недостатки. Таким образом, при выборе Big Data решения следует внимательно учитывать преимущества и слабые стороны каждого инструмента, принимая во внимание характеристики, особенно значимые в каждом конкретном случае.

Список используемых источников

1. Майсор Д., Кхупат Ш., Джайн Ш. Архитектура и шаблоны больших данных [Электронный ресурс] // Информационный менеджмент. 2014. № 1. С. 2–8. URL: https://www.ibm.com/developerworks/ru/library/bd-archpatterns1/bd-archpatterns1-pdf.pdf (дата обращения 04.02.2020).

2. Марц Н., Уоррен Д. Большие данные. Принципы и практика построения масштабируемых систем обработки данных в реальном времени. М. : Вильямс, 2016. 368 с.

3. Самарев Р. С. Обзор состояния области потоковой обработки данных // Труды ИСП РАН, 2007. Т. 29. Вып. 1. С. 231–260.

4. Хеллстрем Я. Обзор потоковых технологий Apache [Электронный ресурс] // Базы данных. 2016. № 1. С. 1–3. URL: https://databaseline.tech/an-overview-of-apache-streaming-technologies (дата обращения 07.02.2020).

5. Радченко И. А, Николаев И. Н. Технологии и инфраструктура Big Data. СПб. : Университет ИТМО. 2018. 52 с.

6. Гольдштейн А. Б., Скоринов М. Ю., Феноменов М. А. Big Data – как выпустить джинна из бутылки? [Электронный ресурс] // Технологии и средства связи. 2015. № 5.

С. 34–38. URL: http://files.iks.sut.ru/publications/2015-015-pp.pdf (дата обращения 15.02.2020).

УДК 004.042
ГРНТИ 20.51.23

СИСТЕМЫ ФИЛЬТРАЦИИ КОНТЕНТА

М. Д. Григорьев, С. А. Давыдова, Н. В. Кривоносова

Санкт-Петербургский государственный университет телекоммуникаций им. проф. М. А. Бонч-Бруевича

В условиях широкого распространения и доступности ресурсов сети Интернет все более актуальной становится фильтрация контента для всех категорий пользователей. Особую важность фильтрация контента имеет в образовательных организациях, в системе «Родительский контроль», а также в работе интернета, на сегодняшний день является обязательной, причём не только в учебных учреждениях, но и в домашних условиях. Обязательной она является, потому что большая часть новой информации, которая появляется в интернете ежечасно, является нежелательной, это могут быть: ресурсы порнографического характера, онлайн-казино, сайтов об оружии, наркотических веществах, сатанизме, насилии и т. д.

динамическая фильтрация, статическая фильтрация, система контроля фильтрации.

Немалую часть сайтов в сети Интернет составляют информационные ресурсы, содержащие нежелательную и небезопасную информацию для определенных категорий пользователей. Например, это ресурсы порнографических сайтов, онлайн-казино, сайтов об оружии, наркотических веществах, сатанизме, насилии и т. д. Так же в число нежелательных входят сайты и порталы, содержащие ненормативную лексику и контрафактный контент.

Данная работа будет посвящена выбору архитектуры системы контентной фильтрации для защиты учебных заведений от несанкционированного информационного контента.

Важной задачей современной телекоммуникационной инфраструктуры является обеспечение социальной безопасности детей и подростков, людей с неустойчивой психикой путем запрета доступа к небезопасному контенту. Кроме того, посещение сайтов с небезопасной информацией ведет к возникновению уязвимостей в информационных системах, повышает вероятность загрузки вредоносного программного обеспечения.

Для выявления нежелательного контента в Интернете и блокировки доступа пользователей к нему используются системы контентной фильтрации (СКФ). В данной работе будет проведен обзор существующих архитектур систем контентной фильтрации и сравнение их по производительности и скорости работы. Акцент на скорости работы сделан не зря – дело в том, что СКФ замедляет работу сети по предоставлению доступа к сети Интернет, вследствие чего инженеры телекоммуникационных сетей нередко устанавливают СКФ в один из сегментов сети, оставляя другие сегменты незащищенными.

По способам установки и использования существуют несколько вариантов СКФ [1]:

– фильтрация на государственном уровне: централизованный государственный подход к фильтрации контента со стороны государства (централизованное, но затратное решение);

– фильтрация на уровне провайдера: создание списков запрещенных ресурсов, опираясь на государственные источники (относительно невысокая стоимость и высокая надежность, но снижение скорости доступа);

– фильтрация на уровне интернет-шлюза (рис. 1): предпочтительный вариант для использования в государственных и образовательных учреждениях, частных компаниях, предусматривает установку специального программного обеспечения, которое отвечает за отслеживание контента. Предполагается настройка сетевого шлюза, через который проходит интернет-трафик всех компьютеров или других устройств в сети (больше возможностей по настройке системы фильтрации, быстрый доступ к сети Интернет, но требует в штате сотрудника – ИТ-специалиста;

– фильтрация на уровне компьютера: предполагает установку и настройку программного обеспечения на сами компьютеры пользователей, используется чаще всего в небольших организациях или для домашнего использования (недорогие и бесплатные решения, требуют знаний пользователя).

На сегодняшний день существует 2 вида фильтрации: статическая и динамическая.

Принцип работы статической фильтрации заключается в том, что, когда пользователь вводит адрес в браузер, СКФ начинает его искать в своей базе данных «черных» списков. Если этот адрес присутствует в «черном» списке, то пользователю страница становится недоступна, также появляется сообщение о блокировке страницы, по причине содержащегося в ней контента. Если же при проверке базы данных СКФ обнаружила искомую страницу в «белом» списке, то она выведет ее пользователю без изменений.

Но, так как количество веб-сайтов постоянно растет, и охватить весь этот диапазон невозможно, появляется еще одно понятие – «серый» список.

Это контент, который не был проверен системой (отсутствует в обоих списках). Так как система не может определить тип трафика «белый/черный», то контент «серого» списка доступен пользователю в полном объеме.

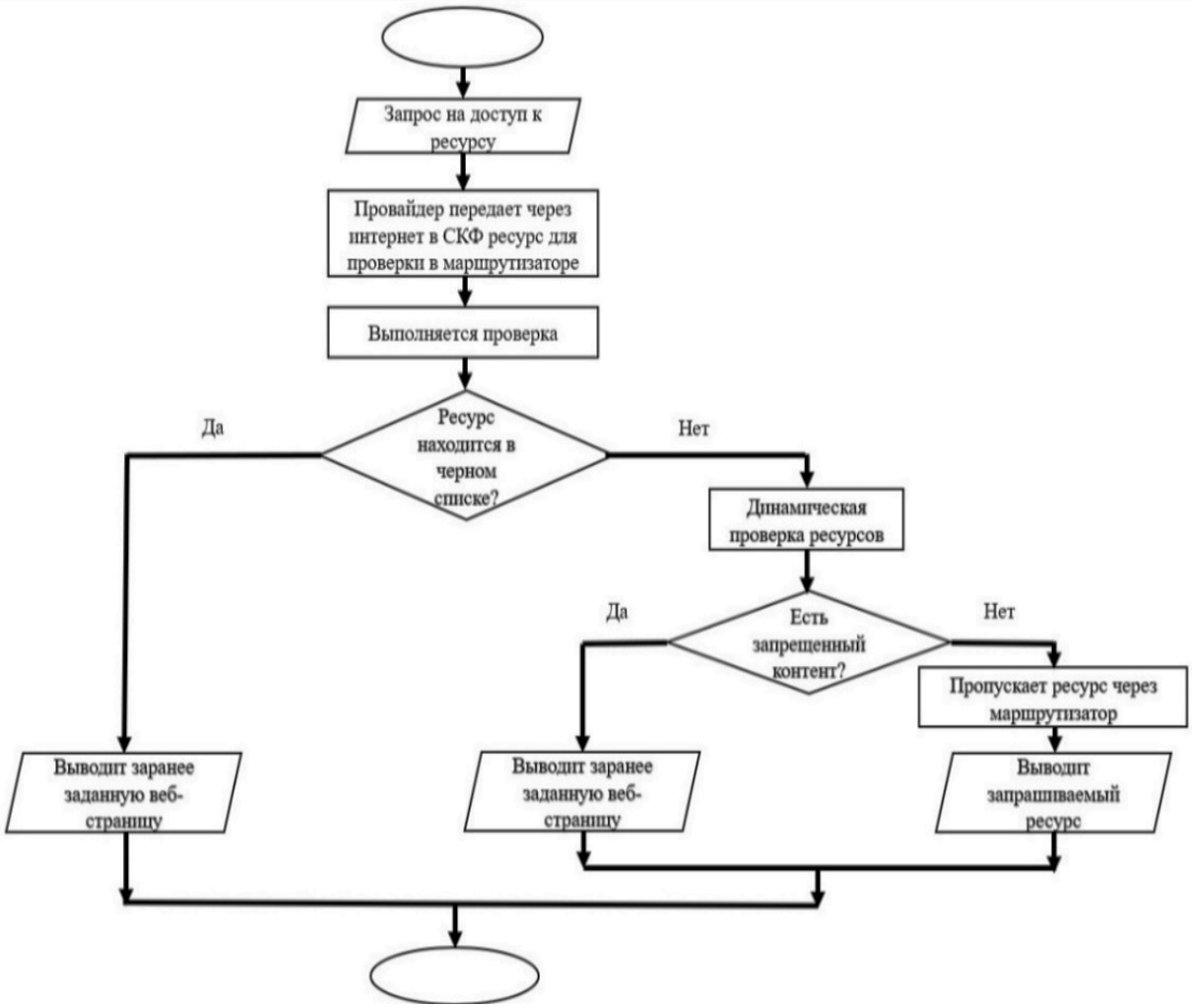


Рис. 1. Интернет фильтрация на уровне интернет шлюза

Из-за наличия непрерывно пополняющегося количества «серых» страниц, был разработан метод динамической фильтрации.

При динамической маршрутизации пользователь вводит адрес нужного ему ресурса в адресную строку, данные из которой передаются системе фильтрации. СКФ в это время обращается к данному ресурсу, формируя содержимое страницы в виде текста, в котором по определенным алгоритмам ищется запрещенный контент. Поиск осуществляется по настройкам фильтра, указанным инженером. В результате проведения фильтрации будет выведен либо контент, который удовлетворяет всем настройкам фильтра, либо сообщение о запрещенном контенте, либо система может вывести часть контента, которую настройки СКФ посчитали удовлетворяющей их требованиям.

Сравнивая способы фильтрации, можно сказать, что статическая явно уступает динамической по предоставляемому контенту.

Безусловный плюс динамической системы в том, что при обращении к какой-либо странице она сканирует содержимое, в отличие от статической, которая просто смотрит по спискам совпадения. Поэтому при изменении контента на странице на запрещенный, динамическая СКФ выведет сообщение о запрещенном контенте, а статическая – выведет контент. Однако динамическая фильтрация требует достаточно серьезных ресурсов.

Реализация наиболее эффективной СКФ возможна путем соединения статической и динамической модели: при обработке адреса веб-страницы сначала проверяется «черный» список, потом «белый» и «серый» списки. Информация будет доступна пользователю только после проверки всех списков. Это позволит охватить больший объем данных, но, к сожалению, данный подход крайне ресурсоемкий.

Для правильного выбора варианта реализации системы контентной фильтрации необходимо провести обзор возможных архитектур. Так как СКФ не работают отдельно от компонентов сетевой инфраструктуры, то они могут быть реализованы в виде:

– служб операционной системы (ОС), находящихся и работающих на компьютерах пользователей;

– служб ОС, находящихся и работающих на промежуточных сетевых узлах;

– модулей расширений или самостоятельных программно-аппаратных устройств, которые относятся к промежуточному сетевому оборудованию.

Так как это довольно обширная предметная область, обзор будет проведен только для наиболее оптимальных вариантов фильтрации контента для госучреждений (рис. 2, см. ниже).

Объектом исследования стала ИТ инфраструктура ГБОУ СОШ № 17 города Санкт-Петербурга. Предмет исследования – выбор средств фильтрации контента на основе требований современного законодательства и имеющихся аппаратных ресурсов.

На основе проведенного анкетирования и интервьюирования с администрацией образовательного учреждения ГБОУ СОШ № 17 Санкт-Петербурга, а также с его техническими специалистами, был выявлен ряд проблем современных средств фильтрации контента (СФК) на основе разработанного тестового стенда. Задача тестового стенда – организация работы СКФ, тестирование на точность и скорость работы. Первым был установлен и протестирован контент фильтр «KinderGate Родительский Контроль». Было зафиксировано замедление скорости соединения, связанное с тем, что алгоритм работы СКФ предполагает последовательную проверку адресов «черного» списка с последующим отображением контента. Далее на тестовом стенде был установлен фильтр «NetPolicePro». Тестирование системы

показало, как и в первой СКФ, уменьшение скорости соединения. Далее было протестировано решение о тотальной блокировке всего запрещенного законодательством контента, что было реализовано с помощью инструмента «СТОиК-Контент». Данный инструмент позволяет формировать репозиторий учебных материалов (например, электронных учебников, презентаций и других материалов), из которого можно извлекать информацию на любом устройстве, будь то компьютер, ноутбук, планшет или даже телефон обучающегося. Извлечение данных происходит путём подключения мобильного устройства к сети Wi-Fi или персонального компьютера к локальной сети. Основной плюс данной методики состоит в том, что для получения нужных, ранее помещённых в хранилище данных, не требуется доступ к сети Интернет, что исключает возможность просмотра запрещенного контента обучающимися. Главной проблемой такого подхода стала неготовность сотрудников мобильно предоставлять методические материалы, а также возможность использования материалов в режиме онлайн. По итогам работы тестового стенда руководством образовательной организации было принято решение об установке «NetPolicePro», так как время отклика ресурсов в данном фильтре все же выше, чем у «Родительского контроля».

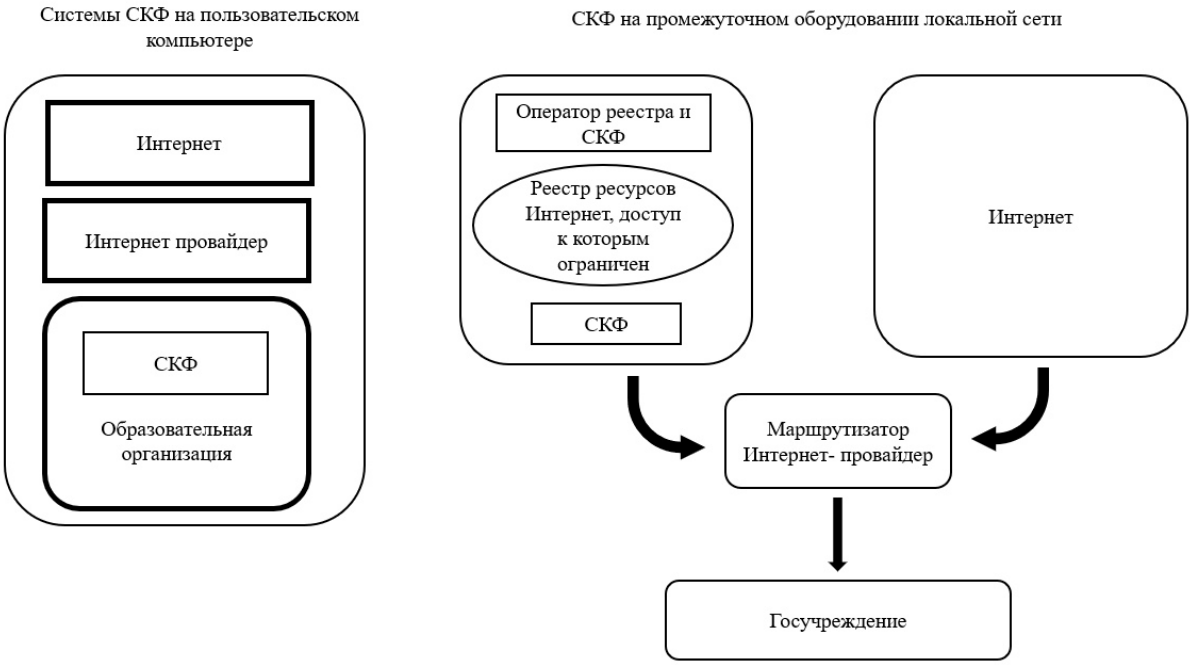


Рис. 2. Устройство СКФ в госучреждениях

Таким образом, для оптимальной работы с контентом на основе современного законодательства в образовательных организациях необходимо сочетать оба метода фильтрации: статический и динамический. Кроме того, ускорить работу системы фильтрации поможет реализация многопоточности. Многопоточность должна быть встроена в программное обеспечение,

которое при установке самостоятельно определит возможное количество потоков. Это позволит СКФ проверять списки URL не поочередно, а параллельно, что существенно сэкономит время и ресурсы.

Список используемых источников

1. Тихомиров И. А., Соченков И. В. Метод динамической контентной фильтрации сетевого трафика на основе анализа текстов на естественном языке // Вестник НГУ. 2008. № 2 (Т. 6). С. 34–39.

Статья представлена доцентом кафедры ПИиВТ СПбГУТ, кандидатом технических наук Д. В. Окуневой.

УДК 536.51; 531.787
ГРНТИ 47.01.81

ВОЛОКОННО-ОПТИЧЕСКАЯ СИСТЕМА КОНТРОЛЯ ТЕМПЕРАТУРЫ АККУМУЛЯТОРНЫХ БАТАРЕЙ ГИБРИДНЫХ ТРАНСПОРТНЫХ СРЕДСТВ НА ОСНОВЕ АДРЕСНЫХ ВОЛОКОННЫХ БРЭГГОВСКИХ СТРУКТУР С ДВУМЯ ИДЕНТИЧНЫМИ СВЕРХУЗКОПОЛОСНЫМИ СПЕКТРАМИ ОТРАЖЕНИЯ

Р. Р. Губайдуллин

Казанский национальный исследовательский технический университет им. А. Н. Туполева

В работе представлена принципиальная схема волоконной оптической радиофотонной системы контроля состояния аккумуляторных батарей гибридных транспортных средств основанной на мониторинге температуры с помощью массива адресных волоконных брэгговских структур с двумя идентичными сверхузкополосными спектрами отражения.

волоконная брэгговская решетка, ВБР, датчик температуры, адресные волоконные брэгговские структуры, гибридное транспортное средство, гибридный автомобиль.

На сегодняшний день с увеличением цен на углеводородное топливо примерно в 5 раз за последние 20 лет [1], а также с ужесточением экологических норм на выбросы продуктов сгорания двигателей внутреннего сгорания автотранспортных средств (Евро 6 в Европе и Евро 5 на территории Российской Федерации), автопроизводители вынуждены все больше внима-

ния уделять альтернативным источникам энергии, таким, как многозарядные аккумуляторные батареи для электрических и гибридных транспортных средств. Однако, использование подобных источников энергии ставит перед инженерами различных областей ряд вопросов, связанных с пожаробезопасностью, экологичностью производства, использованием и утилизацией батарей, контролем технического состояния, зарядкой, компоновкой силовых элементов гибридного транспортного средства. Для решения вопроса технического состояния аккумуляторных батарей, в данной работе была предложена радиофотонная система мониторинга температуры батарей, где в качестве чувствительного элемента используется адресная волоконная брэгговская структура с двумя идентичными сверхузкополосными спектрами отражения (2λ-ВБР) [2, 3, 4, 5], выступающими уникальным идентификатором чувствительного элемента, что в сумме с применением разложения на ряды Фурье сигнала мощности на фотоприёмниках, используемых в качестве устройства, опрашивающего температурные датчики, позволяет отказаться от применения сложных и дорогостоящих устройств опроса – интеррогаторов и спектр-анализаторов, используемых в классических волоконных оптических сенсорных системах (ВОСС), основанных на методе спектрального уплотнения каналов [6]. Согласно данным изложеным в статье [7], данная адресная волоконная брэгговская структура (АВБС), по своей сути, представляет собой две сверхузкополосные ВБР с разнесенными блинами волн Брэгга на адресную частоту. Отклик отражения подобной АВБС, полученной в пакете программ OptiGrating, представлен на рис. 1а, а ее схематичное представление на рис. 1б.

Для эффективной работы системы мониторинга температуры батарей гибридных транспортных средств, разрабатываемая система должна обладать следующими качествами:

– устойчивость к электромагнитным излучениям (ЭМИ), излучаемым от зарядного устройства, электродвигателя и от самих батарей;

– функциональная возможность передачи информационного сигнала о состоянии батарей на бортовой компьютер транспортного средства;

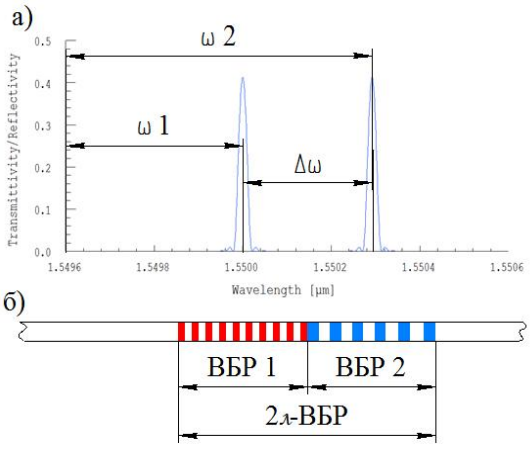


Рис. 1. Адресная волоконная брэгговская структура с двумя идентичными сверхузкополосными спектрами отражения (2λ-ВБР) [3]: а) спектральный отклик АВБС, б) схема АВБС

– возможность организации массива датчиков в единую ВОСС;

– низкая стоимость устройства, опрашивающего оптоволоконные датчики;

– возможность быстрого и простого монтажа и отсоединения батареи с температурным датчиком из силовой системы транспортного средства при ремонте и обслуживании;

– простота обслуживания и ремонтопригодность датчика;

– устойчивость чувствительного элемента и корпуса датчика к длительным тепловым нагрузкам в диапазоне от –40 до 60 °С – для большинства аккумуляторных батарей, и до +300 °С – для батарей Ni-NaCl и Na-S, согласно данным таблицы.

ТАБЛИЦА. Температурные режимы работы различных аккумуляторных батарей [8]

Тип батареи	Рабочая температура, °С
Zebra (Ni-NaCl)	от –40 до 350
Pb-PbO_2	от 0 до 40
Ni-Cd	от –20 до 50
Ni-MH	от 20 до 40
Na-S	от 300 до 350
Li-Ion	от –40 до 60

Значительную часть задач возможно решить с помощью радиофотонных методов измерения. Так, согласно данным, представленным в работе [9], ВБР мало восприимчивы к ЭМИ. На сегодняшний день технологии передачи информации от ВБР на электронные устройства хорошо изучены и широко применяются в технике [10]; как было упомянуто выше, в предложенной радиофотонной системе в качестве опрашивающего устройства используются простые и дешевые фотоприёмники вместо дорогостоящих интеррогаторов или спектр-анализаторов.

Исходя из данных, изложенных в работе [3], предъявленным требованиям к АВБС соответствуют адресные волоконные брэгговские структуры с двумя идентичными сверхузкополосными спектрами отражения. Исходя из ГОСТ 13659-78, верхний рабочий диапазон оптического волокна составляет +300 °С, а температура начала деформации кварцевого стекла – по меньшей мере +1250 °С, согласно ГОСТ 15130-86, что удовлетворяет условиям работы низкотемпературных аккумуляторных батарей и дает основание полагать о возможности использования подобного класса чувствительных элементов для высокотемпературных аккумуляторов.

В зависимости от способа монтажа и схемы расположения аккумуляторных батарей в транспортном средстве, тип АВБС может изменяться. Однако проанализировав существующие модели гибридных автомобилей,

можно сделать вывод о том, что большинство из них создается на основе конструкции обычных бензиновых автомобилей, что вынуждает конструкторов размещать аккумуляторные батареи блоками в различных частях автомобиля. В связи с этим в качестве наиболее перспективного типа АВБС была выбрана 2λ-ВБР, так как она работает на отражение и позволяет подключать массив датчиков последовательно, что значительно упрощает подключение блоков аккумуляторных батарей к силовой системе гибридного транспортного средства [3, 10, 11].

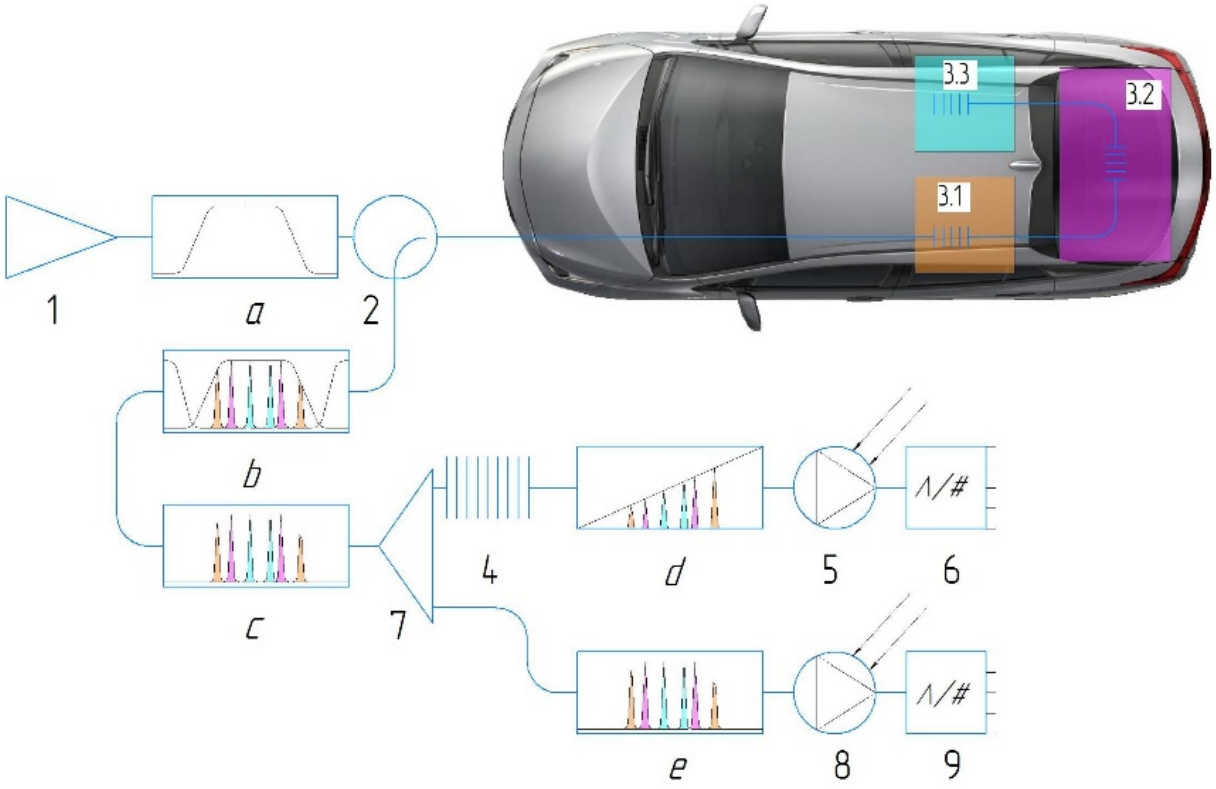


Рис. 2. Оптико электронная схема опроса измерительной системы:
1 – широкополосный лазер, 2 – циркулятор, 3.1–3.3 – 2λ-ВБР чувствительные элементы, 4 – наклонный фильтр, 5 – измерительный фотоприемник, 6 – измерительный аналого-цифровой преобразователь, 7 – оптический делитель, 8 – опорный фотоприемник, 9 – опорный аналого-цифрой преобразователь

Оптико-электронная схема опроса 2λ-ВБР (рис. 2) основана на принципах радиофотонных измерений и предназначена для анализа излучения от АВБС, где широкополосный лазер (1) генерирует непрерывное излучение (диаграмма *a*), которое отражается от АВБС (3.1–3.3) и попадает в циркулятор (2), который перенаправляет отраженный от АВБС сигнал (диаграмма *b*) на оптоволоконный разветвитель (7), где оптический сигнал (диаграмма *c*) делится на два канала: опорный и измерительный. В измерительном канале устанавливается фильтр с линейной амплитудно-частотной характеристикой (4), асимметрично изменяющий амплитуды многочастотного излучения (диаграмма *d*), после чего оптический сигнал

подается на измерительный фотодетектор (5) и принимается на аналого-цифровой преобразователь (АЦП) – (6). В опорном канале сигнал (диаграмма *е*) без изменения мощности попадает на опорный фотоприемник (8) и предается в опорный АЦП (9). Далее все расчеты ведутся не с абсолютным значением мощности светового потока, а с отношением мощностей в измерительном и опорном каналах. Отношение мощностей оптического сигнала на фотоприемниках (5 и 8) дает возможность избавиться от недостатка широкополосного лазера, связанного с колебаниями мощности светового потока, возникающих в оптико-электронной системе [10, 11].

Температуру аккумуляторной батареи в точке установки АВБС датчика можно определить, как функцию температуры от смещения центральной длины волны для датчика Температуру аккумуляторной батареи в точке установки АВБС датчика можно определить, как функцию температуры от смещения центральной длины волны для датчика [12]:

$$T = f(\Delta\lambda_T, c_2, c_1, c_0) = c_2 \cdot \left(\Delta\lambda_T\right)^2 + c_1 \cdot \Delta\lambda_T + c_0,$$

где $\Delta\lambda_T$ – сдвиг центральной длины волны вследствие температурного воздействия; c_i – калибровочные коэффициенты.

Выводы

В ходе проведения работ по разработке волоконно-оптической системы контроля температур аккумуляторных батарей транспортных средств был выполнен следующий список работ:

– обосновано использование волоконно-оптических чувствительных элементов;

– выбран класс и тип чувствительного элемента;

– предложена схема измерительного устройства и методика калибровки температурных датчиков.

Список используемых источников

1. Корнилов Д. А., Макаренко В. С., Макаров В. М. Динамика средних мировых цен на нефть // Иннов: электронный научный журнал. 2017. № 3 (23). URL: http://www.innov.ru/science/economy/dinamika-srednikh-mirovykh-tsen-na-/

2. Хабибуллин Р. А., Морозов О. Г., Нуреев И. И., Сахабутдинов А. Ж., Фасхутдинов Л. М. Методы формирования двухчастотного излучения с разностной частотой, лежащей в терагерцовом диапазоне // Физика волновых процессов и радиотехнические системы. 2017. Т. 20. № 3–2. С. 41–46.

3. Сахабутдинов А. Ж. Адресные волоконные брэгговские структуры на основе двух идентичных сверхузкополосных решеток // Инженерный вестник Дона. 2018. № 3. URL: http://ivdon.ru/en/magazine/ archive/n3y2018/5142

4. Сахабутдинов А. Ж. Радиофотонные сенсорные системы на адресных волоконных брэгговских структурах и их применение для решения практических задач: дис. … д-ра техн. наук : 05.11.07 / Сахабутдинов Айрат Жавдатович. Казань, 2018. 467 с.

5. Иваненко В. А., Алексеев В. Н., Лобанов И. А. и др. Волоконно-оптическая сенсорная система контроля температуры токоведущих шин // Информационные технологии в электротехнике и электроэнергетике: материалы XI всерос. науч.-техн. конф., Чебоксары, 2018 г. Чебоксары : Чувашский государственный университет имени И. Н. Ульянова (Чебоксары), 2015. С. 316–320.

6. Biswanath Mukherjee WDM optical communication networks: Progress and challenges // IEEE Journal on Selected Areas in Communications, vol. 18, no. 10, pp 1810–1824, 2000.

7. Gubaidullin R. R., Agliullin T. A., Morozov O. G., Sahabutdinov A. Jh., Ivanov V. Application of Addressed Fiber Bragg Structures for Measuring Tire Deformation // 2019 Systems of Signal Synchronization, Generating and Processing in Telecommunications (SYNCHROINFO) – Yaroslavl, 2019.

8. Zheng Liu, Rosario Morello, Wei Wu Experiments on battery capacity estimation // Conference Record – IEEE Instrumentation and Measurement Technology Conference. 2015. PP. 863–868. doi: 10.1109/I2MTC.2015.7151382.

9. Варжель С. В. Волоконные брэгговские решётки. СПб.: Университет ИТМО, 2015. 65 с.

10. Бурдин А. В., Бурдин В. А., Воронков А. В., Шишова Н. А. Исследование параметров волоконно-оптической линии передачи. Самара: Министерство ЗФ по связи и информатизации / Поволжская Государственная академия телекоммуникаций и информатики Кафедра линий связи и измерений в технике связи, 2004. 65 с.

10. Gubaidullin R. R., Agliullin T. A., Morozov O. G., Sahabutdinov A. Jh., Ivanov V. Microwave-Photonic Sensory Tire Control System Based on FBG // 2019 Systems of Signals Generating and Processing in the Field of on Board Communications – Moscow, 2019.

11. Gubaidullin R. R., Agliullin T. A., Morozov O. G., Sahabutdinov A. Jh., Ivanov V. Tire Strain Measurement System Based on Addressed FBG-Structures // 2019 Systems of Signals Generating and Processing in the Field of on Board Communications – Moscow, 2019.

12. Нуреев И. И. Постановка задач калибровки совмещенных датчиков давления и температуры // Нелинейный мир. 2015. Т. 13. № 8. С. 26–31.

Статья представлена профессором КНИТУ-КАИ,
доктором технических наук, профессором А. Ж. Сахабутдиновым.

УДК 621.311
ГРНТИ 50.43.19

ОСОБЕННОСТИ ПРИМЕНЕНИЯ ТЕХНОЛОГИЙ ИНТЕЛЛЕКТУАЛЬНЫХ СЕТЕЙ ДЛЯ ПОСТРОЕНИЯ ПОДСИСТЕМЫ НЕПРЕРЫВНОГО МОНИТОРИНГА СЕТИ ЭЛЕКТРОСНАБЖЕНИЯ МЕТРОПОЛИТЕНА

А. В. Давыдова

Петербургский государственный университет путей сообщения Императора Александра I

В статье приведено обоснование применения технологии интеллектуальных сетей для построения подсистемы непрерывного мониторинга сети электроснабжения метрополитена. Представлена характеристика технологии интеллектуальных сетей, подлежащей к применению. Представлены особенности работы многопараметрических комплексов сети электроснабжения метрополитена. Сформирована классификация диагностических параметров, характеристик оборудования и существующих систем для последующих контроля и расчетов.

сеть электроснабжения метрополитена, Smart grid, диагностические параметры, мониторинг.

Сеть электроснабжения метрополитена представляет собой большую сложную электротехническую систему, питающую оборудование разного уровня напряжения. На рис. 1 (см. ниже) представлена обобщенная структурная схема совмещенной тягово-понизительной подстанции (СТП).

Обеспечение надежности, бесперебойности и экономической целесообразности, стабильности энергоснабжения определяется децентрализацией, резервированием, секционированием, селективностью. В связи с этим на подстанции применяется большое количество оборудования, контроль параметров работы которых необходим для своевременного проведения обслуживания [1].

Контроль состояния объектов сети электроснабжения на данный момент формируют такие системы, как комплексная автоматизированная система диспетчерского управления, автоматическая система учета и анализа работы линий метрополитена, автоматизированная информационно-измерительная система коммерческого учета электроэнергии, комплексная система автоматизированного управления движением подъездов метрополитена, а также система регистрации технологических нарушений, реализованная на одной станции метрополитена как экспериментальная, и другие.

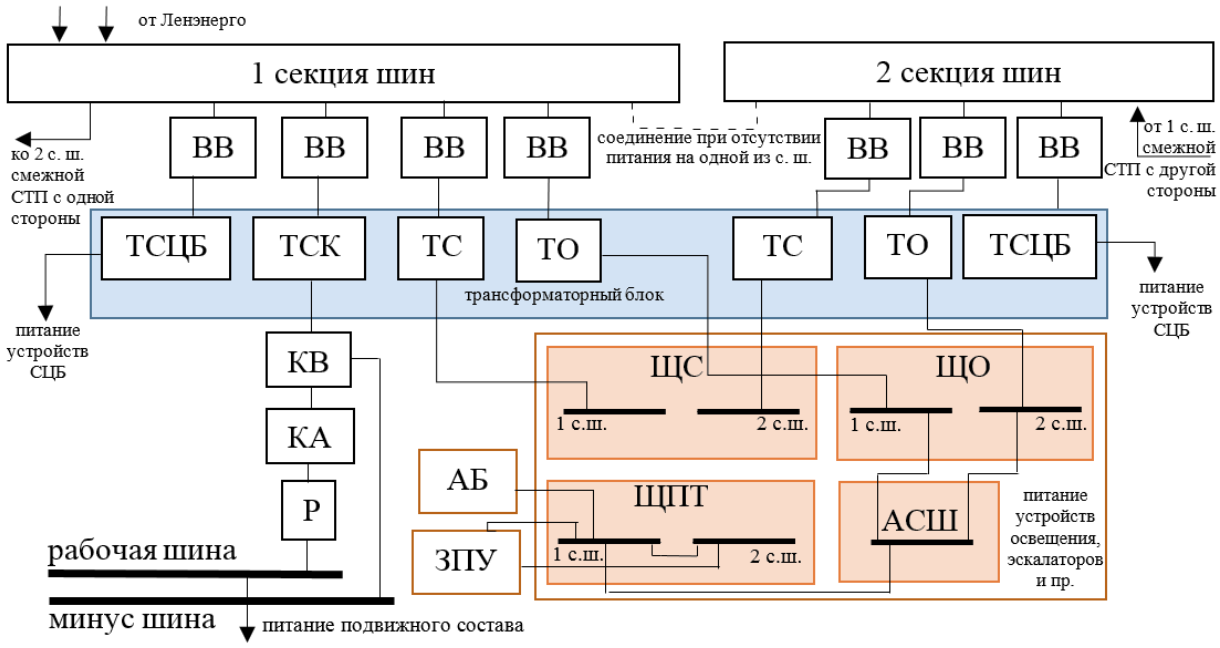


Рис. 1. Обобщенная структурная схема
совмещенной тягово-понизительной подстанции

Каждая из данных систем охватывает и анализирует неполный спектр параметров оборудования метрополитена, не взаимодействует с другими системами, в них отсутствует последующее использование полученной информации, помимо формирования отчетности. На рис. 2 представлены статистические данные посадки и пропажи напряжения за период 2017–2019 гг., которые влекут за собой нарушение работы освещения на станциях, остановку эскалаторов, перекрытие светофоров, отключение вентшахт и др.

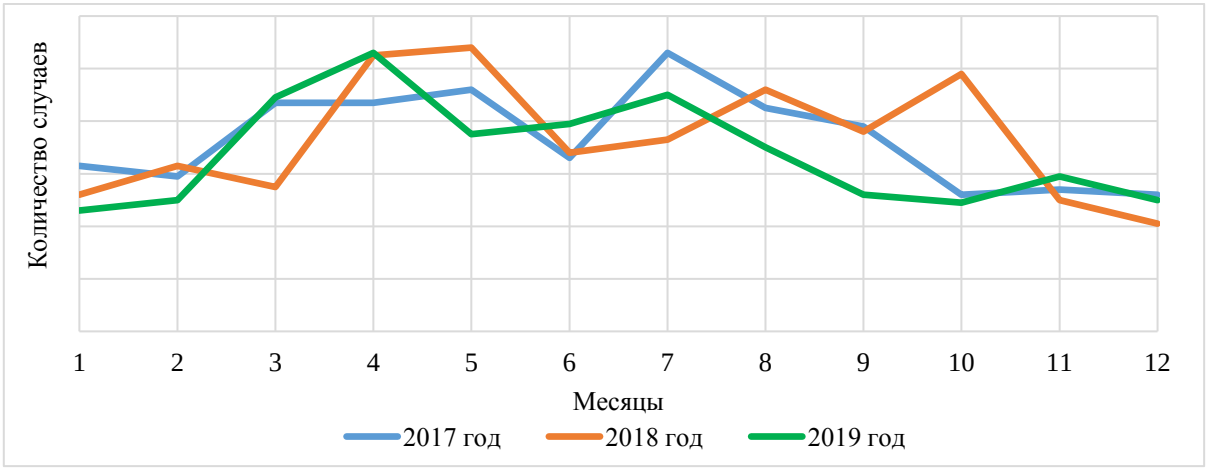


Рис. 2. Посадки и пропажи напряжения

К факторам, оказывающим влияние на уровень и стабильность напряжения в сети, относят такие как:

– переходные режимы работы и тип тягового привода подвижного состава;

– неравномерность потребления электроэнергии оборудованием;

– временной интервал (суточная нагрузка, праздничные дни и т. п.);

– аварийные отключения оборудования.

Осуществление мониторинга сети электроснабжения метрополитена с учетом влияния оборудования потребителей обеспечит комплексная система контроля. Для ее построения необходимо рассмотреть возможность применения интеллектуальной сети. К ней относится технология Smart grid, которая представляет собой концепцию полностью интегрированной, саморегулирующейся и самовосстанавливающейся электроэнергетической системы, имеющей сетевую топологию и включающей в себя все генерирующие источники, магистральные и распределительные сети, и все виды потребителей электрической энергии, управляемые единой сетью информационно-управляющих устройств и систем в режиме реального времени [2].

Технология Smart grid включает в себя следующее:

– измерительные приборы, фиксирующие режимные параметры оборудования;

– система сбора, передачи и обработки данных;

– исполнительные органы и механизмы для изменения топологических параметров сети и взаимодействия с другими объектами;

– средства автоматической оценки текущей ситуации и построения прогнозов работы сети;

– управляющая система общего информационного обмена.

На рис. 3 представлена трехуровневая система Smart grid [3].

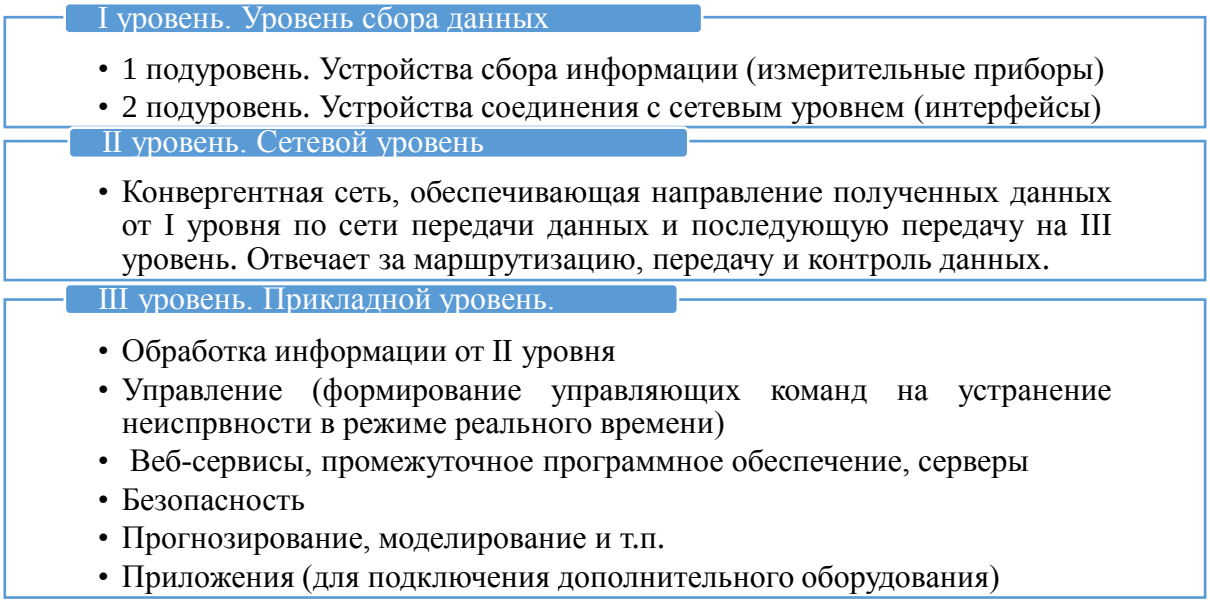


Рис. 3. Трехуровневая система Smart grid

Применительно к сети электроснабжения метрополитена, данная технология позволит осуществить, помимо уже реализованных в системах, следующие функции:

– определить границу работоспособности оборудования с фиксацией приближения параметра к границе области работоспособности;

– произвести переключения без вмешательства оператора;

– выявить возможные причины изменений параметров оборудования сети;

– сформировать, ранжировать и приоритезировать передаваемые управляющие воздействия и команды;

– осуществить контроль качества электроэнергии;

– установить/включить управляемые сетевые элементы, изменяющие параметры, топологию и конфигурацию сети по управляющему воздействию;

– построить прогноз изменения диагностического параметра;

– обеспечить поддержку принятия решения оператору.

Это ставит задачу по разработке моделей и методик эффективного функционирования и прогнозирования с учетом особенностей работы оборудования и применением, адаптацией положений технологии Smart grid.

Для построения начального уровня в таблице представлена информация, необходимая для определения состояния оборудования.

ТАБЛИЦА. Информация о состоянии оборудования

Наименование оборудования	Информация о состоянии оборудования	Наименование оборудования	Информация о состоянии оборудования
Ввод	Токи	Подвижной состав (ПС)	Пусковые токи
	Напряжения		Параметры двигателя
	Изменения токов и напряжений во времени		Тормозные потери
Трансформаторы СЦБ, ТС, ТО, ТН каждой секции шин	Напряжения обмоток		Удельный расход электроэнергии ПС
КП на смежные станции	Токи		Время переходного процесса (разгона, торможения)
Щиты рабочего и аварийного освещения по каждой секции шин	Напряжения		Средняя скорость движения на каждом участке
АБ	Напряжение		Пусковые потери
КВА	Напряжения		Среднее напряжение,

Наименование оборудования	Информация о состоянии оборудования	Наименование оборудования	Информация о состоянии оборудования
			подаваемое на тяговые двигатели
	Токи		Ток возбуждения
Эскалаторы	Двигатели главного и малого приводов:		Ток якоря
	– мощность		Тип привода ПС
	– токи		Время потребления тока ПС
	– напряжения		
	– частоты вращения		
Вентиляционные установки	Двигатели:	Осветительные устройства – на станциях – в тоннеле – на наземных путях	Освещенность на уровне пола и на уровне головки рельса
	– мощность		
	– токи		
	– напряжения		
	– частоты вращения		
	– суммарное паде-ние напряжения	Устройства СЦБ	Параметры путевых трансформаторов
Временной интервал	Суточная нагрузка		Напряжение питания аппаратуры СЦБ
	Календарные дни		Чувствительность аппаратуры рельсовых цепей к колебаниям напряжения и частоты
	Время года		

Заключение

1. Рассмотрены особенности работы многопараметрических комплексов сети электроснабжения метрополитена с обоснованием применения технологии интеллектуальных сетей для построения подсистемы мониторинга сети электроснабжения метрополитена.

2. Представлена характеристика технологии интеллектуальных сетей.

3. Сформирована классификация диагностических параметров, характеристик оборудования для построения первого уровня подсистемы мониторинга сети электроснабжения метрополитена.

4. Обозначено перспективное направление в части разработки моделей и методик эффективного функционирования и прогнозирования с учетом особенностей работы оборудования и применением, адаптацией положений технологии Smart grid.

Список используемых источников

1. Быков Е. И. Электроснабжение метрополитенов. Устройство, эксплуатация и проектирование. М. : Транспорт, 1977. 431 с.

2. Моржин Ю. И., Ядыкин И. Б., Бахтадзе Н. Н. Мультиагентная интеллектуальная иммунная система ИЭС ААС // Автоматизация в промышленности. Алгоритмическое и программное обеспечение: науч.-тех. журн. 2012. № 4. С. 61–64.

3. Yasir S., Mubashir H. R. Internet of Things-aided Smart Grid: Technologies, Architectures, Applications, Prototypes, and Future Research Directions [Электронный ресурс] // Архив электронных публикаций, 2019. URL: https://arxiv.org/abs/1704.08977v2 (дата обращения 20.01.2020).

Статья представлена научным руководителем, доктором технических наук, профессором А. К. Канаевым.

УДК 004.07
ГРНТИ 49.38.49

СТАНДАРТ БЕСПРОВОДНОЙ СЕТИ 802.11ax

Ю. С. Данилова, А. Л. Егорова, С. И. Штеренберг

Санкт-Петербургский государственный университет телекоммуникаций им. проф. М. А. Бонч-Бруевича

Стандарт 802.11ax – это следующая эволюция технологии беспроводной локальной сети. Он, как сообщается, на 30 % быстрее, чем 802.11ac, но скорость – не основное преимущество, которое рекламируют Wi-Fi Alliance и другие эксперты отрасли. Стандарт также обеспечивает меньшую задержку, большее количество одновременно доставляемых данных и повышенную энергоэффективность.

беспроводная сеть, Wi-Fi, стандарт, скорость передачи, точка доступа.

Методы, используемые в стандарте 802.11ax, уменьшают влияние помех и увеличивают пропускную способность в многолюдных городских и пригородных средах, уменьшая типичные проблемы, которые трудно устранить. Преимущества стандарта, по большей части, направленны на плотные корпоративные сети, которые требуют огромной пропускной способности и могут иметь десятки тысяч роуминговых и фиксированных клиентов Wi-Fi [1].

Чтобы объяснить преимущества 802.11ax, необходимо кратко остановиться на том, как работает Wi-Fi. В большинстве стран для использования в сетях, совместимых с Wi-Fi, выделено два блока частот: полоса 2,4 ГГц и полоса 5 ГГц. Эти полосы далее делятся на каналы, которые имеют задан-

ную начальную и конечную частоту. Десятки или сотни близко расположенных сетей могут бороться за один и тот же канал [2]. Отправители и получатели, такие как точка доступа и ноутбук, соглашаются использовать один и тот же канал для обмена данными.

Стандарт 802.11ax улучшает производительность в обоих диапазонах спектра и потенциально обеспечивает несколько гигабит в секунду пропускной способности для десятков устройств, одновременно работающих в одном канале.

Краткое описание преимуществ 802.11ax

Более плотное кодирование данных. Wi-Fi кодирует данные в радиоволны, для которых существуют расчетные пределы для количества данных, переданных на конкретной частоте. Качество передачи данных по Wi-Fi зависит от квадратурной амплитудной модуляции (*quadrature amplitude modulation*, QAM) – она определяет количество информации, которую можно передать одним сигналом. Стандарт 802.11ac смог кодировать на 33 % больше (256-QAM) данных, чем 802.11n в той же ширине спектра [3]. Стандарт 802.11ax увеличивает это еще на 25 % (1024-QAM) (рис. 1).

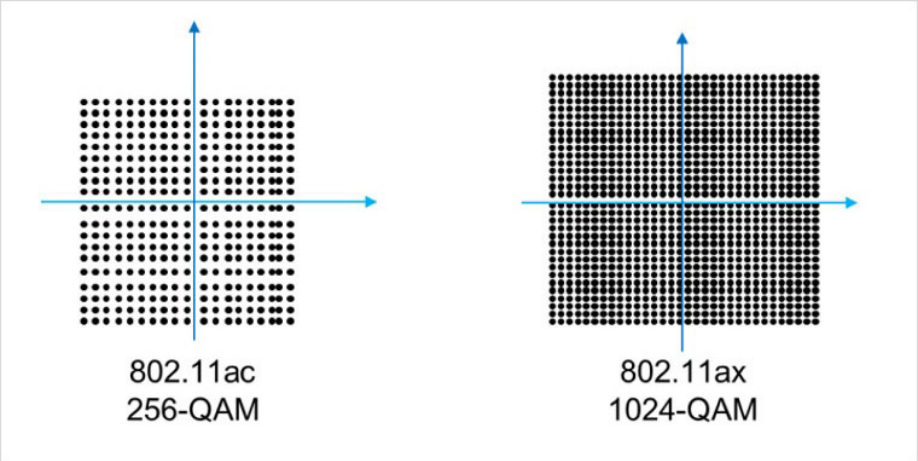


Рис. 1. Квадратурные амплитудные модуляции 256 и 1024

Возврат в диапазон 2,4 ГГц. С появлением 802.11ax осуществлен возврат в диапазон 2,4 ГГц. Ранее, в 802.11ac данный диапазон не поддерживался, но, в конечном итоге, разработчики IEEE поняли, что 5-гигагерцовый диапазон имеет свои недостатки, и в частности, малый радиус действия. Стандарт 802.11ax является первым стандартом за более чем десятилетие, который улучшает производительность на частоте 2,4 ГГц, используя преимущества более длинных волн, по сравнению с 5 ГГц. Более длинные волны лучше проникают в твердые объекты, такие как стены, полы и мебель.

Данное преимущество особенно полезно для mesh-сетей, в которых у узлов обычно есть две радиостанции, одна для 2,4 ГГц, другая для 5 ГГц [4]. Mesh-сеть с 802.11ax, с гораздо более высокими скоростями передачи данных в диапазоне 2,4 ГГц, приводит к лучшей пропускной способности по всей сети.

Многопользовательский MIMO на прием и передачу. Стандарт 802.11n добавил технологию пространственного мультиплексирования, известную как MIMO (множественный вход, множественный выход). MIMO – это средство отправки нескольких потоков данных по разным физическим каналам.

Начиная с 802.11ac, маршрутизаторы получили возможность одновременно общаться с различными устройствами (многопользовательскими или MU-MIMO). В свою очередь, клиентские устройства также смогли одновременно отвечать [5]. Это чрезвычайно важно для потоковых медиаплееров. В 802.11ac технология MIMO позволяла транслировать данные четырем клиентам с помощью разных поднесущих. В 802.11ax число возможных подключений устройств увеличили в два раза – до восьми. Но это преимущество только для дорогого оборудования предприятий, не для домашних устройств.

Субканалы. Технология OFDMA (множественный доступ с ортогональным частотным разделением каналов) позволяет разбить канал Wi-Fi с помощью быстрого преобразования Фурье на несколько тысяч, тесно расположенных, «поднесущих» или подканалов и объединить их в группы, называемые «ресурсными единицами», для обработки отдельных потоков данных (рис. 2, см. ниже). Помехи или шум в одном подканале изолированы от остальных. Это позволяет синхронно транслировать данные сразу нескольким клиентам по стандарту 802.11ax с усредненной скоростью, уменьшая необходимость повторной передачи данных. Стоит учитывать, что все эти клиенты должны обязательно поддерживать стандарт 802.11ax.

Если клиент один, точка доступа отдаст ему весь канал, но как только в сети появятся новые клиенты, пропускная способность канала будет перераспределена между ними. Передача данных может осуществляться на тех поднесущих, которые для данного пользователя наименее подвержены частотно-селективной интерференции. Для выбора таких поднесущих каждая точка доступа отправляет отчеты о качестве передачи с использованием разных поднесущих.

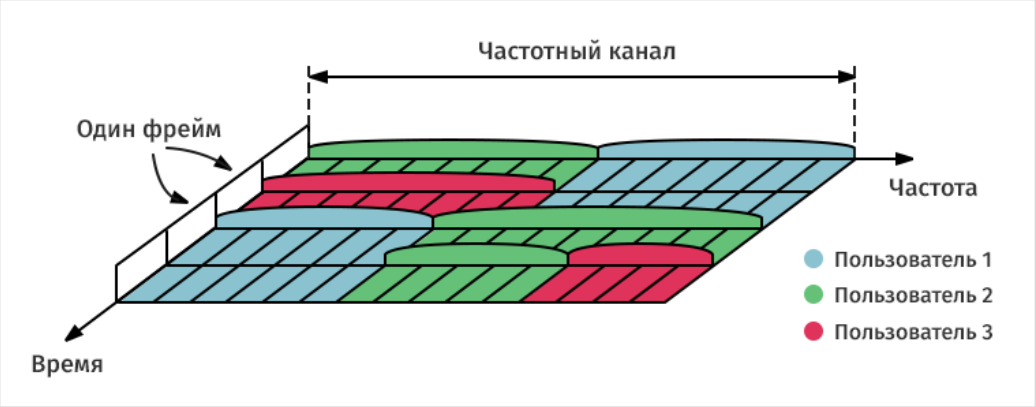


Рис. 2. Технология OFDMA оптимизированная для множества пользователей сети

Лучшая дискриминация других сетей. Во многих городах и пригородах десятки и сотни сетей Wi-Fi пересекаются. Стандарт 802.11ax включает метод, позволяющий стандарту различать сети и слабо принятые сигналы от других сетей, что, в свою очередь, обеспечивает большую пропускную способность [6]. Данный метод заключается в механизме «раскрашивания» (а точнее, маркировки) пакетов в одних и тех же частотных каналах, используемых разными устройствами – BSS coloring (рис. 3). При таком раскладе, обнаружив пакет с «чужим» кодом, устройство проигнорирует его. Помочь процедуре должно автоматическое регулирование порогов обнаружения сигнала для «своих» и «чужих», а также усовершенствование механизма фокусировки передачи в направлении клиентских устройств.

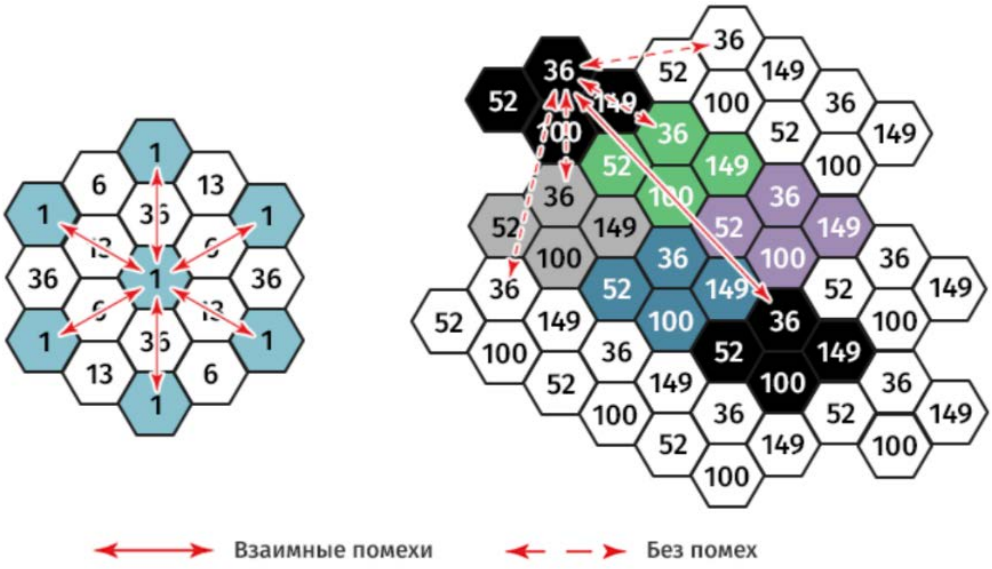


Рис. 3. Перегрузка BSS в одном канале и перегрузка точек BSS только одного «цвета»

Улучшенная производительность батареи клиента. Еще одно преимущество – функция Target Wake Time. Она позволит сетевым клиентским устройствам переходить в режим сна и «просыпаться» по расписанию. Если

гаджет не передает данные в конкретный промежуток времени, его Wi-Fi-переходит в спящий режим, чтобы экономить электроэнергию. Это может значительно снизить энергопотребление, связанное с Wi-Fi, и продлить срок службы батареи [7].

Исходя из указанных выше преимуществ стандарта 802.11ax, данная технология будет полезна при развертывании Wi-Fi-сетей с высокой плотностью. Отдельные решения, например, MU-MIMO и OFDMA, улучшат качество связи в общественных местах, корпоративных сетях, ресторанах, гостиницах и торговых залах.

Обратная совместимость - это всегда забота о новом поколении оборудования. Но история Wi-Fi во многом относилась к предыдущим стандартам без особых компромиссов. Точки доступа, которые объявили себя поддерживающими 802.11ax, также будут беспрепятственно обрабатывать все предыдущие стандарты 802.11, и, наоборот, 802.11g, первая версия, поддерживает более современные методы обеспечения безопасности сети [8]. К 2020-му году стандарт 802.11ax появился в сотнях миллионов новых устройств, но пройдет еще два-три года, прежде чем человечество сможет в полной мере воспользоваться и оценить преимущества новой технологии.

Список используемых источников

1. Григорьев В. А., Никитин В. Н., Кузнецов В. И., Тараканов С. А., Ковцур М. М. Анализ пропускной способности сети радиосвязи стандарта IEEE 1609 // Электросвязь. 2014. № 1. С. 13–15.

2. Красов А. В., Косов Н. А., Холоденко В. Ю. Исследование методов провижининга безопасности сети на мультивендорном оборудовании с использованием средств автоматизированной конфигурации // Colloquium-journal. 2019. № 13–2 (37). С. 243–247.

3. Сахаров Д. В., Штеренберг С. И., Левин М. В., Колесникова Ю. А. Разработка модели обеспечения отказоустойчивости сети передачи данных // Известия высших учебных заведений. Технология легкой промышленности. 2016. Т. 34. № 4. С. 14–20.

4. Красов А. В., Петрив Р. Б., Сахаров Д. В., Сторожук Н. Л., Ушаков И. А. Масштабируемое honeypot-решение для обеспечения безопасности в корпоративных сетях // Труды учебных заведений связи. 2019. Т. 5. № 3. С. 86–97.

5. Душин С. Е., Красов А. В., Кузьмин Н. Н. Моделирование систем управления : учеб. пособие / Под ред. С. Е. Душина. М., 2012.

6. Исаченков П. А., Красов А. В., Левин М. В. Исследование эффективности метода управления потоками трафика на основе информации о нагрузке в программно-определяемой сети с неравными метриками маршрутов // Современная наука и инновации. 2017. № 2 (18). С. 32–38.

7. Билятдинов К. З., Красов А. В., Меняйло В. В., Пешков А. И., Карпов А. Н. Теория информационных процессов и систем; учеб. изд., Санкт-Петербург, 2019.

8. Билятдинов К. З., Красов А. В., Меняйло В. В. Исследование систем и анализ результатов испытаний : учеб. пособие. СПб.: СПбГУТ, 2019.

УДК 003.26.09
ГРНТИ 81.93.29

СТЕГОСИСТЕМА ДЛЯ ИЗОБРАЖЕНИЙ ПРИ КОНТУРНОМ ВЛОЖЕНИИ И ОБНАРУЖЕНИИ С ИСПОЛЬЗОВАНИЕМ NIST-ТЕСТОВ

А. В. Даньшина, В. И. Коржик, З. К. Нгуен

Санкт-Петербургский государственный университет телекоммуникаций им. проф. М. А. Бонч-Бруевича

В данной статье представлена одна из современных стегосистем, реализованная с помощью контурного вложения сообщений, зашифрованных стойким шифром. Вложение информации в контур изображения обеспечивает лучшую защищенность от визуального обнаружения, по сравнению с вложением в "сглаженные" области. Поэтому в контур изображения можно вложить больший объем информации. Проверено, как влияет на качество изображения погружение информации в контур. Предложен метод обнаружения СГ-К, основанный на проверке псевдослучайности извлекаемой криптограммы

стегосистема, стегоанализ, контурное вложение, NIST-тесты.

Наиболее популярными методами скрытия данных в изображениях являются: метод погружения в наименьшие значащие биты (НЗБ) [1] и метод погружения информации в контуры изображения. Второй метод вложения обеспечивает лучшую защищенность, как минимум, от визуального обнаружения. На рис. 1 представлена структура контурного погружения информации.

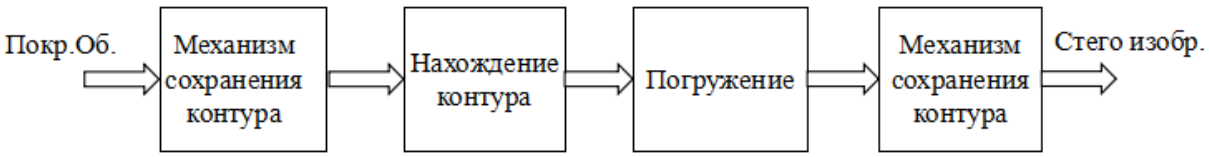


Рис. 1. Общая схема контурного погружения

На первой стадии представленной схемы производится обнаружение контура. Это можно сделать с помощью одного из известных методов: Кэнни [2], Робертса [2], Собеля [3], Прюитт [4], IVIF (*Interval-valued intuitionistic fuzzy*) [5, 6] и т. д. На второй стадии выполняется контроль за тем, чтобы обнаруженный контур не изменился после погружения. Это необходимо для того, чтобы пиксели, лежащие на контуре до и после погружения, были одинаковыми.

При погружении информации применяется механизм, который можно назвать расширенным НЗБ, поскольку в каждый пиксель, лежащий на контуре, вкладывается не один (как в простом НЗБ), а несколько бит секретной информации.

Далее представлена формула, по которой происходит вложение информации:

$$y' = y \oplus_k m,$$

где y – значения пикселя ПО, m – зашифрованное сообщение, y' – полученное значение стего-пикселя после вложения бит, $\oplus_k$ – оператор замещения, а значение k (количество вложенных бит) отличается для контурных пикселей (k_e) от значений для гладких пикселей (k_s), где k_e больше, чем k_s.

После вложения информации её необходимо извлечь, что можно выполнить с помощью формулы:

$$m' = k\text{НЗБ}(y').$$

Иллюстрация данного метода представлена ниже (рис. 2–2.4, см. ниже).

Для оценки качества изображения после вложения, удобно использовать метрику Peak Signal to Noise Ratio (PSNR) (в ДБ) [7]. Данная метрика обычно применяется для оценки качества компрессии изображения. Значение PSNR, рассчитанное для 10 стегоизображений СГ-К, приведены в таблице 1 (см ниже).

Очевидно, чем больше значение PSNR, тем лучше оказывается качество изображения. Из таблицы 1 видно, что при малых k, качество изображения СГ-К лучше, однако, при этом, скорость вложения меньше.

Рис. 2. Покрывающее изображение

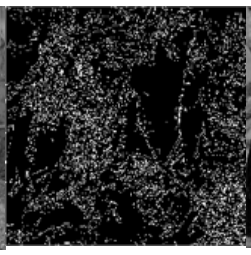


Рис. 2.1. Контуры покрывающего изображения

Рис. 2.2. Стегоизображение

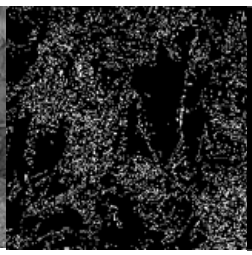


Рис. 2.3. Контуры стегоизображения

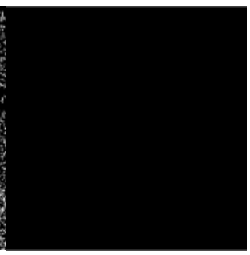


Рис. 2.4. Различие между контурами изображений

Из рис. 2–2.4, можно сделать вывод, что контур до и после вложения информации не изменился и, следовательно, с помощью визуальной атаки, обнаружить стегосистему будет достаточно сложно.

ТАБЛИЦА 1. Значения PSNR 10 стего-изображений СГ-К

Вложенные параметры СГ-К	PSNR значение									
	Изоб. 1	Изоб. 2	Изоб. 3	Изоб. 4	Изоб. 5	Изоб. 6	Изоб. 7	Изоб. 8	Изоб. 9	Изоб. 10
k_e =3, k_s =2	40.75631	40.01210	40.63794	40.77199	40.73204	40.71585	40.83036	40.73570	40.36467	40.73244
k_e =2, k_s =1	48.84909	47.98348	48.91472	49.01596	48.96839	49.04740	49.27447	49.07954	48.48274	48.89644

Однако, такую СГ все же можно обнаружить с помощью стегоанализа на основе использования NIST-тестов [8]. Такой стегоанализ не требует знания алгоритма погружения информации в покрывающий объект и изучения статистики покрывающего объекта, а требует лишь знания (или умения найти) алгоритма извлечения информации. Если известен алгоритм извлечения информации из некоторой «предполагаемой» стегосистемы, то она должна представлять собой стеганограмму, удовлетворяющую всем проверкам на псевдослучайность. Техника такой проверки – это 15 NIST-тестов [9], представленных в таблице 2.

Алгоритм обнаружения состоит в следующем: сначала происходит извлечение бит предполагаемой криптограммы, далее производится анализ извлечённой двоичной последовательности при помощи NIST-тестов. Если будут пройдены все (или почти все) тесты, то принимается решение о том, что присутствует стеганограмма.

ТАБЛИЦА 2. Перечень NIST-тестов

№ Теста	Название теста
1	The frequency test
2	Frequency test within a block
3	The runs test
4	Tests for the longest-run-of-ones in a block
5	The binary matrix rank test
6	The discrete Fourier transform (spectral) test
7	The non-overlapping template matching test
8	The overlapping template matching test
9	Maurer’s “Universal Statistical” test

№ Теста	Название теста
10	The linear complexity test
11	The serial test
12	The approximate entropy test
13	The cumulative sums (cusums) test
14	The random excursion test
15	The random excursions variant test

Далее был проведён такой стегоанализ.

В эксперименте выбраны следующие параметры: $k_e = 3; k_s = 2$. А для шифрования использовался стойкий шифр AES-128 [10]. В таблице 3 (см. ниже) представлены результаты NIST-тестирования для 15 различных последовательностей, выделенных из СГ изображений при контурном вложении.

Из таблицы 3 видно, что все из СГ изображений прошли почти все NIST-тесты. В таблице 4 (см. ниже) представлены результаты NIST-тестирования для покрывающего объекта (ПО) без каких-либо вложений.

Можно заметить, что таблица 4 содержит значительно больше ячеек белого цвета, чем таблица 3. Это означает, что при оптимально выбранном пороге, равному в данном случае 12, как показали результаты дополнительного эксперимента для 1000 различных ПО и СГ, вероятность ошибочной классификации (ПО/СГ) оказалось равной 7,3 %, что можно считать приемлемым результатом.

ТАБЛИЦА 3. Результаты NIST-тестирования для 15 различных изображений, извлеченных из СГ для изображений при контурном вложении (серый цвет – прохождение теста, белый – не прохождение)

№ послед. / Тест	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15
1															
2															
3															
4															
5															
6															
7															
8															
9															
10															
11															

№ послед. / Тест	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15
12	■	■	■	■	■	■	■	■	■	■	■	■	■	■	■
13	■	■	■	■	■	■	■	■	■		■	■	■	■	■
14	■		■		■		■	■		■	■	■	■	■	■
15	■		■		■		■	■		■	■	■	■	■	■

ТАБЛИЦА 4. Результаты NIST-тестирования для 15 различных последовательностей, извлеченных из ПО (серый цвет – прохождение теста, белый – не прохождение)

№ послед. / Тест	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15
1	■	■		■			■	■	■			■		■	
2						■									
3				■		■			■						
4									■					■	
5		■	■	■	■		■	■	■	■	■	■	■	■	
6	■	■	■		■	■	■	■		■	■	■		■	
7		■	■			■			■						
8						■			■						
9		■										■		■	
10	■	■	■	■	■	■	■	■		■	■	■	■	■	■
11						■			■			■			
12									■					■	
13	■	■		■		■	■		■			■		■	
14				■						■	■	■			
15	■		■	■			■			■	■	■		■	

Таким образом, в статье был исследован метод погружения информации в контур изображения, при использовании которого в изображение можно поместить больше информации, чем в «сглаженные» области, при этом, визуальное обнаружение вложения оказывается практически невозможным, так как края изображения не изменяются. Однако, как показано в статье, данный метод СГ все же можно обнаружить при помощи стегоанализа, основанного на NIST-тестах.

Список используемых источников

1. Коржик В. И., Небаева К. А., Герлинг Е. Ю., Догиль П. С., Федянин И. А. Цифровая стеганография и цифровые водяные знаки. Часть 1. Цифровая стеганография / Под общ. ред. проф. В. И. Коржика. СПб.: СПбГУТ, 2016. 226 с. ISBN 978-5-89160-125-3.

2. Canny J. A computational approach to edge detection // IEEE Transactions on pattern analysis and machine intelligence. 1986. N. 6. P. 679–698.

3. Kanopoulos N., Vasanthavada N., Baker R. L. Design of an image edge detection filter using the Sobel operator // IEEE Journal of solid-state circuits. 1988. N 23 (2). P. 358–367.

4. Seif A., Salut M. M., Marsono M. N. A hardware architecture of Prewitt edge detection // 2010 IEEE Conference on Sustainable Utilization and Development in Engineering and Technology. IEEE, Petaling Jaya, Malaysia, 2010. P. 99–101.

5. Afsari F., Eslami E., Eslami P. Interval-valued intuitionistic fuzzy generators: Application to edge detection // Journal of Intelligent & Fuzzy Systems. 2014. N 27 (3). P. 1309–1324.

6. Dadgostar H., Afsari F. Image steganography based on interval-valued intuitionistic fuzzy edge detection and modified LSB // Journal of information security and applications. 2016. N 30. P. 94–104.

7. Fridrich J. Steganography in digital media: principles, algorithms, and applications. Cambridge University Press, Cambridge, England, 2009. 462 p. ISBN-13: 978-0521190190.

8. Korzhik V., Fedyanin I., Godlewski A., Morales-Luna G. Steganalysis based on statistical properties of the encrypted messages // International Conference on Mathematical Methods, Models, and Architectures for Computer Network Security. Lecture Notes in Computer Science, vol 10446. Warsaw, Poland, 28-30 August 2017. P. 288–298.

9. Bassham III L. E., Rukhin A. L., Soto J., Nechvatal J. R., Smid M. E., Barker E. B., Leigh S.D., Levenson M., Vangel M., Banks D.L., Heckert N.A., Dray J.F., Vo S. Sp 800–22 rev. 1a. a statistical test suite for random and pseudorandom number generators for cryptographic applications // National Institute of Standards and Technology. 2010. 131 p. URL: https://www.nist.gov/publications/statistical-test-suite-random-and-pseudorandom-number-generators-cryptographic (дата обращения 26.02.2020).

10. Коржик В. И., Яковлев В. А. Основы криптографии : учеб. пособие. 1-е изд. СПб. : ИЦ Интермедия, 2016. 296 с.

УДК 004.056
ГРНТИ 50.01.29

МОДЕЛИРОВАНИЕ АТАКУЮЩИХ ВОЗДЕЙСТВИЙ В БЕСПРОВОДНЫХ САМООРГАНИЗУЮЩИХСЯ СЕНСОРНЫХ СЕТЯХ

В. А. Десницкий[1,2], А. В. Мелешко[1]

[1]Санкт-Петербургский институт информатики и автоматизации Российской академии наук
[2]Санкт-Петербургский государственный университет телекоммуникаций им. проф. М. А. Бонч-Бруевича

В настоящее время все большее развитие и распространение в различных сферах применения получают беспроводные самоорганизующиеся сенсорные сети. Такие сети применяются для сбора и агрегации данных от физических сенсоров устройств, а также их обработки и передачи по сети в условиях, изменяющихся во времени харак-

теристик загрузки коммуникационных каналов связи, местоположения устройств и режимов их работы. В работе раскрывается подход к моделированию и анализу атакующих воздействий, учитывающие, в том числе, характер самоорганизации таких систем.

беспроводная сенсорная сеть, самоорганизация, информационная безопасность.

Беспроводные сенсорные сети (БСС) в последнее время получают все большее распространение в различных сферах жизнедеятельности человека, например, в промышленности, сельском хозяйстве, безопасности, транспорте и других сферах. Наличие функций самоорганизации предоставляют дополнительные возможности нарушителю выполнять несанкционированные действия под видом легитимных физических и логических перестроений сети, таких как отключение узла от сети, динамическое добавление нового узла, перестроение топологии сети, изменение маршрутов пересылки данных.

В отечественной и зарубежной литературе имеется множество работ, посвященных безопасности БСС, в которых описываются возможные атаки на сеть, их ранжирование по уровням сетевого взаимодействия, требования к безопасности, протоколы передачи данных. При этом вопросы моделирования атак, эксплуатирующих самоорганизацию сенсорных сетей в современной научно-технической литературе освещены в недостаточной степени.

В статье [1] рассматриваются вопросы безопасности беспроводных сетей, состоящих из небольших датчиков с ограниченными ресурсами для передачи, сбора, и хранения данных в различных приложениях. Авторы разделяют атаки по трем основным категориям: конфиденциальности – данные не должны быть нелегитимно получены третьими лицами; доступности – узлы должны быть всегда доступны; целостности – данные сети не должны быть нелегитимно модифицированы.

В статье [2] раскрываются проблемы, с которыми можно столкнуться в процессе обеспечения безопасности БСС, в том числе ограниченность вычислительных ресурсов узлов БСС, ограниченная мощность приемо-передающих устройств. С ограничением ресурсов необходимо уделить внимание надежности передачи данных, свежести данных, аутентификации узлов, конфиденциальности, целостности и др. Помимо этого в этой статье также дается представление атак на различных уровнях функционирования БСС и приведена таблица с описанием контрмер для предотвращения перечисленных видов атак [2].

Yang и др. описывают типовые угрозы безопасности БСС, узлы которых размещаются под водой для выполнения специфичных прикладных задач [3]. Описывается структура подводной БСС, в которой часть сенсоров находится под водой на некоторой глубине, и они передают данные

на маяк – буй, который, в свою очередь, может передать их далее по беспроводному каналу связи. В случае подводной БСС добавляется также акустический канал связи. Из особенностей подводных БСС можно выделить: ненадежность канала связи, окружающий шум и потери при передаче в водной среде, многолучевое распространение и выраженный эффект Доплера.

Kumar и др. рассматривают проблемы безопасности подводной БСС [4]. Описаны различные архитектуры построения подводных БСС, такие как 1D-UWSN архитектура, 2D-UWSN архитектура, 3D-UWSN архитектура, 4D-UWSN архитектура. Эти архитектуры отличаются количеством уровней сенсоров, ограничением их перемещения в пространстве, а также возможностью каждого узла быть концентратором.

Grover и Sharma отмечают разноплановость и техническую сложность проблемы обеспечения безопасности беспроводной сенсорной сети, в особенности в условиях решения вопросов экономии её энергопотребления [5]. В это статье раскрываются следующие виды атак: Wormhole, HelloFlood, Селективные атаки, Sybil-атаки, атаки типа Sinkhole. Целью Wormhole-атаки является убедить отправителя и получателя узлов, что они расположены на расстоянии одного или двух хопов друг от друга, но фактическое расстояние между ними много больше, возможно, даже вне диапазона подсети. Атака HelloFlood направлена на перегрузку сети и, как следствие, в том числе, уменьшение энергии узлов. В селективных атаках злонамеренный узел прерывает процесс коммутации. При этом атакующий узел по сути отбирает полученные пакеты, и другие узлы начинают искать альтернативные маршруты в сети. В Sybil-атаках узел подключается только к заражённым Sybil-узлам. Атаки типа Sinkhole заключаются в том, что узлы передают данные только через зараженный узел, предполагая, что это кротчайший путь. То есть весь трафик идет через Sinkhole-узел. Кроме того, в этой статье исследуются существующие защищенные протоколы, используемые в БСС, такие как SPIN (обеспечивает конфиденциальность, аутентификацию и целостность), LEAP, TINYSEC (облегченный протокол, поддерживает целостность, конфиденциальность и аутентификацию), ZigBee, и проводят их сравнительный анализ [5].

Gehi и Jain исследуют вопросы конфиденциальности пересылаемых данных в самоорганизующейся БСС, в том числе вопросы безопасного распределения ключей и добавление новых узлов в сеть [6]. Вместе с тем, авторы демонстрируют высокозащищенную структурированную и иерархически организованную (древовидную) самоорганизующуюся БСС с возможностью автоматического добавления нового беспроводного узла. Базовый узел, который является корневым узлом дерева, добавляет и удаляет инициализацию всех узлов, а также проводит генерацию отдельных закрытых ключей для каждого узла, располагающегося под ним, в рамках реализуемой иерархии. Авторы продемонстрировали результаты

моделирования процессов функционирования данной БСС в программном средстве MATLAB, в том числе, добавление узлов, а также генерацию и распределение ключей шифрования между узлами.

Kalita и Kar предложили безопасную схему защищенной передачи данных в БСС [7]. Предложенная схема является схемой инфраструктуры открытых ключей без использования сертификатов, в которой открытый ключ каждого узла изначально не известен новому узлу. Вместо этого только после успешного добавления нового узла ему передаются открытые ключи доверенного узла и базовой станции. Собственно, защита обеспечивается путем шифрования данных на транспортном уровне с помощью открытого ключа получателя, а аутентификация заголовка сетевого уровня защищается с применением функции хеширования на основе секретного ключа отправителя. Результаты моделирования показали, что, несмотря на значительное повышение уровня защищенности, в сравнении с передачей данных в открытом виде, применение этого подхода к защищенной передаче данных негативно сказывается на энергопотреблении узлов сети.

Предложенный в настоящей работе подход к построению модели атакующего состоит в следующем: на основе анализа спецификаций БСС строится матрица релевантных категорий атакующего [8] и анализируется возможность выполнения тех или иных действий атакующего. Исходя из специфики конкретной сети, имеющегося функционала и ограничений на действия пользователей, возможно значительно сократить набор признаков. Каждая ячейка матрицы представляет собой некоторую категорию злоумышленника с фиксированными значениями признаков, таких как тип доступа нарушителя к элементам БСС, локация атакующего, вид возможной атаки (активная или пассивная) и др.

Определим следующие типы атак на БСС, эксплуатирующие свойства ее самоорганизации.

Тип 1. За счет динамического перестроения сети атакующий узел или несколько узлов способны вклиниться в сеть для того, чтобы все или часть маршрутов доставки данных и служебных команд в сети проходили через атакующий узел (атака типа *man-in-the-middle*). В результате атакующий оказывается способен прослушивать, модифицировать передаваемые данные, отправлять команды на перестроение сети и др.

Тип 2. Атака подмены или модификации узла сети (*tampering*-атака, атака типа *man-in-the-end*), при которой легитимная возможность временного отсоединения узла эксплуатируется нарушителем для обеспечения перестроения топологии сети с целью модификации или подмены атакуемого узла.

Тип 3. Разновидность атаки типа 2, при которой атакующий принудительно отключает узел от сети под видом ее легитимной модификации.

При этом целью нарушителя может быть, как нарушение выполнения бизнес-задач атакуемого узла, так и нарушение связности и процессов маршрутизации сети в условиях работы атакуемого узла в роли узла-маршрутизатора сети.

Тип 4. Атака несанкционированно инициированного перестроения БСС, имеющее цели повышения расхода энергоресурсов, вычислительных ресурсов сети, а также воздействия на коллаборативные функции взаимодействия узлов сети и принятия коллективных решений в контексте решения им определенных бизнес-задач, таких как задачи выборочного мониторинга и поиска физических объектов на местности или в водном пространстве.

Для решения задач моделирования самоорганизующихся БСС и атак на них используются методы моделирования, включающее аналитическое, имитационное и натурное моделирование. Аналитическое моделирование используется для построения модели атакующего и анализа его возможностей и ограничений. Фактически, проводится верификация моделей представления [9] беспроводной сенсорной сети на предмет выполнимости условий осуществления атакующих воздействий возможным нарушителем информационной безопасности сети. Такая верификация направлена проверку всех возможных категорий нарушителя для определения критичности атаки и условий ее выполнения.

Натурное моделирование позволяет провести реализацию возможных атак на имеющемся программно-аппаратном прототипе БСС. По сути, прототип является упрощенной реализацией БСС, функционирующей в рамках модельных условий и допущений, и базируется на беспроводных коммуникационных модулях DigiXBee s2 и микроконтроллерах Arduino. Подобное моделирование применяется для атак, моделирование которых не требует наличия большого числа узлов и вычислительных ресурсов.

В рамках имитационного моделирования, БСС моделируется при помощи специализированных программных средствах, таких как OMNeT++, NS-2, JSim и др.Такое моделирование применяется для моделирования атак, повышенная сложность которых препятствует натурному модулированию таких атак, как, например, DDoS-атаки или определенные виды атак истощения энергоресурсов.

В работе предложен подход к моделированию атакующих воздействий в беспроводных сенсорных сетях на основе комбинирования принципов аналитического, натурного и имитационного моделирования. Проведен анализ возможных видов атак, которые используют свойства самоорганизации узлов сети. В дальнейшем планируются оценка показателей сложности и эффективности конкретных видов атакующих воздействий, а также разработка средств выявления аномальных данных от сенсоров БСС с использованием методов искусственного интеллекта.

Работа выполнена при финансовой поддержке гранта Российского Фонда Фундаментальных Исследований (РФФИ) № 19-07-00953.

Список используемых источников

1. Khan M. A., Khan M. Review on Security Attacks and Solution in Wireless Sensor Networks // American Journal of Computer Science and Information Technology. 2019. Vol. 7. No. 1:31. PP. 1–7.
2. Vikhyath K. B., Brahmanand S. H. Wireless sensor networks security issues and challenges: a survey // International Journal of Engineering & Technology. 2018. Vol. 7. PP. 89–94.
3. Yang G., Dai L., Wei Z. Challenges, Threats, Security Issues and New Trends of Underwater Wireless Sensor Networks // Sensors. MDPI. 2018. Vol. 18. PP. 1–26.
4. Kumar S., Kumari B., Chawla H. Security Challenges and Application for Underwater Wireless Sensor Network // Kalpa Publications in Engineering. 2018. Vol. 2. PP. 15–21.
5. Grover J., Sharma S. Security Issues in Wireless Sensor Network – A Review // 5th International Conference on Reliability. Infocom Technologies and Optimization (ICRITO). 2016. PP. 397–404.
6. Gehi S., Jain R. Self Organizing Secure WSN for IOT Implementation // International Journal of New Technology and Research (IJNTR). 2019. Vol. 5. Issue 7. PP. 112–117.
7. Kalita H. H., Kar A. A new algorithm for end-to-end security of data in a secure self-organized wireless sensor network // Journal of Global Research in Computer Science. 2010. Vol. 1. PP. 28–34.
8. Десницкий В. А., Чечулин А. А. Обобщенная модель нарушителя и верификация информационно-телекоммуникационных систем со встроенными устройствами // Технические науки – от теории к практике. 2014. № 39. С. 7–21.
9. Desnitsky V., Kotenko I., Chechulin A. An abstract model for embedded systems and intruders. Proceedings of 19th International Euromicro Conference on Parallel, Distributed, and Network-Based Processing (PDP 2011). Ayia Napa, 2011. PP. 25–26.

УДК 004.056.5
ГРНТИ 81.93.29

ОБОБЩЕННЫЙ АЛГОРИТМ АНАЛИЗА ЗАЩИЩЕННОСТИ БЕСПРОВОДНЫХ СЕНСОРНЫХ СЕТЕЙ ОТ АТАКУЮЩИХ ВОЗДЕЙСТВИЙ

В. А. Десницкий[1,2], И. Б. Паращук[2,3]

[1]Санкт-Петербургский государственный университет телекоммуникаций им. проф. М. А. Бонч-Бруевича
[2]Санкт-Петербургский институт информатики и автоматизации Российской академии наук
[3]Национальный исследовательский университет ИТМО

Рассматривается подход к формулировке и содержательной оценке этапов обобщенного алгоритма анализа защищенности беспроводных сенсорных сетей от атакую-

щих воздействий. Алгоритм включает этапы моделирования процессов функционирования беспроводных сенсорных сетей и поведения нарушителя, способного применять многошаговые атакующие воздействия, как физического, так и программно-информационного характера. Алгоритм призван повысить достоверность и оперативность анализа защищенности сетей такого класса, его ключевые этапы используют современные принципы обработки данных и событий информационной безопасности на основе технологии Больших Данных и нейронных сетей.

беспроводная сенсорная сеть, защищенность, воздействие, данные, угроза, анализ, моделирование, нарушитель, ресурс.

К перечню приоритетных направлений развития науки, технологий и техники Российской Федерации, безусловно, относятся беспроводные сенсорные сети (БСС) и проблемы их защищенности.

Это объективно обусловлено повышением роли и стремительным распространением БСС, возрастанием совокупной стоимости активов устройств, программного обеспечения и критически важных данных, циркулирующих в сетях такого класса, а также ростом числа уязвимостей и атакующих воздействий на них. Все это, вне всяких сомнений, подчеркивает актуальность задач: анализа защищенности программно-аппаратного обеспечения БСС; контроля корректности предоставляемых ими сервисов с последующим принятием контрмер на основе результатов анализа защищенности; выработки рекомендаций по повышению защищенности БСС.

Беспроводные сенсорные сети технологически находятся на стыке предметных областей сетей встроенных устройств и систем Интернета вещей [1]. Они представляют собой сравнительно новый вид информационно-телекоммуникационных инфраструктур и объединяют множества встроенных устройств и сенсоров. Сети такого класса включают разнообразные электронные устройства, физические объекты и пользователей с возникающими между ними коммуникационными соединениями и семантическими связями, потребностями в обработке, хранении, отображении и защите разнородной информации. Это самоорганизующиеся беспроводные системы специализированного назначения, включающие в свой состав различные встроенные устройства, программно-аппаратные сенсоры, исполнительные элементы, созданные на основе современных микросхем, в т. ч. на основе одноплатных компьютеров.

Специфика построения и применения БСС обуславливает особенности и наличие, как традиционных, так и нетрадиционных, угроз их информационной безопасности. Эти угрозы связаны с появлением новых классов, осуществляемых на БСС программно-информационных и физических атакующих воздействий, и требуют новых путей и механизмов защиты [2].

Методологической основой выбора и обоснования путей и механизмов защиты являются результаты анализа защищенности программно-аппарат-

ного обеспечения БСС. Анализ защищенности БСС – сложная, нетрадиционная задача, поскольку имеют место важные особенности таких систем. Они заключается в ограниченности аппаратных ресурсов БСС, задействованных программно-аппаратных модулей и их относительно низкой производительности по сравнению с другими видами вычислительных систем и телекоммуникационных сетей. Кроме того, существуют специфические возможности потенциального нарушителя в БСС, он способен совершать действия одновременно, как на физическом уровне, так и на программно-информационном. Важной особенностью является изменчивость программно-аппаратного окружения БСС и способов коммуникации между устройствами сети, а также наличие уникальных семантических связей.

Очевидно, что в современных условиях анализ защищенности БСС от атакующих воздействий может и должен быть организован с использованием принципов обработки данных и событий информационной безопасности на основе технологии Больших Данных и нейронных сетей для выявления аномальных данных от сенсоров, на основе анализа возможных видов нарушителей в системах Интернета вещей, а также с учетом специфичных многошаговых атакующих воздействий на программно-информационном и аппаратно-физическом уровнях представления [3].

Обобщенный алгоритм анализа защищенности БСС от атакующих воздействий должен быть ориентирован на моделирование, анализ и практическую реализацию, оценивания защищенности сетей такого класса в условиях наличия разнородных и, взаимодействующих между собой, устройств, использующих беспроводные протоколы передачи данных, и с учетом повышенных требований к защищенности таких систем (сетей).

К основным этапам обобщенного алгоритма анализа защищенности БСС от атакующих воздействий можно отнести:

– этап моделирования БСС, специфицирующего физические и логические связи между узлами сети, их типы, роли, процессы динамической маршрутизации;

– этап моделирования поведения нарушителя в БСС – этот этап задает возможные многошаговые атакующие воздействия, классифицируемые по характеристикам нарушителя;

– этап верификации атакующих воздействий в БСС с определением системы основных показателей для оценки таких атакующих воздействий;

– этап контроля БСС на предмет выполнимости условий осуществления атакующих воздействий нарушителем;

– этап распределенных сбора, обработки и анализа больших массивов данных от программных и аппаратных сенсоров БСС в режиме, близком к режиму реального времени, с использованием вычислительного кластера;

– этап выявления аномальных данных от сенсоров БСС на основе применения аппарата нейронных сетей с учетом классификации атакующих воздействий и их признаков;

– этап окончательного анализа защищенности программно-аппаратных компонентов БСС беспроводных сенсорных сетей;

– этап выработки предложений по повышению защищенности БСС на основе полученных результатов.

Особого внимания, на наш взгляд, заслуживают первый и второй этапы – этапы моделирования БСС и поведения нарушителя. На первом этапе строятся динамические модели, отображающие физические и логические связи между узлами сети, определяются типы узлов сети и их роли в контексте свойств самоорганизации БСС и процессов маршрутизации в ней. Эти модели также отображают динамические характеристики и потоки данных в сети, позволяют создавать профили по настройке параметров узлов БСС, отправке, получению и распознаванию тестовых и сервисных команд в сети такого класса.

Модели, предлагаемые к использованию на первом этапе обобщенного алгоритма анализа защищенности БСС от атакующих воздействий, строятся с учетом наличия обратных связей от моделей к объектам программно-аппаратной инфраструктуры сети. Эти связи учтены в виде специализированных программно-аппаратных триггеров и актуаторов, инициирующих конкретные события в БСС (отправка пакета данных, обновление ключа шифрования и др.).

Эти модели также предназначены, в частности, для анализа атакующих воздействий и инцидентов безопасности на уровне манипуляции командами представления с использованием унифицированных команд обращения к узлам БСС, ее данным и предоставляемым сервисам. В качестве аппарата для построения и реализации моделей используются графы и алгоритмы их обхода и анализа. Для построения моделей разработаны компоненты распределенного сбора данных и управления БСС с использованием современных микроконтроллеров и беспроводных коммуникационных интерфейсов.

На втором этапе строится комбинированная модель нарушителя БСС с учетом возможных многошаговых атакующих воздействий и семантики внутрисетевых взаимодействий узлов сети. В рамках комбинированной модели нарушителя приведена классификация атакующих воздействий в беспроводных сенсорных сетях, включающая несанкционированную модификацию конфигурационных настроек узлов сети, атаку перехвата данных в сети, атаку модификации данных, атаку внедрения ложного узла сети, DoS-атаку и атаку нарушения процесса маршрутизации в сети.

Достоинствами предлагаемого подхода к формулировке, наполнению и чередованию этапов обобщенного алгоритма анализа защищенности БСС

от атакующих воздействий являются комбинирование и учет различных моделей нарушителя, осуществляющего многошаговые воздействия, как физического, так и программно-информационного характера, с использованием предлагаемой системы показателей нарушителя. Кроме того, моделирование компонентов БСС, различных видов нарушителей и атак реализуется с возможностью формирования обратных связей от моделируемых программно-аппаратных компонентов сети к киберфизическим модулям прототипа конкретной сети. Обобщенный алгоритм предполагает применение, основанного на нейронной сети, подхода к выявлению аномальных данных от сенсоров БСС с использованием признаков распознавания аномалий на основе классификации атакующих воздействий.

Предложенный подход, по мнению авторов, позволит повысить достоверность и оперативность анализа защищенности БСС от атакующих воздействий, что, в свою очередь, позволит повысить качество принимаемых решений по управлению защитой информационных ресурсов сетей такого класса.

Работа выполнена при финансовой поддержке РФФИ (проект 19-07-00953) в СПИИРАН.

Список используемых источников

1. Ghildiyal S., Gupta A., Vaqur M., Semwal A. Analysis of wireless sensor networks: security, attacks and challenges // IJRET: International Journal of Research in Engineering and Technology. Volume 03. Issue 03. 2014. pp. 160–164.

2. Desnitsky V. A., Kotenko I. V. Modeling and analysis of security incidents for mobile communication mesh Zigbee-based network // XX IEEE International Conference on Soft Computing and Measurements (SCM), St. Petersburg. 2017. pp. 500–502.

3. Десницкий В. А., Паращук И. Б. Показатели доступности, целостности и конфиденциальности данных пользователей беспроводных сенсорных сетей в интересах анализа и обеспечения их защищенности // Информационная безопасность регионов России (ИБРР-2019) : материалы XI межрег. конф., Санкт-Петербург, 23–25 октября 2019 г. СПб.: СПОИСУ, 2019. С. 114–116.

УДК 654.739
ГРНТИ 49.33.29

АНАЛИЗ КОМПЛЕКСНЫХ ПОКАЗАТЕЛЕЙ МУЛЬТИСЕРВИСНЫХ ТЕЛЕКОММУНИКАЦИОННЫХ СЕТЕЙ НА БАЗЕ АРХИТЕКТУРНЫХ КОНЦЕПЦИЙ FN

Э. М. Джафарова, Б. Г. Ибрагимов, С. Р. Исмайлова

Азербайджанский технический университет

В данной работе предметом исследования является сетевая мультисервисная инфраструктура с использованием инновационных технологий следующего и будущего поколений, поддерживающая широкий спектр мультимедийных услуг и приложений. Проанализированы комплексные показатели мультисервисных телекоммуникационных сетей на базе архитектурных концепций будущих сетей FN. На основе исследования предложен метод расчета комплексных показателей МТС на базе архитектурной концепции FN. Получены аналитические выражения, позволяющие оценить показатели эффективности и качество работы сетей связи общего пользования, информационной безопасности, качество обслуживания QoS гетерогенного трафика и структурной надежности функционирования системы при оказании мультимедийных услуг.

качество функционирования, SDN, мультисервисная телекоммуникационная сеть, FN, производительность сети, мультимедийные услуги, NFV, Будущие сети, ресурсы.

В настоящее время проблема развития единого инфокоммуникационного обеспечения цифровой экономики, формирование планов стратегической «Дорожной карты цифровизации» в республике Азербайджан и начало Четвёртой промышленной революции требуют глобального подхода для построения высокоэффективных МТС на базе архитектурной концепции будущих сетей FN (FN, *Future Networks*) с повышенной производительностью [1, 2]. Стоит отметить, что в основу будущих сетей [3, 4], как и сетей NGN (*Next Generation Network*), положен принцип «Множества мультимедийных услуг – одна сеть». Поэтому анализируемые сети с использованием современных инновационных технологий являются высокоскоростными сетями электросвязи последующих NGN и будущего поколения FN, представляющие собой универсальную базовую сеть общего пользования, единого инфокоммуникационного пространства и единой многооператорской среды. Последние открывают новые возможности для оказания широкого спектра основных, дополнительных и интеллектуальных услуг с гарантированным качеством обслуживания – QoS (*Quality of Services*).

Одним из важнейших направлений развития мультисервисных телекоммуникационных сетей (МТС), связанных с использованием и представ-

лением мультимедийных услуг, является расширение и улучшение возможностей, предназначенных для повышения качества и эффективности использования существующих разнородных ресурсов. Эти ресурсы являются, как физические (аппаратно-программные средства первого уровня – коммутаторы, маршрутизаторы, сервера, различные линии связи и терминальное оборудование), сетевые, канальные, виртуальные, так и информационные. При этом, возникает задача управления перечисленными ресурсами и их оптимального распределения в узлах МТС для оказания различных мультимедийных услуг и приложений разным группам пользователей с учетом многочисленных требований параметров QoS&QoE (*Quality of Experience*).

Под мультимедийными услугами и приложениями понимается множество мультимедийных услуг, как “Triple Play services”, “Mobile Satellite Service”, интеллектуальные приложения (SUN – *Smart Ubiquitous Networks, Cognitive Networks*), “Broadcast Satellite Service”, так и “Bandwidth on Demand”, которым требуются высокоскоростные оптические каналы связи и разнородные ресурсы [4].

Вышеперечисленные услуги являются инфокоммуникационными услугами, а разнородные ресурсы являются ИКТ-технологиями [5]. Без опережающего развития этих сетей [6] невозможно повсеместное распространение ИКТ-технологий, включая и глобальный интернет. Поэтому, исследование комплексных показателей МТС для оказания мультимедийных услуг и приложений при эффективном использовании разнородных ресурсов [7] с целью обеспечения их качественного функционирования, представляет значительный интерес.

Цель работы – анализировать и исследовать возможности оценивания комплексных показателей мультисервисных телекоммуникационных сетей при оказании мультимедийных услуг и приложений. Учитывая важность построения МТС на базе FN [5] с коммутацией пакетов (ITU-T, Y.3000÷Y.3499) для гарантированного качества обслуживания QoS гетерогенного трафика, порождающих инфокоммуникационные услуги, следует обратить особое внимание на их комплексные показатели.

Наши исследования посвящены решению задачи – разработке методов расчета комплексных показателей МТС на базе архитектурной концепции FN, позволяющей оценить эффективную, надежную, защищенную и устойчивую передачу. Проведенный анализ показал, что основными и наиболее востребованными услугами исследуемой сети являются мультимедийные услуги и приложения, а также цифровой метод широкополосного доступа в сети интернет, в котором необходимо более детально исследовать поток гетерогенного трафика, возникающего при создании этих услуг. Кроме того, этим мультимедийным услугам требуются многоскоростные системы обслуживания, достаточного объема информационного, сетевого и канального

в сети интернет, в котором необходимо более детально исследовать поток гетерогенного трафика, возникающего при создании этих услуг. Кроме того, этим мультимедийным услугам требуются многоскоростные системы обслуживания, достаточного объема информационного, сетевого и канального ресурса, различной скорости передачи данных, защита информации с использованием квантовых технологий [6, 7]. При реализации вышеуказанных услуг в звене сети появляется источник нагрузки, который генерирует гетерогенный трафик.

Гарантированное QoS&QoE обслуживание этих нагрузок в сетях требуют определенные характеристики [5, 6]: максимальное значение пропускной способности, средняя задержка при передаче пакета, функциональная надежность, информационная безопасность и повышенные коэффициенты эффективного использования разнородных ресурсов, а также многочисленные параметры качества связи. Это в полной мере относится и к реализации вопросов инфокоммуникационного обеспечения цифровой экономики для построения МТС связи нового поколения. Для реализации заявленных целей на первый план выходят четыре целевые установки создания Будущих сетей с рекомендациями ITU-T, Y.3001, и инновационные технологии будущего поколения [5, 6, 7].

Решение поставленной задачи требует комплексного подхода для исследования основных показателей МТС на базе архитектурной концепции FN, использующих SDN&NFV (*Software Defined Networking& Network Functions Virtualization*), искусственного интеллекта, облачных вычислений, больших данных, мобильных технологий LTE (*Long Term Evolution*) & UMTS (Universal Mobile Telecommunications System), IoT (*Internet of Think*), технологий построения распределенных сетей связи [1].

Проанализированы алгоритмы работы технического состава аппаратно-программных средств и исследованы методы построения МТС нового поколения [1, 4, 6]. С учетом последних предположений и на основе исследования, разработаны методы расчета комплексных показателей МТС при оказании мультимедийных услуг и приложений.

Для формализации вышеизложенных задач предлагается метод расчета комплексных показателей сетей связи следующего поколения, который будет наиболее точно отражать информационные и телекоммуникационные процессы, протекающие в исследуемом звене сети при оказании мультимедийных услуг и приложений.

На основе системно-технического анализа, математическая формулировка реализации постановки задачи предлагаемого метода расчета комплексных показателей МТС на базе архитектурной концепции FN описывается следующей целевой функцией [4, 7]:

$$Q_{\text{кф}} = W\{Arg \max_{i}[П_{\text{пр}}(\lambda_i, H)]\},\ i = \overline{1,k}\}, \quad (1)$$

при следующих ограничениях:

$$E_{\text{эфф.}}[\lambda_i] \le E^{\text{доп.}}_{\text{эфф}}(\lambda_i)],\ P_{i.\text{нф}}(t,\Lambda_i) \ge P(t,\Lambda_i)^{\text{доп.}}_{i.\text{нф}},\ T_{\text{ввх}}(\lambda_i) \le T^{\text{доп.}}_{\text{ввх}}(\lambda_i),$$

$$P_{i.ny} \ge P^{\text{доп.}}_{i.ny},\ \ N_{i.k} \le N^{\text{доп.}}_{i.k}\ ,\ K_{i.\text{иб}}(\lambda) \le K^{\text{доп.}}_{i.\text{иб}}(\lambda), C_{i.a} \le C^{\text{доп.}}_{i.a},\ \ i = \overline{1,k}, \quad (2)$$

где $E_{\text{эфф}}(\lambda_i)$ – функция, учитывающая эффективность функционирования МТС с интенсивностью λ_i при обслуживании *i*-го потока пакетов и $E_{\text{эфф}}(\lambda_i) = [C_{\max}(\lambda_i), E_{I.T.E}]$, $i = \overline{1,k}$; $E_{I.\text{Ч.}E}$ – информационная, частотная и энергетическая эффективность сетей связи общего пользования и $E_{I.T.E} = [E_I, E_{\text{ч}}, E_E]$; $P_{i.ny}$ – функция, учитывающая показатели качества работы сетей связи при приеме *i*-го потока пакетов трафика и $P_{i.ny} = [P_{\text{ош}}, V_{i.k}]$, $i = \overline{1,k}$; $V_{i.k}$ – скорость работы программно-аппаратных и терминальных средств при обслуживании *i*-го пакета трафиков; $P_{\text{нф}}(t,\Lambda_i)$ – функция, учитывающая показатели функциональной и структурной надежности функционирования системы с интенсивностью отказов Λ_i и характеризуется единичным и комплексным показателем надежности программно-аппаратных и терминальных средств в момент времени *t* и $P_{\text{нф}}(t,\Lambda_i) = [K_{\Gamma}, P_{\text{ВБР}}(t,\Lambda_i), P_{\text{отк}}]$, $i = \overline{1,k}$; K_{Γ} – коэффициент оперативной готовности сетей связи; $P_{\text{ВБР}}(t,\Lambda_i)$ – вероятность безотказной работы системы с интенсивностью отказов Λ_i в момент времени *t*; $K_{\text{иб}}(\lambda_i)$ – функция, учитывающая показатели информационной безопасности сетей связи с интенсивностью λ_i, использующие SDN&NFV и IMS технологии при обслуживании *i*-го пакета трафиков и $K_{\text{иб}}(\lambda_i) = [R_i, P_{\text{уг.}}(\lambda_i)]$, $i = \overline{1,k}$; R_i – коэффициент риска информационной безопасности, влияющий на качество функционирования сети, $P_{\text{уг.}}(\lambda_i)$ – вероятность угрозы с интенсивностью λ_i при обслуживании *i*-го пакета трафиков, $i = \overline{1,k}$; $T_{i.\text{ввх}}(\lambda)$ – функция, учитывающая показатели вероятностно-временных характеристик гетерогенного трафика с интенсивностью λ_i при обслуживании *i*-го потока пакетов трафика $T_{\text{ввх}}(\lambda_i) = [T_{i.\text{ср.з}}, \rho_i, L_{cd}(\lambda_i)]$, $i = \overline{1,k}$; $C_{i.a}$ – стоимость аппаратных и программных средств МТС при обслуживании потоков пакетов *i*-го трафика с использованием технологий SDN/NFV и IMS, $i = \overline{1,k}$; $P_{\text{ош}}$ – вероятность ошибки приема потоков пакетов трафика; N_{ik} – общее число используемых в сетях МТС комплексов программно-аппаратных и терминальных средств для обслуживания *i*-го потока пакетов, работающие на основе алгоритма «End to end»; $P_{\text{отк}}$ – вероятность отказа в обслуживании пакета поступающего трафика; $C_{\max}(\lambda_i)$ максимальное значение пропускной способности

МТС в зависимости от интенсивности λ_i входящего потока пакетов трафиков; ρ_i – коэффициент эффективного использования ресурсов сетей связи при обслуживании потоков пакетов *i*-го трафика; $T_{i.\text{ср.з}}$ среднее время задержки при обслуживании потока пакета *i*-го трафика, $i=\overline{1,k}$; $R_{i.er}$ – показатели, учитывающие эффективность использования виртуальных, информационных, канальных и сетевых ресурсов в МТС при передаче *i*-го потока пакетов, $i=\overline{1,k}$; $f(H)$ – функция, учитывающая свойство самоподобия поступающей нагрузки, и равно $f(H)=2H$; H коэффициент Хэрста для потока пакета локального и глобального полезного и служебного трафиков, и 0,5 < H < 1,0.

Выражения (1) и (2) определяют сущность рассматриваемого нового подхода, на основе которого предлагается метод расчета комплексных показателей МТС на базе архитектурных концепций FN с использованием технологий SDN/NFV и IMS при оказании мультимедийных услуг и приложений. Помимо этого, выражения (1) и (2) учитывают критерии качества функционирования сетей связи и описывают производительность Будущих сетей с учетом четырех целевых установок.

Критерием качества функционирования МТС на базе архитектурных концепций FN с использованием цифровых ИКТ-технологий выбрана производительность сетей связи общего пользования, которая отражает способность системы и обеспечивает требуемые комплексные показатели:

– эффективность и устойчивость сетей связи общего пользования;
– функциональная и структурная надежность системы;
– виртуальные, канальные, информационные и сетевые ресурсы;
– вероятностно-временные характеристики гетерогенного трафика;
– свойства самоподобия мультисервисных трафиков;
– QoS&QoE при оказании мультимедийных услуг и приложений.
– системы защиты информации с использованием квантовых технологий.

Таким образом, в результате исследования предложен метод расчета комплексных показателей МТС на базе архитектурной концепции FN с внедрением передовых технологий будущего поколения. Получены важные аналитические выражения, позволяющие оценить характеристики качества функционирования МТС при оказании мультимедийных услуг и приложений.

Список используемых источников

1. Ефимушкин В. А., Ледоковских Т. В., Иванов А. Б., Шалагинов В. А. Роль технологий SDN/NFV в инфраструктуре цифровой экономики. Опыт тестирования и внедрения // Электросвязь. 2018. № 3. С. 27–36.

2. Шваб Клаус. Четвёртая промышленная революция: перевод с английского. М. : Энергия, 2017. 208 с.

3. Пшеничников А. П. Этапы цифровизации сетей связи // Методические вопросы преподавании инфокоммуникаций в высшей школе. 2019. № 2. С. 65–71.

4. Ибрагимов Б. Г., Гумбатов Р. Т., Ибрагимов Р. Ф., Исаев А. М. Анализ показателей производительности мультисервисных телекоммуникационных сетей будущего поколения с использованием технологий ПКС // Вестник компьютерных и информационных технологии. 2019. № 5. С. 39–44.

5. Росляков А. В., Ваняшин С. В. Будущие сети (Future Networks). Самара : ПГУТИ, 2015. 274 с.

6. Кучерявый А. Е., Бородин А. С., Кричек Р. В. Сети связи 2030 // Электросвязь. 2018. № 11. С. 52–56.

7. Ibrahimov B. G., Humbatov R. T., Ibrahimov R. F. Performance multiservice telecommunication networks based on the architectural concept future networks using SDN technology // T-Comm. 2018. Vol. 12. No 12. PP. 84–88.

УДК 004.5
ГРНТИ 81.93.29

ИССЛЕДОВАНИЕ СОВРЕМЕННЫХ МЕТОДОВ СЕТЕВОЙ СТЕГАНОГРАФИИ

В. Н. Диордица, А. В. Красов, А. И. Таргонская

Санкт-Петербургский государственный университет телекоммуникаций им. проф. М. А. Бонч-Бруевича

В настоящее время актуальность применения стеганографии сильно возросла в связи с стремительным развитием информационной сферы. Современная стеганография находит своё применение в различных областях информационной сферы, позволяя решить широкий спектр задач: начиная от создания цифровых отпечатков, подтверждающих авторство и защищающее исключительное право на продукт деятельности, заканчивая скрытной передачей данных, использование которой в купе с использованием надёжной криптографической защитой обеспечивает максимальную безопасность данных. В рамках данной работы будут рассмотрены различные методы и алгоритмы стеговложения в сетевые пакеты (WLAN, LACK), каждому из рассмотренных методов будет дана оценка на основании различных параметров и критериев стойкости системы.

сетевая стеганография, сокрытие данных, wlan, lack, hiccups, sip, mac.

Введение

С древних времен люди, обменивающиеся важной информацией, нуждались в сокрытии передаваемых данных от глаз посторонних наблюдателей. Именно эту задачу помогает решить стеганография – наука о скрытной

передаче данных. В отличие от криптографии, основной целью которой является сокрытие содержимого передаваемого сообщения, стеганография скрывает сам факт передачи данных. Таким образом стеганография не заменяет, а дополняет криптографию, надёжно скрывая сам факт передачи информации. Стеганография применялась ещё с незапамятных времен, однако получила известность в широких кругах только благодаря появлению интернета. Именно обмен данными в глобальных сетях поспособствовал появлению целого отдельного направления стеганографии, названного сетевой стеганографией. В сетевой стеганографии данные могут быть сокрыты не только в обычных открытых сообщениях, но и в самом протоколе связи, и в измененной логике его работы. В настоящее время стеганография используется для широкого спектра задач: от подтверждения владения некоторой информацией с помощью системы встраивания водяного знака, до сокрытия информации при проведении хакерских атаках.

Одним из наиболее востребованных применений стеганографии является решение задачи защиты авторского права, использующее для проверки подлинности, как уже было упомянуто ранее, встраивание водяного знака в данные, авторство которых, необходимо проверить. Таким образом, используя методы стеганографии можно решить сразу несколько важных задач: можно определить автора данного материала, а также, следовательно, подтвердить принадлежность данного материала тому или иному лицу. Стеганография также может быть использована для решения задачи проверки целостности некоторой информации, так как при подмене данных чаще всего искажается и стеганографическое вложение внутри контейнера, что в свою очередь является прямым доказательством попытки несанкционированной модификации сообщения. Хотя данный метод и не является распространённым применением стеганографии, он может быть использован в некоторых системах проверки подлинности.

Однако весьма широкое распространение стеганография получила именно в кругах разного рода злоумышленников, использующих её для сокрытия факта передачи запрещенных материалов в сети. Используя стеганографию злоумышленникам, удаётся передать секретные данные по открытым каналам связи, минуя различные системы безопасности сети, и остаться незамеченными. Известно достаточно много случаев применения стеганографии злоумышленниками: ярким примером использования стеганографии в незаконных целях может служить координация террористических структур с помощью вложения информации в изображения с дальнейшей публикацией их в сети, другим примером использования стеганографии злоумышленниками является вложение хакерами вредоносного кода в изображения для обхода сетевого фильтра.

Именно поэтому методы вложения информации и методы обнаружения вложений требуют всестороннего и тщательного анализа.

1. Классификация методов сетевой стеганографии

Методы сетевой стеганографии можно разделить на 3 группы (рис. 1):

1. Методы, основанные на модификации пакетов:

1.1. Методы, изменяющие данные в полях служебных заголовков сетевых протоколов.

1.2. Методы, изменяющие данные в полях полезной нагрузки пакетов.

1.3. Методы, объединяющие оба вышеперечисленных метода.

2. Методы стеганографии, изменяющие структуру и параметры передачи пакетов:

2.1. Методы, в которых изменяется порядок следования пакетов.

2.2. Методы, изменяющие задержку между пакетами.

2.3. Методы, вводящие преднамеренные потери пакетов путём пропуска порядковых номеров у отправителя.

3. Смешанные (гибридные) методы стеганографии – изменяет все вышеупомянутые параметры пакетов. При этом используются два подхода: преднамеренные задержки аудио пакетов LACK (*Lost Audio Packets Steganography*) и ретрансляция пакетов RSTEG (*Retransmission Steganography*).

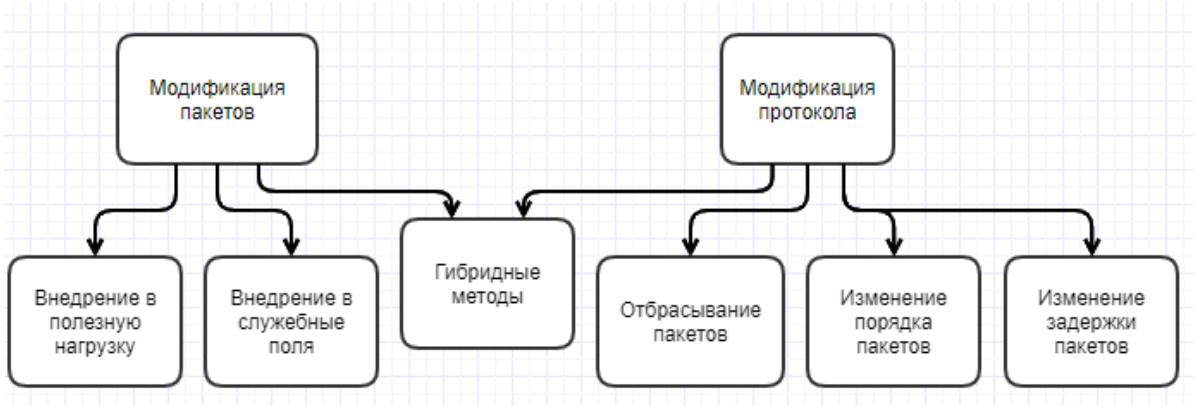


Рис. 1. Классификация методов сетевой стеганографии

2. Метод LACK

Lost Audio Packets Steganography – метод стеганографического вложения, основанный на использовании намеренных задержек аудиопакетов [1]. Данный метод используется для скрытой передачи данных через протоколы VoIP. При рассмотрении VoIP, можно узнать, что для установления и поддержания канала используется две служебные части: сигнальная и разговорная. Обе части участвуют в двухстороннем обмене данными. В качестве сигнального протокола чаще всего используется протокол SIP (*Session Initiation Protocol*), а для передачи аудиопакетов используется протокол RTP (*Real-time Transport Protocol*) [2]. Установление соединения начинается с обмена

SIP сообщениями между SIP клиентами, которые проходят через SIP сервера. Обмен данными сообщениями выполняется для поиска SIP клиентами друг друга. После успешного обмена SIP сообщениями и установления сессии, начинается двухсторонний обмен аудио пакетами по протоколу RTP. Так как пропускная способность RTP канала довольно высока, скорость скрытой передачи данных также довольно высока. Однако намеренное введение помех в канал может вызвать подозрение у сторонних наблюдателей, что может привести к обнаружению стеганографического вложения и рассекречиванию системы передачи скрытых сообщений. Также стоит отметить, что данный метод довольно сложно реализовать в рамках некоторых операционных систем. Исходя из всего вышеперечисленного, можно отметить, что метод обладает средней сложностью обнаружения и довольно высокой сложность реализации относительно других методов стеганографических вложений в сетевые пакеты.

3. Метод WLAN (Система HICCUPS)

Система стеганографических вложений HICCUPS, является комбинированной стеганографической системой, использующей особенности передачи аудио данных в сетевой среде, такие как шум, помехи и искажение данных. Система HICCUPS используется в беспроводных сетях в виду наличия в них особенностей, подходящих для корректной работы алгоритма. Основная причина использования беспроводных сетей состоит в том, что такой вид передачи данных более восприимчив к искажению, нежели передача данных по проводу, именно поэтому создаваемые в канале связи помехи являются достаточно удобным средством для вложения скрытых данных в передаваемые пакеты. Для реализации системы HICCUPS необходимо чтобы система отвечала определённым требованиям: необходимо наличие возможности перехвата и модификации пакетов или создания заведомо повреждённого пакета с вложенными в него данными. В данном случае использование беспроводных сетей обуславливается возможностью возникновения в них битовых ошибок, что обеспечивает возможность посылать намеренно искаженные кадры. Такой метод имеет относительно низкую пропускную способность, имеет довольно сложную реализацию, но он так же имеет высокую сложность обнаружения. Не смотря на заявленную ранее высокую сложность обнаружения вложения этим методом всё же возможно обнаружить благодаря проверке контрольной суммы [3].

Первым этапом установления секретного канала является согласование общего секретного ключа для алгоритмов шифрования, встроенных в данную систему. Последующий обмен данными происходит на основе векторов инициализации и MAC-адресов устройств, участвующих в скрытом обмене данными. После установления соединения канал с ограниченной пропускной способностью может использоваться как среда для скрытой передачи

коротких сообщений. Для передачи большего количества данных станции переходят в режим модификации кадров, обеспечивающий широкую полосу пропускания. Работая в таком режиме, информация скрывается внутри полезной нагрузки кадра с неверной контрольной суммой. Скрытность системы в этом случае обуславливается механизмом отброса пакетов с неверной контрольной суммой на станциях, не принадлежащих к скрытой группе [4].

4. Сравнение методов

На рис. 2 представлена диаграмма, отражающая сравнительные характеристики описанных выше методов сетевой стеганографии, полученные в результате исследований, описанных в следующих статьях «Stream Control Transmission Protocol Steganography», а также в «Retransmission steganography and its detection» и «Using Transcoding for Hidden Communication in IP Telephony» [5, 6, 7]. Методы стеганографии сравнивались по следующим параметрам: максимальная пропускная способность оцениваемого алгоритма, сложности обнаружения стеганографического вложения, стоимости реализации алгоритма и сложности реализации алгоритма. Оценка методов производилась в условных единицах и не отражает количественных характеристик.

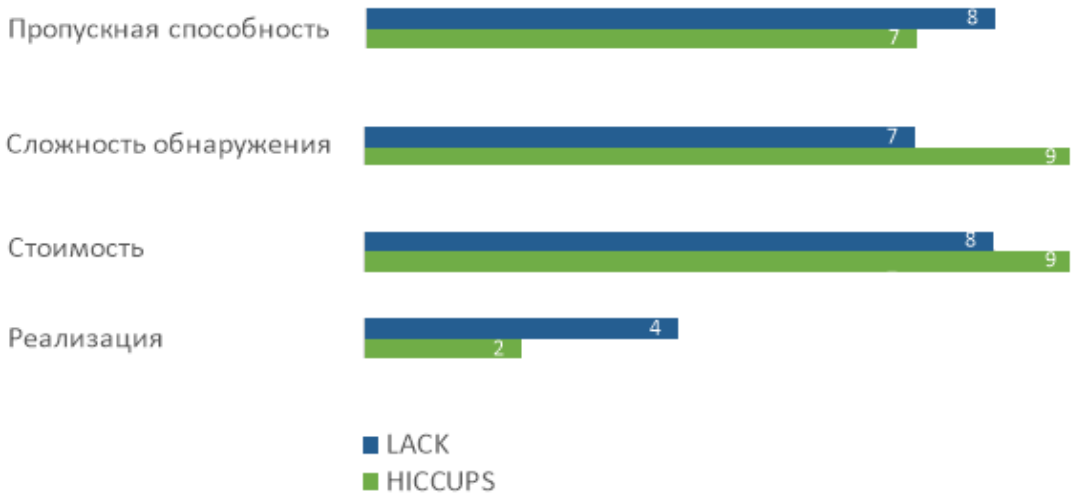


Рис. 2. Сравнение LACK и WLAN (HICCUPS)

Заключение

В данной работе были рассмотрены различные методы современной стеганографии, а также были даны оценки на основании различных характеристик. Рассмотренные методы обладают достаточно высокой пропускной способностью, высокой сложностью обнаружения и низкой сложностью реализации, что делает данные методы достаточно простыми и надежными в использовании.

Список используемых источников

1. Mazurczyk, J. Lubacz, K. Szczypiorski. On steganography in lost audio packets [Электронный ресурс] // Security and Communication Networks. 2014. URL: https://arxiv.org/ftp/arxiv/papers/1102/1102.0023.pdf (дата обращения 23.03.2020).
2. Stewart R., Ed. Stream Control Transmission Protocol. RFC 4960–Request for Comments: 4960, 2007 [Электронный ресурс] // IETF Tools. URL: http://tools.ietf.org/html/rfc4960 (дата обращения 23.03.2020).
3. Пескова О. Ю., Халабурда Г. Ю. Применение сетевой стеганографии для скрытия данных, передаваемых по каналам связи // Известия Южного федерального университета. Технические науки. 2012. № 12 (137). С. 167–176.
4. Белкина Т. А. Аналитический обзор применения сетевой стеганографии для решения задач информационной безопасности // Молодой ученый. 2018. № 11. С. 36–44. URL: https://moluch.ru/archive/197/48821/ (дата обращения: 27.03.2020).
5. W. Frączek, W. Mazurczyk, K. Szczypiorski. Stream Control Transmission Protocol Steganography // Warsaw University of Technology, Institute of Telecommunications. 2010. URL: http://arxiv.org/abs/1006.0247 (дата обращения 21.03.2020).
6. Wojciech Mazurczyk, Paweł Szaga, Krzysztof Szczypiorski. Retransmission steganography and its detection [Электронный ресурс] // IT2Net. 2012. URL: https://secure.tele.pw.edu.pl/wmazurczyk/art/RSTEG.pdf (дата обращения 20.03.2020).
7. Wojciech Mazurczyk, Paweł Szaga, Krzysztof Szczypiorski. Using Transcoding for Hidden Communication in IP Telephony [Электронный ресурс] // Warsaw University of Technology, Institute of Telecommunications. URL: http://arxiv.org/pdf/1111.1250v1.pdf (дата обращения 19.03.2020).

УДК 004.056
ГРНТИ 81.93.29

ПОДДЕРЖКА ПРИНЯТИЯ РЕШЕНИЙ ПО ПОВЫШЕНИЮ ЗАЩИЩЕННОСТИ ОТ ИНЦИДЕНТОВ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ С ИСПОЛЬЗОВАНИЕМ БАЗЫ MITRE ATT&CK

Е. В. Дойникова[1,2], О. С. Дудкина[1], И. Б. Саенко[2]

[1]Санкт-Петербургский государственный университет телекоммуникаций им. проф. М.А. Бонч-Бруевича
[2]Санкт-Петербургский институт информатики и автоматизации Российской академии наук

Задача автоматизации процесса принятия решений по реагированию на инциденты информационной безопасности является сложной и актуальной. Одной из проблем в данной области является стандартизация возможных мер реагирования и автоматическое сопоставление данных мер разным типам инцидентов. В данной работе рассматривается одно из решений в данной области – база атак и средств защиты –

Mitre Att&ck. А также анализируются способы ее применения для поддержки принятия решений по повышению защищенности информационных систем.

информационная безопасность, инцидент, принятие решений, MITRE ATT&CK.

Индустриальный Интернет вещей является привлекательной целью для злоумышленника, а нарушение информационной безопасности его систем может нанести как материальный ущерб, так и ущерб жизнедеятельности граждан. Поэтому задача разработки для него новых средств и методик противодействия угрозам информационной безопасности является важной. При этом необходимо учитывать специфику предприятия, проводить регулярный мониторинг ключевых показателей, прогнозировать риски, а также моделировать угрозы. В последние годы источники данных безопасности, которые могут использоваться для этих целей, активно развиваются. В данной статье рассматривается один из таких источников – база атак и средств защиты – MITRE Att&ck (*Adversarial Tactics, Techniques, and Common Knowledge* – Тактики, Техники и общие знания) [1]. Анализируются способы ее применения для принятия решений по повышению защищенности информационных систем, в том числе, систем индустриального Интернета вещей, а также ее достоинства и недостатки.

Описание MITRE Att&ck

MITRE Att&ck – это открытая база знаний о тактике и технике противника, основанная на реальных наблюдениях. Она может использоваться в качестве основы для разработки конкретных моделей и методологий угроз [2].

Организация MITRE запустила базу Att&ck в 2013 году для документирования общих тактик, методик и процедур, которые используются в рамках атак на корпоративные сети Windows [3]. Она была создана для решения следующих задач:

1) определение поведения злоумышленника;

2) слишком высокий уровень абстракции существующих моделей жизненного цикла кибератаки;

3) применимость к реальной среде;

4) общая классификация тактик, методик и процедур.

На данный момент база расширилась от Windows до других платформ и технологий. Att&ck используется многими правительственными организациями и секторами промышленности, включая финансовые, медицинские, розничные и технологические.

На сегодняшний день структура базы состоит из 12 тактик (этапов):

1. Начальный доступ – злоумышленник пытается проникнуть в периметр сети, используя различные векторы входа.

2. Выполнение – злоумышленник пытается внедрить и запустить вредоносный код.

3. Постоянство/упорство – злоумышленник, проникнув в систему, старается сохранить свою позицию.

4. Повышение привилегий – попытка получить разрешения более высокого уровня.

5. Уклонение от защиты/обход защиты – злоумышленник пытается избежать обнаружения.

6. Получение учетных данных – попытка украсть учетные записи и пароли, что позволит получить доступ к системам, затруднить обнаружение, а также создавать новые учетные записи, которые помогут достичь цели.

7. Обнаружение – злоумышленник изучает окружение для получения больших знаний о системе, нахождение новых точек входа, чтобы понять, что может принести пользу для достижения своей цели.

8. Боковое перемещение – противник перемещается по среде, чтобы найти цель и определить способ получения к ней доступа.

9. Сбор данных – злоумышленник пытается собрать данные. Источниками могут быть различные диски, браузеры, электронная почта, аудио и видео.

10. Командование и управление – попытка управления и контроля скомпрометированных систем.

11. Эксфильтрация/утечка данных – злоумышленник пытается украсть данные путем передачи их по каналам управления или по альтернативному каналу, используя сжатие и шифрование.

12. Воздействие – попытка манипулирования или уничтожения данных, или системы.

Интерес для обеспечения информационной безопасности индустриальных систем представляет раздел Att&ck for ICS (*Industrial Control Systems*, автоматизированная система управления) – это база знаний, предназначенная для описания действий, которые может предпринять противник при работе в сети ICS [4]. ICS – системы, которые обеспечивают эффективную и безопасную автоматизацию физических процессов на производстве. Матрица Att&ck для ICS – это обзор тактик и методов атак на ICS. Данная матрица также включает в себя 11 техник и методов, применяемых в промышленных системах управления. Один из вариантов использования Att&ck для ICS – разработка сценария отказов. Для этого необходимо выявить отказы, определить их причину, затем определить последовательность действий, которые могут привести к этому отказу. Определенная последовательность действий или методов поможет выявить особенно уязвимые точки системы, где необходимо использовать средства защиты, чтобы перекрыть точку входа для злоумышленников.

Помимо этого, в базе представлен список возможных вариантов реагирования на атаки или их предотвращения. Для предприятий представлен 41 вариант [5], для мобильных устройств – 13 [6]. Каждый метод реагирования или предотвращения атаки имеет идентификатор, имя и краткое описание. Для удобства пользования они сведены в таблицу.

Далее, рассматривается пример одной строки вышеупомянутой таблицы: M1036 – правила использования учетной записи. Здесь описана рекомендация по настройке функций учетных записей для предотвращения их взлома. В частности, описан метод взлома, именуемый Brute Force, который подразумевает перебор паролей. Для борьбы с подбором пароля к учетной записи, MITRE рекомендуют ограничивать время входа в учетную запись и устанавливать политики безопасности таким образом, чтобы учетная запись блокировалась после нескольких неудачных попыток входа.

Сравнение баз CAPEC и Att&ck

Альтернативой MITRE Att&ck является база CAPEC (*Common Attack Pattern Enumeration and Classification*, перечисление и классификация шаблонов атак) [7]. CAPEC представляет собой исчерпывающий словарь известных шаблонов атак, используемых злоумышленниками для эксплуатации известных недостатков системы. Она может использоваться аналитиками, разработчиками, тестировщиками для усиления защиты.

CAPEC сфокусирована на безопасности приложений и описывает общие атрибуты и методы, используемые злоумышленниками для эксплуатации известных уязвимостей в системах (например SQL *Injection*, XSS, *Session Fixation*, *Clickjacking*). Она включает социальную инженерию и связана с общим перечнем слабых мест Common Weakness Enumeration.

Att&ck, в свою очередь, фокусируется на защите сети и описывает этапы, конкретные тактики и методы, которые использует злоумышленник. Данная база может применяться для обнаружения злоумышленника, аналитики, анализа угроз, оценки защищенности, а также эмуляции противника и тестирования на проникновение. Решение всех этих задач важно для адекватного противодействия киберугрозам.

Применение Att&ck

Базу Att&ck рекомендуется применять постоянно. Своевременный анализ применяемых злоумышленником техник позволяет вовремя обнаружить критичные уязвимости системы, найти слабые и сильные стороны систем безопасности, выявить неверные конфигурации устройств или технические неполадки последних, что, в свою очередь, позволяет выбирать актуальные средства защиты.

Используя матрицу техник для исследования и тестирования известных способов применения конкретных методов, важно помнить о том, что всегда

существует несколько способов выполнения техник Att&ck, чтобы избежать появления пробелов в защите системы. Такие пробелы могут оставаться незамеченными специалистами по информационной безопасности, в то время как для злоумышленников они являются основной целью – точкой входа в систему. Необходимо оценивать эффективность существующих инструментов защиты и при необходимости производить их обновление [8].

Для описания поведения злоумышленника при помощи базы Att&ck и его детализации используется три характеристики [9]:

1) тактика – технические цели противника – какую цель стремится достигнуть злоумышленник в вашей системе (например, получить доступ к учетным данным);

2) техника – как злоумышленник достигает этих целей – какие уязвимости системы он использует;

3) процедуры – какие действия в системе выполняет злоумышленник для достижения своих целей.

Для понимания целостности картины происходящего, в системе необходимо собрать как можно больше деталей. В частности, важно определить тип злоумышленника. Он может быть сотрудником компании, клиентом, или не иметь никакого отношения к предприятию. Это может определять цели злоумышленника. Так, например, сотрудник или недовольный клиент могут иметь цель - отомстить компании. Нарушитель, не имеющий отношения к компании, обычно преследует цель – получить выгоду, чаще всего финансовую.

Определившись с типом нарушителя, необходимо выяснить – каким путем он может достичь поставленной цели, какими средствами он будет оперировать, и насколько серьезный ущерб принесут компании данные манипуляции. Затем необходимо определить порядок действий службы безопасности для предотвращения или предупреждения инцидента информационной безопасности.

Моделирование поведения злоумышленника при помощи базы Att&ck позволяет специалистам обнаружить уязвимости системы до того, как они будут проэксплуатированы, а, поставленные в соответствие различным типам поведения, средства предотвращения атак позволяют повысить уровень защищенности информационных систем, в том числе, систем индустриального интернета вещей.

Заключение

База Att&ck является историей, совершенных ранее, киберпреступлений, в ней описаны все известные техники и методы, которые использовали злоумышленники, а также существующие методы противодействия злоумышленникам. К ее достоинствам относятся: возможность автоматизации

процессов моделирования поведения злоумышленника, анализа защищенности на его основе, а также поддержки принятия решений по реагированию на атаки, в том числе, направленных на индустриальные системы. Кроме того, такая база является основой для связи высокоуровневого абстрактного описания поведения злоумышленника и процесса атаки с низкоуровневыми атрибутами, значения которых получены в результате наблюдения за реальной системой. К недостаткам Att&ck относится то, что она включает только известные тактики и методы. С каждым днем появляется все больше уязвимостей, которыми может воспользоваться злоумышленник, но для которых еще не придуманы методы противодействий. Это необходимо учитывать при применении баз данных безопасности для анализа и повышения защищенности информационных систем.

Работа выполнена при финансовой поддержке РФФИ (проект 19-07-01246).

Список используемых источников

1. Официальный сайт MITRE Att&ck [Электронный ресурс]. URL: https://attack.mitre.org/ (дата обращения 25.02.2020).

2. Att&ck makes defenders stronger by dissecting cyber adversary behavior [Электронный ресурс]. URL: https://www.mitre.org/publications/project-stories/attck-makes-defenders-stronger-by-dissecting-cyber-adversary-behavior (дата обращения 02.03.2020).

3. Blake Strom. ATT&CK 101 [Электронный ресурс]. URL: https://medium.com/mitre-attack/att-ck-101-17074d3bc62 (дата обращения: 03.03.2020).

4. ATT&CK® for Industrial Control Systems [Электронный ресурс]. URL: https://collaborate.mitre.org/attackics/index.php/Main_Page (дата обращения 15.03.2020).

5. Enterprise Mitigations [Электронный ресурс]. URL: https://attack.mitre.org/mitigations/enterprise/ (дата обращения 21.03.2020).

6. Mobile Mitigations [Электронный ресурс]. URL: https://attack.mitre.org/mitigations/mobile/ (дата обращения 21.03.2020).

7. ATT&CK Comparison [Электронный ресурс]. URL: https://capec.mitre.org/about/attack_comparison.html (дата обращения 26.03.2020).

8. What Is MITRE ATT&CK and How Is It Useful [Электронный ресурс]. URL: https://www.anomali.com/resources/what-mitre-attck-is-and-how-it-is-useful (дата обращения 27.03.2020).

9. Frequently Asked Questions [Электронный ресурс]. URL: https://attack.mitre.org/resources/faq/ (дата обращения 05.03.2020).

УДК 004.056
ГРНТИ 81.93.29

ПРОГНОЗИРОВАНИЕ ПОВЕДЕНИЯ АТАКУЮЩЕГО С ИСПОЛЬЗОВАНИЕМ МЕТОДОВ ИНТЕЛЛЕКТУАЛЬНОГО АНАЛИЗА ДАННЫХ

Е. В. Дойникова[1,2], Е. С. Новикова[2]

[1]Санкт-Петербургский государственный университет телекоммуникаций им. проф. М. А. Бонч-Бруевича
[2]Санкт-Петербургский институт информатики и автоматизации Российской академии наук

Раннее обнаружение инцидентов безопасности и корректное прогнозирование их развития в анализируемой системе является основой для эффективного и своевременного реагирования. Развитие атаки зависит от доступных злоумышленнику шагов атаки, а также его целей и «профиля», который определяет поведение атакующего в системе. Под «профилем» атакующего понимается набор его характеристик, как внутренних, таких как мотивы или квалификация, так и внешних, таких как финансовые возможности или используемые инструменты. Определение характеристик атакующего позволит определить тип атакующих, которых привлекает анализируемая система, и сложность защитных мер, которые необходимо реализовать. Цель работы – проанализировать существующие методики определения поведения атакующего, «профиля» атакующего и, его применения для прогнозирования дальнейших шагов и целей атаки. На основе проведенного анализа выделены виды существующих подходов к прогнозированию развития атак и формированию «профиля» атакующего, а также существующие в данной области сложности и возможные варианты их преодоления. Предложен подход к прогнозированию целей атакующего.

инцидент безопасности, атакующий, прогнозирование, профиль атакующего, характеристики, цели атаки.

Определение модели атакующего является одним из важных этапов анализа защищенности информационных систем от кибератак. От нее зависят результаты анализа защищенности и выбор защитных мер для целевой информационной системы. Кроме того, модель атакующего может использоваться при решении задач цифровой криминалистики. На сегодняшний день разработан ряд моделей атакующего. Их можно разделить на модели верхнего уровня абстракции и модели низкого уровня абстракции. Под моделью верхнего уровня абстракции будем понимать модель, в рамках которой, для определения класса атакующего используются верхнеуровневые атрибуты. К таким атрибутам относятся: цель, положение атакующего (внутренний или внешний), сложность используемых уязвимостей (низкая, средняя или высокая). Используя эти атрибуты, можно отнести атакующего к одному из классов, такому как хакеры, шпионы,

террористы, корпоративные рейдеры, профессиональные преступники, вандалы, или вуайеристы [1].

Под моделью низкого уровня абстракции будем понимать модель, в рамках которой для определения атакующего используются низкоуровневые атрибуты (или признаки). К таким атрибутам относятся: порт получателя, сигнатура предупреждения, порт источника, хост, и т. п. Модель такого типа используется, чтобы определить не только класс атакующего, но и его/ее модель поведения или даже конкретную личность.

Модели первого типа обычно используются в рамках следующих подходов к определению класса атакующего и анализу кибератак: подходы, основанные на построении и анализе графов атак. Модели второго типа обычно используются в рамках следующих подходов: подходы, основанные на скрытых Марковских моделях; подходы, основанные на нечеткой логике; подходы, основанные на атрибуции кибератак с использованием методов интеллектуального анализа данных, включая нейронные сети, статистические методы, и др.

Вторая группа подходов выглядит предпочтительнее, т. к. дает более точные результаты, основанные на измерении характеристик анализируемой системы в процессе атаки. Это позволяет определить высокоуровневые характеристики атакующего на основе низкоуровневых характеристик. Поэтому в рамках данной работы разрабатывался подход к прогнозированию поведения атакующего и развития атаки на основе отношений между признаками «сырых» данных безопасности и атрибутами атакующего, определяющих его или ее «профиль» и поведение.

В процессе исследования были проанализированы работы, использующие различные подходы к определению «профиля» атакующего и прогнозированию его/ее поведения. В результате чего были выявлены следующие основные проблемы в этой области, которые необходимо преодолеть для реализации заявленного подхода:

1) отсутствие единообразия при классификации атакующих, метрик и атрибутов, а также определений одних и тех же классов и метрик;

2) пробел между «сырыми» данными (такими как сетевой трафик и журналы событий), «профилем» атакующего, и прогнозированием поведения атакующего, а также отсутствие методов обнаружения отношений между ними;

3) отсутствие размеченных наборов данных, подходящих для исследования отношений между шагами атакующих и их целями;

4) отсутствие исследований, подтверждающих, что профилирование и атрибуция атакующих существенно влияют на прогнозирование атак.

Решить проблемы отсутствия единообразия попытались авторы работы [2]. Они выделили ряд признаков для описания атакующего из «сырых» данных, а также определили верхнеуровневые атрибуты атакующего,

однако не рассмотрели вторую выделенную проблему, связанную с определением отношений между ними. Попытка решить вторую проблему была сделана в рамках проекта STIX (*Structured Threat Information Expression*, структурированное представление информации об угрозах) [3]. Сам STIX представляет собой язык для определения угроз и их автоматического анализа. Тем не менее, остается неясным как автоматически определить низкоуровневые атрибуты из «сырых» данных и связать их с верхнеуровневыми атрибутами. Вторая проблема тесно связана с третьей, состоящей в отсутствии подходящих наборов данных для анализа и обнаружения отношений между нижнеуровневыми и верхнеуровневыми атрибутами. В настоящее время для решения этой проблемы используются следующие подходы:

1) использование существующих наборов данных для конкретных атак;

2) использование honeypot для генерации данных;

3) использование нормальных данных и добавление в них данных об атаках (генераторы атак).

Отсутствие подходящих наборов данных может также объясняться тем, что до конца неясно, существует ли необходимость профилирования атакующего для прогнозирования развития атаки. Как следствие, существующие наборы данных обычно не размечены с точки зрения разных типов атакующих. Поэтому необходимо также решить четвертую проблему, связанную с проведением исследования, демонстрирующего наличие или отсутствие влияния профилирования атакующего на точность прогнозирования развития атаки.

Для прогнозирования поведения атакующего в рамках данного исследования предлагается следующий подход:

1. Выделение источников «сырых» данных. Данные можно разделить на структурированные и неопределенные. К источникам структурированных данных безопасности относятся [4]:

базы уязвимостей,

базы шаблонов атак,

базы слабых мест,

базы программного и аппаратного обеспечения, и др.

К неопределенным данным отнесем сетевой трафик и журналы событий.

2. Извлечение признаков из наборов данных сетевого трафика и событий для формирования низкоуровневых атрибутов, определяющих «профиль» атакующего.

3. Определение и классификация верхнеуровневых атрибутов, определяющих «профиль» атакующего.

4. Выявление структурных и семантических отношений между источниками данных, объектами предметной области и метриками.

5. Использование вышеупомянутых атрибутов и отношений между ними для:

разработки алгоритмов вычисления метрик (определения значений, соответствующих верхнеуровневым атрибутам, на основе значений, соответствующих нижнеуровневым атрибутам);

обучение нейронечеткой сети для прогнозирования поведения атакующего.

Для успешного выполнения 5-го этапа подхода, необходимо выполнить первые четыре этапа и решить четыре выделенных проблемы. Это является направлением будущих исследований.

Таким образом, в данном исследовании были проанализированы существующие модели и подходы в области прогнозирования поведения атакующего и выделены ключевые проблемы в данной области. Кроме того, был предложен общий подход к прогнозированию поведения атакующего с использованием методов интеллектуального анализа данных. В будущем исследовании планируется определить все этапы предложенного подхода.

Работа выполнена при финансовой поддержке стипендии президента РФ (СП-751.2018.5).

Список используемых источников

1. Howard J. D., Longstaff T. A. A Common Language for Computer Security Incidents: report. Sandia National Labs. Albuquerque, NM, USA and Livermore, CA, USA, 1998. 32 p.

2. Rocchetto M., Tippenhauer N. O. On Attacker Models and Profiles for Cyber-Physical Systems // Lecture Notes in Computer Science : proceedings of the ESORICS, 2016 / Eds. Askoxylakis I., Ioannidis S., Katsikas S., Meadows C., Springer: Cham, Switzerland, 2016.

3. Structured Threat Information eXpression (STIX™) 1.x Archive Website [Электронный ресурс]. URL: https://stixproject.github.io/ (дата обращения 31.03.2020).

4. Kotenko I., Fedorchenko A., Doynikova E., Chechulin A. An Ontology-based Hybrid Storage of Security Information // Inf. Technol. Control. 2018. N 47. P. 655–667.

УДК 004.056
ГРНТИ 81.93.29

АНАЛИЗ ПРОБЛЕМ, ИХ ВОЗМОЖНЫХ РЕШЕНИЙ, А ТАКЖЕ СУЩЕСТВУЮЩИХ ПЕРСПЕКТИВ В ОБЛАСТИ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ БЕСПРОВОДНЫХ МЕДИЦИНСКИХ УСТРОЙСТВ

Е. В. Дойникова[1,2], А. Н. Полубарьева[3]

[1]Санкт-Петербургский институт информатики и автоматизации Российской академии наук
[2] Санкт-Петербургский государственный университет телекоммуникаций им. проф. М.А. Бонч-Бруевича
[3]Национальный исследовательский университет ИТМО

В работе проведен анализ актуальности информационной безопасности для беспроводных медицинских устройств. Проведен анализ уязвимостей медицинских устройств, стандартов и требований в данной области. В рамках исследования были выделены существующие и прогнозируемые проблемы, которые стоят перед медицинскими учреждениями, намеревающимися обеспечить информационную безопасность при передаче данных по сети, и производителями беспроводных медицинских устройств. Приведены варианты решений выделенных проблем. Задача исследования состоит в том, чтобы показать «интернет уязвимых вещей», в частности, беспроводных медицинских устройств, функционирующих в киберфизических системах при переходе к стандарту Индустрии 4.0, а также негативные последствия нарушения информационной безопасности в данной сфере, как для отдельного человека, так и для общества и государства в целом.

информационная безопасность, индустрия 4.0, умная медицина, интернет вещей, беспроводные устройства.

Актуальность ИБ для беспроводных медицинских устройств

Информационная безопасность (ИБ) беспроводных медицинских устройств с каждым годом становится все более обсуждаемым вопросом. В Российской Федерации (РФ) защите медицинских учреждений (МУ), медицинских данных и медицинского оборудования (МО) уделяется мало внимания. При этом стоимость одной медицинской карточки на черном рынке может составлять в 10–20 раз больше, чем информация о кредитной карте. Высокая ценность хранимых и используемых медицинскими учреждениями данных объясняет, почему в 2019 г. здравоохранение подверглось большему количеству кибератак, чем другие отрасли [1]. Неадекватные методы обеспечения ИБ, устаревшие системы и программы, слабые пароли и уязвимости открывают для злоумышленников путь к манипуляциям с данными учреждений здравоохранения. Согласно данным Министерства национальной

безопасности США и Управления пищевых продуктов и лекарственных средств США, множество уязвимостей существует в автоматах по продаже лекарств и в помпах по вливанию лекарственных препаратов. Кроме того, с развитием применения в здравоохранении облачных технологий и систем интернета вещей, растет их уязвимость. Согласно [2] в 2019 г. «умное здравоохранение» лидирует в качестве цели киберпреступников.

Согласно статистическим данным [3], за последние годы изменился характер нарушений кибербезопасности в сфере медицины. С 2009 по 2015 гг. большую часть нарушений составляли хищения и потеря данных пациентов и информации о здоровье, хранящейся в электронном виде. В начале 2016 г. рост киберпреступлений с помощью программ-вымогателей составил 320 % по сравнению с 2015 г. [4]. В последние годы наибольшее число нарушений связано с хакерскими действиями и инцидентами в компьютерных системах. С 2017 по 2020 гг. количество атак на МУ с помощью программ-вымогателей увеличилось в четыре раза. По прогнозам, к 2021 г. их количество увеличится в пять раз, по сравнению с предыдущими годами, что приведет к увеличению спроса со стороны МУ на продукты по защите в сфере ИБ. Также изменились векторы проведения кибератак. Раньше большему воздействию подвергалась конфиденциальность данных, теперь МУ чаще сталкиваются с компрометацией доступности и целостности данных.

Все вышесказанное показывает, что существующих мер защиты МУ и МО недостаточно, и требуется изменение стратегий обеспечения информационной безопасности в сфере здравоохранения. В данной работе были исследованы опыт и стандарты США и стран ЕС. С внедрением в РФ «умного здравоохранения» необходимо заранее предусмотреть все возможные риски, используя опыт этих стран.

Стандарты и требования в области кибербезопасности медицинских учреждений и медицинского оборудования

В ЕС основным документом, регулирующим вопросы безопасности данных, является GDPR (*General Data Protection Regulation*), в США – HIPAA (*Health Insurance Portability and Accountability* Act, 1996) и HITECH (*Health Information Technology for Economic and Clinical Health*) Act of 2009. Подобные специализированные законы, нормативно-правовые акты (НПА), а также, на законодательном уровне закрепленные, стратегии кибербезопасности имеются практически в каждой стране. В РФ такие стандарты и требования находятся на стадии становления, именно поэтому важно уже сейчас изучать опыт стран, где такие НПА уже действуют. Отметим, что для обеспечения необходимого уровня ИБ в здравоохранении, все, причастные к инфраструктуре здравоохранения, компании и лица должны четко понимать, какие стандарты должны соблюдаться, и эти стандарты должны быть одинаковыми и строгими для всех.

«Интернет медицинских вещей» и переход к индустрии 4.0

В сфере «умной медицины» появился достаточно новый термин – «интернет медицинских вещей». Он состоит из инфраструктуры и различных медицинских устройств, соединяющихся по сети [5]. Выделяются следующие типы «медицинских вещей»: умные носимые устройства (мониторы частоты сердечных сокращений, уровней пота, уровня кислорода в крови и уровня алкоголя); медицинские приборы домашнего использования (мониторы глюкозы, измерители артериального давления, инсулиновые помпы); имплантируемые устройства (дефибрилляторы кардиовертеров, кардиостимуляторы); наборы для оказания медицинской помощи (диагностические тесты, анализаторы); системы экстренного реагирования (реагирование на сигналы тревоги); виртуальные домашние помощники (например, контролеры соблюдения рецептов); киоски выдачи медицинских изделий; датчики (RFID) в упаковках для фармацевтических препаратов; мобильные приложения для здравоохранения.

С развитием технологий общее количество подключенных медицинских устройств растет. К преимуществам таких устройств относятся: немедленный доступ к результатам анализов или рентгеновским снимкам как для пациента, так и для врача; доступ в режиме реального времени к медицинским данным; простая аналитика с помощью датчиков и исполнительных механизмов; автоматическая корреляция данных из разных источников; предупреждения о вреде для здоровья в случае постоянного мониторинга; дистанционный мониторинг хронических заболеваний; легкое управление лекарственными средствами с помощью электронных рецептов; снижение затрат на здравоохранение. Перечисленные особенности «интернета медицинских вещей» дают основание предполагать его дальнейшее развитие, а, следовательно, и задач в сфере обеспечения его ИБ и соответствующих стандартов.

Наиболее важные слабые места МУ и способы их устранения

Согласно [6] существует 20 наиболее важных для МУ слабых мест, которые необходимо учитывать при обеспечении их ИБ. К ним относятся: внутренний нарушитель (множество атак осуществляются в виде фишинга, социальной инженерии и подобных методов, также встречаются случаи корпоративного шпионажа и иной криминальной деятельности); наличие третьей стороны (связь контрагентов с компьютерной сетью МУ); подключенные к сети медицинские устройства (медицинские мониторы, МРТ, компьютерный томограф могут иметь уязвимости, которыми может воспользоваться злоумышленник); злой умысел и целенаправленные атаки; мобильные устройства (представляют собой дополнительную точку входа для атак); уязвимость к кражам или мошенническим манипуляциям с меди-

цинскими персональными данными; уязвимость к организованным киберпреступлениям; уязвимость к атакам, спонсируемым и поддерживаемым государствами; устаревшие операционные системы (ОС) и программы, и др. Отметим, что для разных МУ могут быть, в большей или меньшей степени, характерны разные слабые места.

В качестве основной меры, предлагаемой для защиты от внутренних угроз, выступают тренинги для персонала. Для защиты от угроз, представляемых третьей стороной, рекомендуется составление соглашений, в которых будут оговорены все вопросы ИБ и ответственности сторон. Для защиты от атак, реализуемых за счет уязвимостей подключенных устройств, предлагается вывести их в отдельный сегмент сети. Для защиты от целенаправленных атак и организованных киберпреступлений применяется обучение персонала, кроме того, важна усиленная защита на конечных точках. Для защиты от атак, реализуемых через мобильные устройства, все принесенные персоналом МУ мобильные устройства должны проходить дополнительную проверку. Для защиты персональных данных от кражи необходимо проводить тренинг персонала, кроме того, необходимо применять средства защиты данных. Защитой от устаревших ОС и программ является инвентаризация и своевременное обновление ОС и техники. Для обеспечения высокого уровня ИБ все эти решения должны приниматься комплексно.

При переходе к «умной медицине», проблемы ИБ в здравоохранении становятся еще более актуальными. Выделим следующие важные для ИБ особенности МУ в контексте «умной медицины» [5]:

1) уязвимости оборудования, приобретенного без учета аспектов ИБ;

2) взаимосвязанность устройств, что приводит к возможности распространения атак и ущерба от них по сети;

3) однородность Интернета вещей, как следствие – достаточно обнаружить уязвимость в одном МО, чтобы скомпрометировать другое подобное МО;

4) отсутствие моделей угроз и моделей нарушителей для специфического МО;

5) отсутствие тренингов для персонала МУ;

6) персональная медицинская информация считается даже более ценной, чем финансовая информация.

Отметим, что ИБ медицинских устройств должна закладываться еще на этапе их проектирования и производства, с учетом их возможного подключения к компьютерным сетям. В качестве одного из инструментов по обеспечению безопасности МО и медицинских устройств выступают эталонные архитектуры для проектирования МУ. Примером является эталонная архитектура ISOSCELES (*Intrinsically Secure, Open, and Safe Cyber-Physically Enabled, Life-Critical Essential Services*), целью которой является ИБ медицинских устройств [7]. Она основана на принципах проектирования

медицинских устройств, изоляции программных компонентов на основе гипервизора и других технологий разделения. При этом создание архитектуры для конкретных медицинских устройств поддерживается процессом разработки на основе анализа архитектуры и языка проектирования. Архитектурные модели поддерживают анализ безопасности и защиты как часть более широкой структуры управления рисками. Эталонная архитектура ISOSCELES нацелена на небольшие подключенные медицинские устройства (инфузионные помпы, электрокардиографы, вентиляторы). Она предполагает наличие четырех уровней:

1) аппаратного обеспечения;

2) разделительный уровень;

3) платформы;

4) приложений конкретного медицинского устройства (например, инфузионная помпа).

К каждому уровню предъявляются свои требования для обеспечения ИБ. Разделительный уровень вводится для изоляции программных компонентов друг от друга, за исключением специально разрешенных взаимодействий.

Заключение

Здравоохранение – элемент критической инфраструктуры, привлекательный для злоумышленников. При переходе к формату Индустрии 4.0, с развитием «интернета медицинских вещей», растет уязвимость данной отрасли к кибератакам. Медицинские устройства, оборудование, системные компоненты и сети становятся автономными, вездесущими и взаимосвязанными. Хотя обеспечению их информационной безопасности уделяется внимание, статистика кибератак указывает на недостаточность усилий в данной области. Как следствие, перед системой здравоохранения стоит задача создания новых стандартов, подходов и методов обеспечения информационной безопасности устройств в течение всего жизненного цикла.

Список используемых источников

1. 2019 Cybersecurity Almanac: 100 Facts, Figures, Predictions and Statistics, Cybercrime magazine, 06.02.2019 [Электронный ресурс]. URL: https://cybersecurityventures.com/cybersecurity-almanac-2019/(дата обращения 29.02.2020).

2. 82 % IoT Devices of Health Providers, Vendors Targeted by Cyberattacks [Электронный ресурс]. URL: https://healthitsecurity.com/news/82-iot-devices-of-health-providers-vendors-targeted-by-cyberattacks (дата обращения 29.02.2020).

3. Healthcare Data Breach Statistics, HIPAA Journal [Электронный ресурс]. URL: https://www.hipaajournal.com/healthcare-data-breach-statistics/ (дата обращения 29.02.2020).

4 Сборник Законов о передаче данных и учёте в системе медицинского страхования. Разработка правил. Окончательные правила в федеральном реестре [Электронный ресурс] // Министерство здравоохранения и социального обеспечения США: электрон.

журн., 25 янв. 2013. URL: https://www.hhs.gov/hipaa/for-professionals/privacy/laws-regulations/combined-regulation-text/omnibus-hipaa-rulemaking/index.html (дата обращения 29.02.2020).

5. Безопасность Умных госпиталей и устойчивость умных медицинских услуг и инфраструктуры [Электронный ресурс] // Отчет Агентства Европейского союза по кибербезопасности, 24 нояб. 2016 г. URL: https://www.enisa.europa.eu/publications/cyber-security-and-resilience-for-smart-hospitals (дата обращения 29.02.2020).

6. The Top 20 Security Vulnerabilities Healthcare Organizations Should Address, by John Nye, specialist of a Cynergistek, 16.05.2018 [Электронный ресурс]. URL: https://insights.cynergistek.com/information-security-officer/the-top-20-security-vulnerabilities-healthcare-organizations-should-address (дата обращения 29.02.2020).

7. Харп С., Карпентер Т., Хэтклифф Дж. Эталонная архитектура для обеспечения безопасности медицинских устройств // Биомедицинский инструментарий и технологии. 2018. № 5. С. 27–29.

УДК 004.056
ГРНТИ 49.33.35

СОВРЕМЕННЫЕ МЕХАНИЗМЫ БЕЗОПАСНОСТИ БЕСПРОВОДНЫХ СЕТЕЙ

А. Д. Докшин, А. А. Киселева, Д. В. Юркин

Санкт-Петербургский государственный университет телекоммуникаций им. проф. М. А. Бонч-Бруевича

Одной из быстро развивающихся современных телекоммуникаций является беспроводная вычислительная сеть. При этом для данных сетей очень актуален вопрос безопасности и защиты передаваемых данных. Созданные в этой сфере технологии, изначально имели низкую степень защиты. Группа стандартов связи беспроводной сети IEEE 802.11 с момента создания и до нашего времени претерпела множество изменений, в том числе, усовершенствовались и механизмы безопасности. В статье проведено исследование, затрагивающие последние изменения в разделе безопасности, описаны принципы построения безопасности в механизмах Wi-Fi Protected Access 2 и 3. Статья будет полезна для быстрого ознакомления с современными механизмами безопасности беспроводных сетей.

беспроводная сеть, механизмы безопасности сети, Wi-Fi, IEEE 802.11, WPA2, WPA3.

Беспроводные локальные сети стремительно набирают популярность. Устройства, поддерживающие технологии беспроводного доступа, уже не кажутся невероятными и труднодоступными. Но, как и множество других инновационных технологий, использование беспроводных сетей влечет не только положительные, но и отрицательные последствия. Появление возможности беспроводного соединения породило ряд новых способов

взлома сети и атак пользователей и корпоративной инфраструктуры, поэтому безопасность является одной из основных задач в области беспроводной связи. Защита радиоканала от несанкционированного воздействия нарушителем в беспроводных сетях осуществляется за счет внедрения криптографических протоколов удостоверения подлинности, имитозащиты и шифрования данных, автоматического, безопасного и достоверного распределения ключевого материала на канальном уровне модели OSI/ISO.

Wi-Fi Protected Access 2 (WPA2) [1] на сегодняшний день является обязательным в использовании при построении корпоративной сети. WPA2 – механизм, основанный на стандарте IEEE 802.11 [2] и предназначенный для аутентификации беспроводных устройств с использованием протокола Advanced Encryption Standard (AES), и служащий для предотвращения подслушивания хакерами данных, передаваемых беспроводным путём. Шифрование передаваемых данных обеспечивается протоколом блочного шифрования с имитовставкой и режимом сцепления блоков и счётчика (*Counter Mode with Cipher Block Chaining Message Authentication Code Protocol* – CCMP) [3]. Используя надежный предварительный общий ключ или аутентификацию 802.1X, CCMP невозможно взломать, потому что единственной возможностью становится проверка возможных ключей, то есть 2^128 ключей.

В 2009 году Институт инженеров электротехники и электроники (IEEE) утвердил поправки к стандарту 802.11 – 802.11w-2009 – для повышения безопасности его кадров управления [4]. Цель поправок заключается в повышении безопасности путем обеспечения конфиденциальности данных кадров управления, механизмов, обеспечивающих целостность данных, подлинность источника данных.

Защита кадров управления *(Protected Management Frames* – PMF) включает в себя обеспечение безопасности кадров управления, передаваемых после того, как точка доступа и станция согласуют обмен ключами. Кадры управления, отправленные до обмена ключами, по-прежнему не будут зашифрованы. Таким образом, подвергаются шифрованию следующие кадры: «Disassociation frames», «De-authentication frames» и «Action management frames».

Введение защищенных кадров управления решило проблему возникновения атаки, направленной на принудительное отключение клиента от легитимной точки доступа и подключение к точке доступа злоумышленника. При использовании механизма PMF кадры управления подписываются ключом, известным только авторизованным клиентам и легитимным точкам доступа. В результате чего, клиент может определить, от легитимной ли точки доступа получен данный кадр.

Кроме того, поправка 802.11w предоставила новый ключ IGTK – временный ключ группы целостности. IGTK используется для проверки целостности кадров управления широковещательной и многоадресной передачей и для вычисления кода целостности сообщения (MIC – *Message Integrity Code*) для этих кадров.

Поправки IEEE 802.11w также добавлены в механизм WPA2.

В 2018 году организация Wi-Fi Alliance анонсировала новый механизм безопасности Wi-Fi Protected Access 3 (WPA3) [5]. Представлен новый метод аутентификации устройства Simultaneous Authentication of Equals (SAE). SAE – это вариант установления связи по методу стрекозы (*dragonfly handshake*), использующего криптографию для предотвращения угадывания пароля злоумышленником. SAE заменяет метод Pre-Shared Key (PSK). SAE работает на основании предположения о равноправности устройств, таким образом, любая из сторон может отправить запрос на соединение, после чего устройства начинают независимо друг от друга отправлять удостоверяющую их информацию. При каждом новом соединении устанавливается новый шифрующий пароль, поэтому даже если атакующий в какой-то момент проникнет в сеть, он сможет украсть только пароль от данных, переданных после этого момента. Кроме того, защищенные кадры управления являются обязательными в режиме WPA3-SAE.

WPA3-Enterprise обладает шифрованием в 192 бита. На сегодняшний день Wi-Fi работает с безопасностью в 128 бит. Безопасность в 192 бита, при использовании механизма WPA3, не является обязательной, но представляет собой усиление безопасности WLAN. Шифрование в 192 бита целесообразно использовать в корпоративной сети, особенно, если происходит обработка критически значимой информации.

Чтобы гарантировать подобающий уровень безопасности всей сети, в WPA3-Enterprise предлагается использовать следующие протоколы и методы: 256-битный протокол Galois/Counter Mode для шифрования, 384-битный Hashed Message Authentication Mode режим для создания и подтверждения ключей, и алгоритмы Elliptic Curve Diffie-Hellman exchange, Elliptic Curve Digital Signature Algorithm для аутентификации ключей. При этом на каждом шагу должно поддерживаться шифрование в 192 бита.

Кроме того, представлена технология Wi-Fi Easy Connect, предназначенная для упрошенного подключения и быстрой настройки устройств Wi-Fi. Wi-Fi Easy Connect включает в себя надежное шифрование с помощью криптографии с открытым ключом, чтобы обеспечить безопасность сетей при добавлении новых устройств. Упрощается инициализация благодаря использованию QR-кодов и выбранного пользователем устройства для управления доступом к сети. Также Wi-Fi Easy Connect позволяет заменять точки доступа без необходимости повторной регистрации всех устройств.

Следует также упомянуть об отдельном протоколе Enhanced Open, разработанном для защиты пользователя в открытой сети. Enhanced Open использует оппортунистическое беспроводное шифрование (OWE), определённое в стандарте IETF RFC 8110, чтобы защищаться от пассивного подслушивания. В этом случае не требуется дополнительная защита с аутентификацией, так как OWE концентрируется на улучшении шифрования данных, передаваемых по публичным сетям, с целью предотвратить их кражу. OWE предотвращает инъекцию пакетов, предназначенную для нарушения работы сети путем создания и передачи пакетов данных, которые выглядят как нормальная работа сети.

Введение нового механизма безопасности беспроводных сетей WPA3 должно избавить от некоторых атак, например, Key Reinstallation Attacks (KRACKs). С помощью данной атаки появляется возможность прервать серию рукопожатий (4-*way handshake*) и ввести в заблуждение, что соединение с маршрутизирующим устройством временно разорвалось. На самом деле в этот момент производится анализ рукопожатий до того момента, пока нужный пароль не будет получен. WPA3 предоставляет решение: протокол SAE блокирует возможность подобных атак.

Несмотря на, казалось бы, совершенные методы безопасности, представленные в WPA3, атаки на данный механизм уже существуют. Эксперты в области безопасности Мати Ванхойф (*Mathy Vanhoef*) и Эйал Ронен (*Eyal Ronen*) представили возможные уязвимости в реализации WPA3-Personal [6].

Во-первых, это атака, связанная с переходным режимом работы для устройств (связано с тем, что какое-то время многие устройства смогут поддерживать только механизм WPA2). При этом, устройства с поддержкой WPA3 подключаются с помощью WPA2.

Во-вторых, атака по побочному каналу на основе кэша. Алгоритм кодирования пароля в SAE (методе «стрекозы») содержит условные ветви. Если злоумышленник может запустить непривилегированный код на компьютере-жертве, возможно использовать атаки на основе кеша, чтобы определить, какая ветвь была предпринята в первой итерации алгоритма генерации пароля. Эта информация может быть использована для выполнения атаки с разделением пароля.

В-третьих, атака по побочному каналу на основе синхронизации. Когда при рукопожатии по методу «стрекозы» используются определенные мультипликативные группы, алгоритм кодирования пароля использует переменное число итераций для кодирования. Точное количество итераций зависит от используемого пароля и MAC-адреса точки доступа и клиента. Злоумышленник может выполнить временную атаку на алгоритм кодирования пароля для определения количества итераций, требуемых для кодирования этого

пароля. Восстановленная информация может быть использована для выполнения парольной атаки.

Однако, данные уязвимости можно отследить специальными инструментами: Dragondrain, Dragontime, Dragonforce и Dragonslayer, и перекрыть на своих устройствах программным путем.

В таблице сведены параметры безопасности, относящиеся к каждому из механизмов WPA2 и WPA3.

ТАБЛИЦА. Параметры безопасности механизмов WPA2 и WPA3

Параметр безопасности	WPA2	WPA3
Поддерживаемые режимы безопасности	Personal, Enterprise	Personal, Enterprise
Шифрование	Counter Mode with Cipher Block Chaining Message Authentication Code Protocol с использованием AES (CCMP + AES)	256-битный протокол Galois/Counter Mode Protocol (GCMP-256)
Целостность данных	Cipher Block Chaining Message Authentication Code (CBC-MAC)	384-bit Hashed Message Authentication Mode (HMAC) with Secure Hash Algorithm (SHA)
Длина ключа, бит	128	192
Управление ключами	4-way handshake (4-этапное рукопожатие)	Elliptic Curve Diffie-Hellman (ECDH)
Протокол обмена ключами	Pre-Shared Key (PSK)	Simultaneous Authentication of Equals (SAE)
Защита кадров управления	Не все устройства поддерживают	Обязательно к использованию
Стандарт упрощенного создания беспроводного соединения	Wi-Fi Protected Setup (WPS)	Wi-Fi Easy Connect с использованием Device Provisioning Protocol (DPP)

Безопасность беспроводных сетей остается одним из главных вопросов в области телекоммуникаций. Создание новых методов и технологий защиты беспроводных сетей порождает новые атаки и механизмы взлома. Поэтому необходимо тщательно подходить к процессу создания беспроводной сети, подбирать средства защиты и исключать возможность появления нелегитимных точек доступа. Также важно проводить постоянное изучение механизмов безопасности с целью выявления новых уязвимостей для дальнейшего повышения уровня безопасности беспроводных сетей.

Список используемых источников

1. Lashkari A. H., Danesh M. M. S., Samadi B. A survey on wireless security protocols (WEP, WPA and WPA2/802.11i) // The 2nd IEEE International Conference on Computer Science and Information Technology. 2009. N 2. PP. 48–52.

2. Benton K. The Evolution of 802.11 Wireless Security // UNLV Informatics-Spring. 2010. N 795. PP. 1–56.

3. Ковцур М. М., Юркин Д. В. Основы защиты информации в беспроводных локальных сетях: методич. указания. СПбГУТ, 2016. 61 с.

4. IEEE Std 802.11w-2009. Telecommunications and information exchange between systems. Local and metropolitan area networks. Specific requirements. Wireless LAN Medium Access Control and Physical Layer Specifications. Protected Management Frames. : IEEE SA-Standards Board, 2009. 91 c.

5. Discover Wi-Fi. Security [Электронный ресурс]. URL: https://www.wi-fi.org/discover-wi-fi/security (дата обращения 10.03.2020).

6. Vanhoef M, Ronen E. Dragonblood: Analyzing the Dragonfly Handshake of WPA3 and EAP-pwd // Proceedings of the 2020 IEEE Symposium on Security and Privacy-S&P. 2020. PP. 808–824.

УДК 004.77
ГРНТИ 49.33.29

РАЗРАБОТКА МЕТОДИКИ ТЕСТИРОВАНИЯ SDN-КОНТРОЛЛЕРА НА ОСНОВЕ МОДЕЛЕЙ СЕТИ 5G

А. А. Долгомер, А. С. А. Мутханна

Санкт-Петербургский государственный университет телекоммуникаций им. проф. М. А. Бонч-Бруевича

Технологии сетей связи пятого поколения 5G/IMT-2020 являются относительно новой и перспективной парадигмой в развитии глобальной сетевой архитектуры. В статье будет выполнен обзор архитектур по организации сервисов сетей пятого поколения и существующего программного обеспечения (утилит) для проведения тестирования модельной сети, находящейся в свободном доступе.

модельная сеть, SDN, тестирование, контроллер, 5G.

Введение

Количество подключенных устройств IoT будет составлять от 10 до 12 миллиардов к 2021 году [1], что вызывает необходимость введения новой сетевой архитектуры. Она обязана обеспечивать потребности клиента за счёт введения новых технологий и сервисов, таких как связь между устройствами (D2D), туманные и пограничные мобильные вычисления [2]. Все эти процедуры подразумевают правильное распределение ресурсов между несколькими службами, что является нелёгкой задачей. В настоящее время происходит разработка архитектур MEC и FOG [3].

В данной работе будет выполнено тестирование модельной сети 5G. Результатом станет вывод о пригодности использования технологий интеллектуальных вычислений в архитектуре сетей нового поколения.

Структура лабораторного стенда и модельной сети

Для проведения тестирования архитектуры по организации сервисов для сетей 5G/IMT-2020 использовалась и дорабатывалась модельная сеть лаборатории «Программируемые сети» кафедры Сетей связи и передачи данных. Для реализации взаимодействия физической и виртуальной программно-конфигурируемой сети, и оборудования использовался OpenFlow контроллер OpenDayight версии Berilium SR-4 с открытым исходным кодом (*open-source*). В качестве OpenFlow коммутаторов был выбран виртуальный коммутатор OpenVSwitch, имеющий поддержку протокола OpenFlow 1.3, посредством которого происходило управление логикой коммутации. Также использовались сервер с платформой, основанной на Linux, и гипервизоре KVM с установленным на нем программным обеспечением Internet of Things Data Management (IoTDM), который осуществляет функции централизованного сбора и управления Интернет вещами. Для соединения физического сегмента и NFV сегмента программно-конфигурируемой сети (виртуального и физического) использовались коммутаторы Cisco Catalyst 3750g. В качестве полезной нагрузки в сети используется трафик Интернета вещей, который генерируется с помощью программного обеспечения «Генератор трафика Интернета вещей по протоколу Http», разработанного специалистами лаборатории «Программируемые сети» кафедры Сетей связи и передачи данных.

Результаты тестирования

Исследование использования ресурсов SDN-контроллера модельной сети в режиме Unit-тестирования, в зависимости от частоты подключения/отключения виртуальных машин (10s,1s,100ms,10ms,1ms), с помощью ПО «Трафик-генератор виртуальных машин. На рис. 1–5 (см. ниже) представлены результаты данного исследования.

Заключение

Анализ результатов тестирования SDN-контроллера программным обеспечением «Генератор трафика виртуальных машин» показал, что контроллер OpenDaylight Beryllium SR4 пригоден для масштабирования. Присутствует возможность построения стабильно работающей сети, которая достаточна гибкая для масштабирования, что показывают графики производительности, оперативной памяти и состояния сети.

Рис. 1. Использование ресурсов процессора, оперативной памяти и состояния сети SDN-контроллера модельной сети в режиме Unit-тестирования при частоте подключения/отключения ВМ 10 секунд

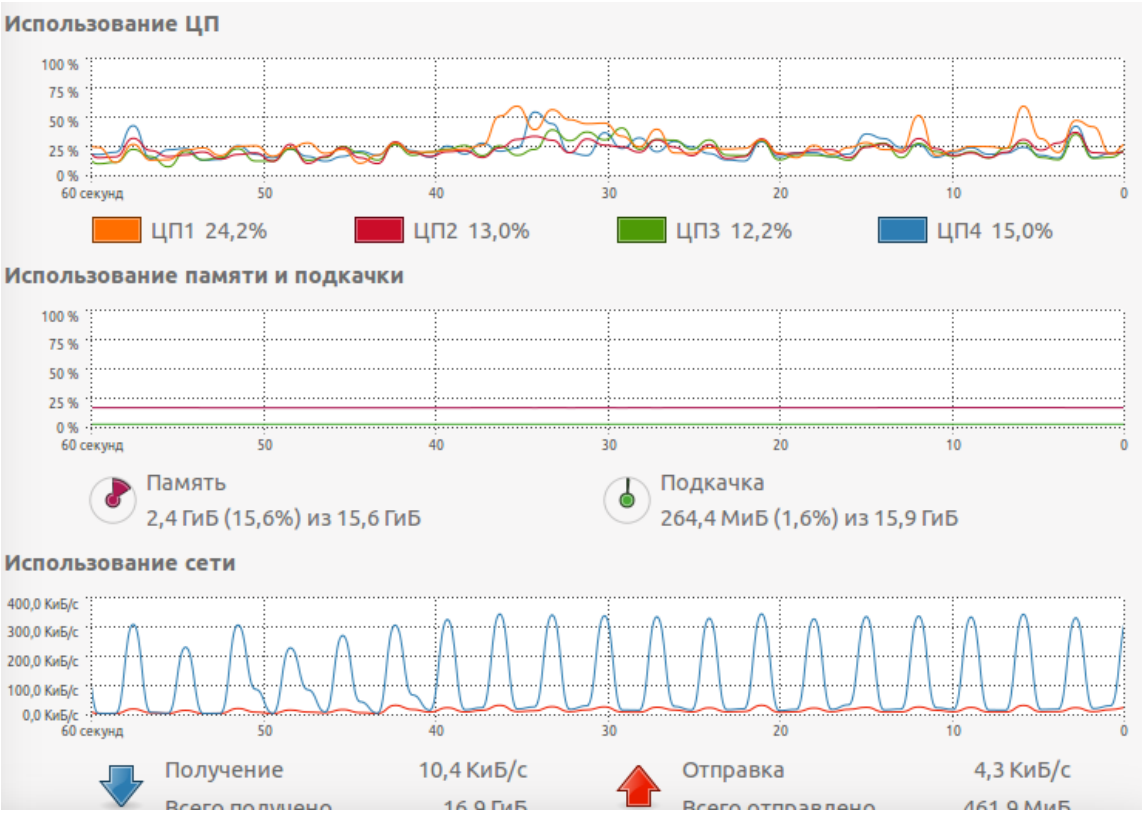


Рис. 2. Использование ресурсов процессора и оперативной памяти SDN-контроллера модельной сети в режиме Unit-тестирования при частоте подключения/отключения ВМ 1 секунда

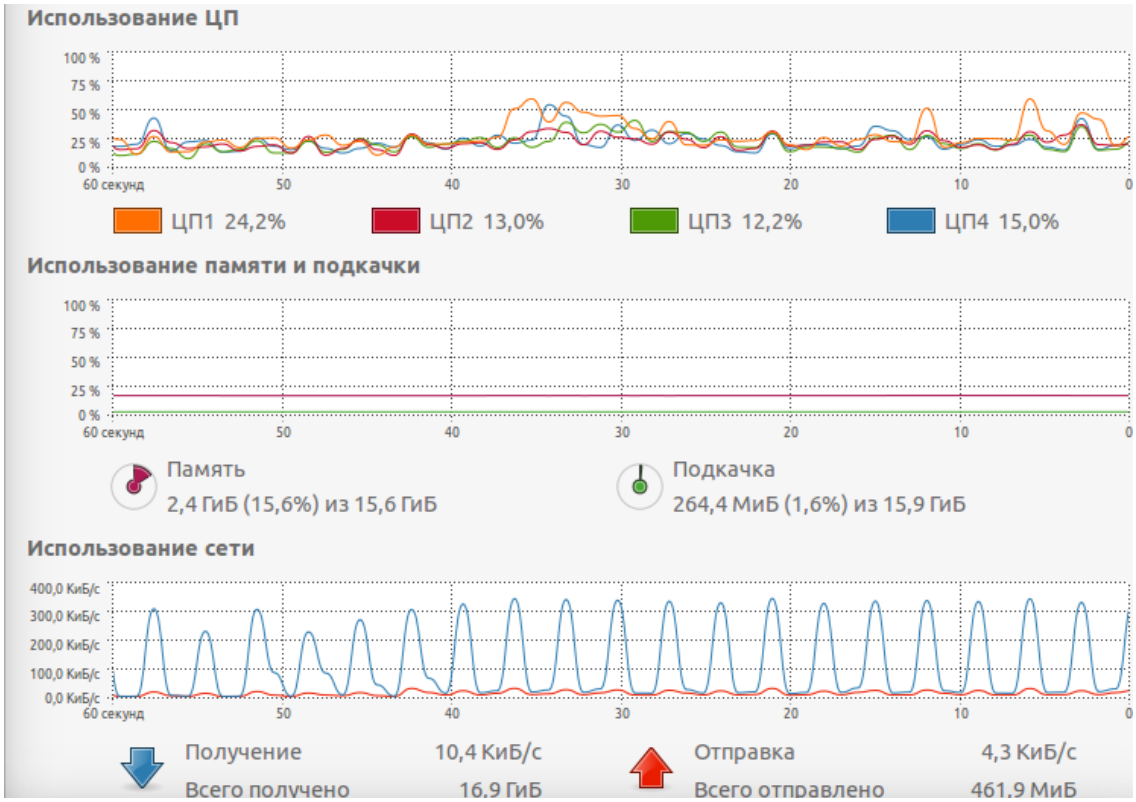


Рис. 3. Использование ресурсов процессора и оперативной памяти SDN-контроллера модельной сети в режиме Unit-тестирования при частоте подключения/отключения ВМ 100 миллисекунд

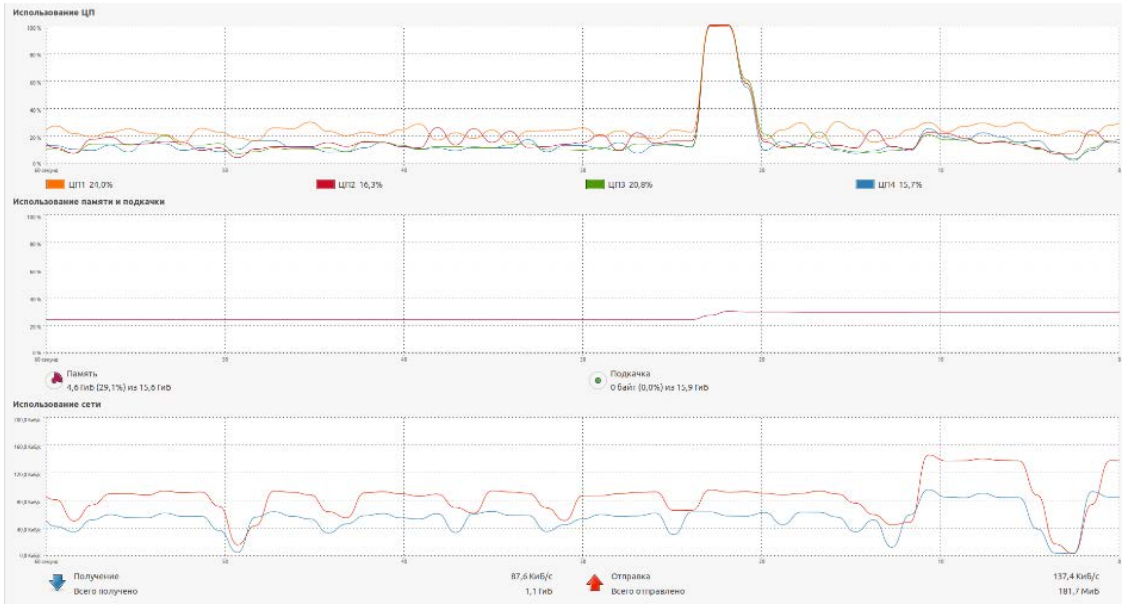


Рис. 4. Использование ресурсов процессора и оперативной памяти SDN-контроллера модельной сети в режиме Unit-тестирования при частоте подключения/отключения ВМ 10 миллисекунд

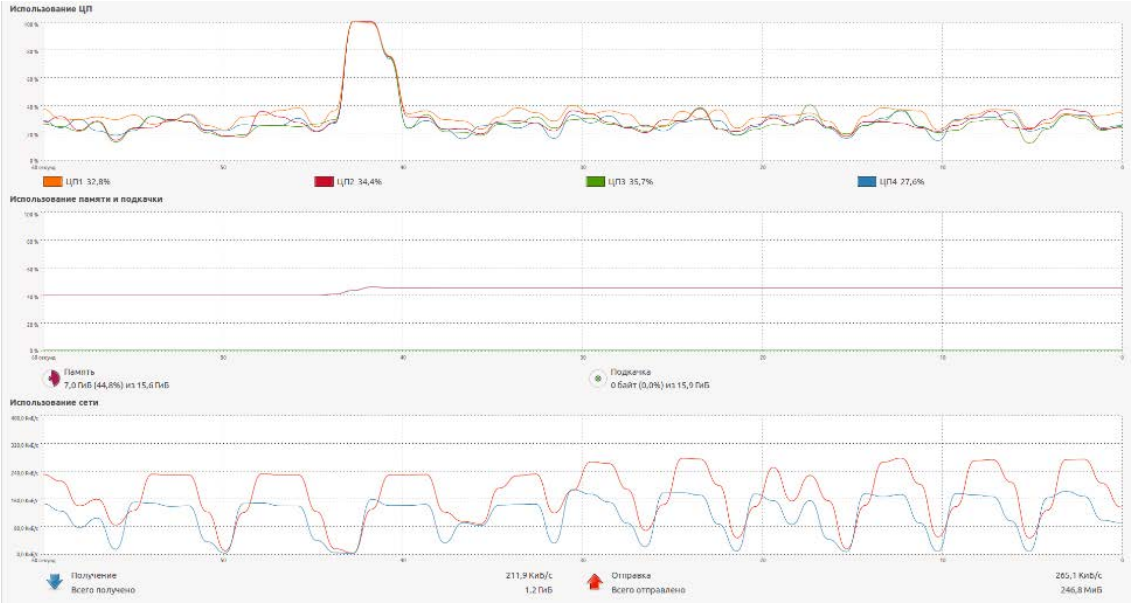


Рис. 5. Использование ресурсов процессора и оперативной памяти SDN-контроллера модельной сети в режиме Unit-тестирования при частоте подключения/отключения ВМ 1 миллисекунда

Список используемых источников

1. Index C. V. N. Global mobile data traffic forecast update, 2016–2021. White paper. 2017.

2. Gupta, A.; Jha, R. K. A survey of 5G network: Architecture and emerging technologies // IEEE Access 2015, 3, 1206–1232.

3. De Brito, M. S.; Hoque, S.; Magedanz, T.; Steinke, R.; Willner, A.; Nehls, D.; Keils, O.; Schreiner, F. A service orchestration architecture for fog-enabled infrastructures // In Proceedings of the Second International Conference on fog and Mobile Edge Computing (FMEC), Valencia, Spain, 8–11 May 2017; pp. 127–132.

УДК 654.739
ГРНТИ 71.01.85

РАЗРАБОТКА МОДЕЛЕЙ АВТОМАТИЗАЦИИ БИЗНЕС-ПРОЦЕССОВ НА БАЗЕ СИСТЕМЫ ЭЛЕКТРОННОГО ДОКУМЕНТАОБОРОТА СПБГУТ

В. О. Долгун, Ю. П. Ревенко

Санкт-Петербургский государственный университет телекоммуникаций им. проф. М. А. Бонч-Бруевича

В данной статье описаны проблемы и особенности автоматизации бизнес-процессов системы 1С:Документооборот на примере СПбГУТ. Автоматизация бизнес-

процессов системы документооборота состоит из определенных этапов: проведение исследования предметной области, подготовка инфраструктуры, настройка СЭД (система электронного документооборота), разработка моделей, проведение приёмо-сдаточных испытаний, обучение сотрудников, проведение опытной эксплуатации. Цель внедрения – повышение эффективности деятельности за счет совершенствования делопроизводства.

1С:Документооборот, автоматизация, 1С, СЭД.

В настоящее время, эффективная и успешная работа любой организации во многом зависит от скорости обработки документов, оперативного распределения информации между подразделениями организации, а также от надежности и целостности информационной составляющей. В связи с этим, все чаще встает вопрос об усовершенствовании и автоматизации документооборота. Автоматизированный документооборот сложно назвать новшеством, так как все большее число организаций активно внедряют и используют системы электронного документооборота (СЭД).

На сегодняшний день ни одно учреждение не обходится без контроля и системной обработки документов. Устные процедуры взаимодействия могут обеспечить эффективное управление только в небольших компаниях с простой организационной структурой и низкой ротацией кадров. Объем созданных и поступивших в организацию документов за определенный промежуток времени является основным критерием выбора формы делопроизводства, при переходе на системы электронного документооборота компаний со сложной и разветвленной системой департаментов.

Правильно организованная система документооборота компании позволяет структурировать весь объем документов и предполагает регламентацию порядка их движения, а также применение единых правил оформления. Автоматизации деятельности компании заключается в оптимизации документооборота, сокращении времени поиска необходимых документов, а также повышении контроля принимаемых управленческих решений.

Электронный документооборот представляет собой единый механизм движения и обработки документов, созданных с использованием компьютерных средств, подписанных электронной цифровой подписью [1].

Основными задачами и целями внедрения СЭД являются: экономия рабочего времени сотрудников, снижение влияния человеческого фактора, организация коллективной и групповой работы, информационная безопасность организации, укрепление исполнительной дисциплины, повышение качества управляемости организации и системная интеграция с другими информационными системами (ИС) организации.

В системе электронного документооборота существует классификация, компонентами которой являются: договора и их производные, служебные записки, организационно-распорядительные документы, организационно-справочные документы, учебные договора.

В процессе исследования предметной области был выполнен комплексный анализ делопроизводства университета, который выявил ряд проблем, возникающих при работе с документами:

1. Трудности поиска необходимых документов.

2. Избыток времени, затрачиваемого на согласование, подписание, возврат документов и их доработку.

3. Отсутствие оперативной доставки документов.

4. избыточные затраты времени работников на мониторинг исполнения документов.

5. Формирование отчетов по контролю исполнения документов, на основе предоставленных данных без предоставления подтверждающих документов.

6. Передача поступающих документов в структурные подразделения без гарантии сохранности оригинала документа.

7. Отсутствие в некоторых подразделениях университета возможности сканирования документов.

8. Требуется длительное время на согласование документов в связи с использованием исключительно последовательных маршрутов движения проектов документов.

Один из основных вопросов построения эффективной системы управления любой компании в настоящее время — это реализация прозрачной «вертикали» функций управления [2].

В результате проведенного исследования была разработана схема движения обращения сотрудника в техническую поддержку, разработан вид документа – нормативно-справочной информации, разграничение доступа по видам подразделений, определен перечень документов, которые подлежат к контролю системы 1С, утверждён шаблон документов, определена зона ответственности за контроль и жизненный цикл документа, определены ответственные лица от подразделений, определен перечень документов для автоматизации и хранения в электронном виде.

Число документов, заведенных в СЭД составляет не одну тысячу и поэтому в системе необходимо было разработать обращение пользователя в техподдержку, т. к. в процессе согласования возникает ситуация, когда необходимо перенаправить бизнес-процесс на другого пользователя или изменить тип документа. На данный момент обращение в техническую поддержку производится таким образом, что исполнение обращений сотрудников происходит несвоевременно или вовсе не исполняется.

В процессе работы, была разработана модель бизнес-процесса, которая позволяет «не потерять» заявку. Рассмотрим комплексный процесс «Обращение в техническую поддержку» (рис. 1, см. ниже). Данный алгоритм позволяет настроить произвольный маршрут обработки обращения, который может изменяться в зависимости от исходных данных.

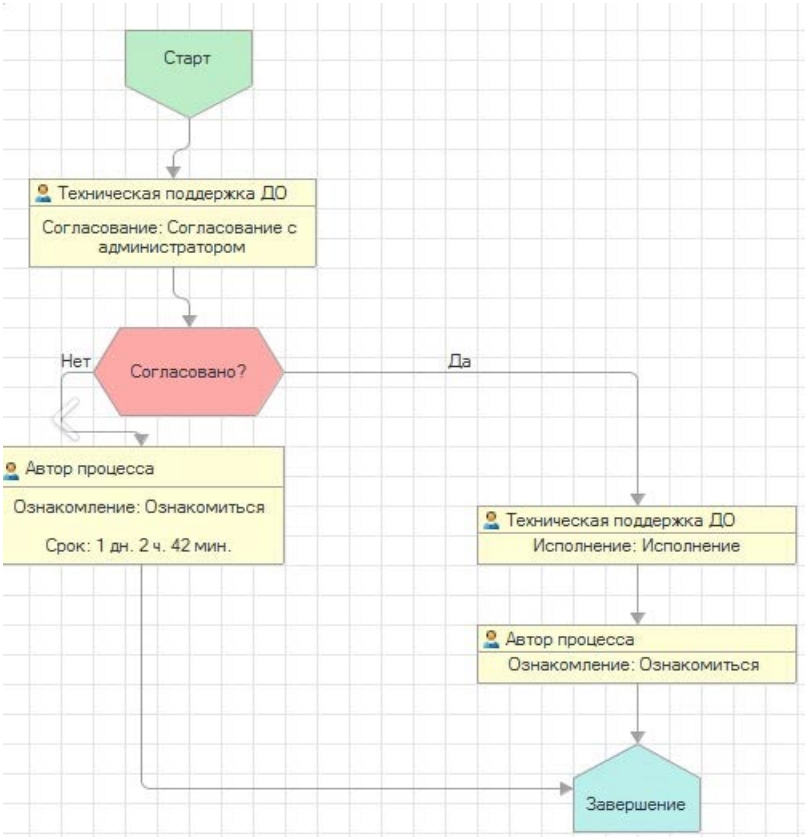


Рис. 1. Комплексный процесс «Обращение в техническую поддержку»

Рассматривая каждый этап обработки обращения, можно увидеть, что позволяет сделать каждое действие начиная с этапа «Согласование с администратором» (рис. 2). Данное действие позволяет прописать и предусмотреть условия дальнейшей обработки.

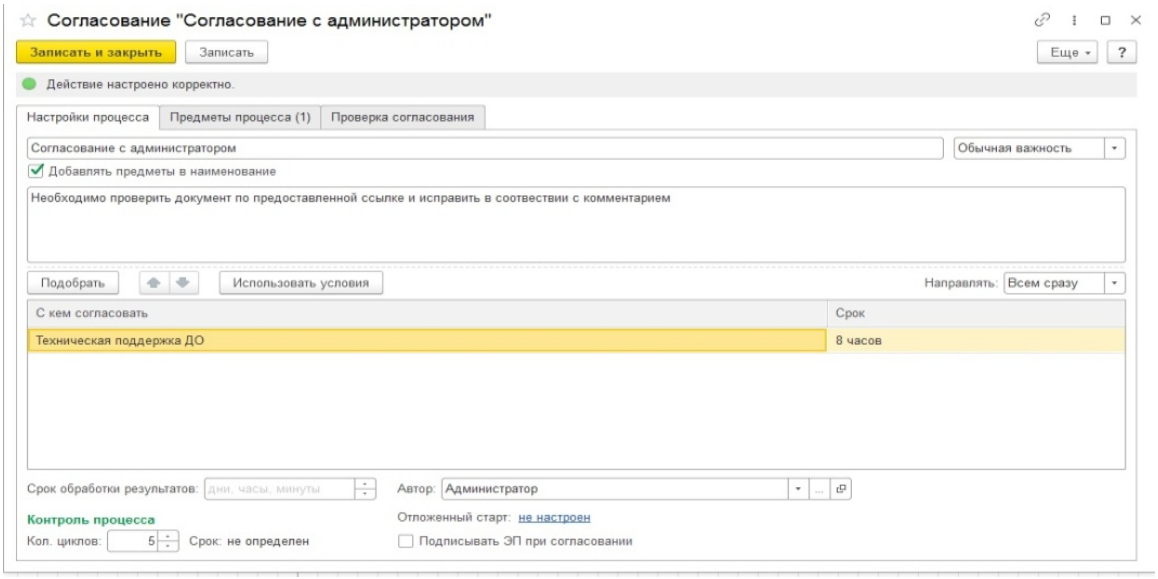


Рис. 2. Этап «Согласование с администратором»

Далее пользователь получает уведомление о том, что его заявка рассмотрена и выполнена на этапе «Ознакомление» (рис. 3). Система ДО позволяет отправлять оповещения, как на электронную почту, так и в самой программе, имеется мобильная версия программы и оповещения через СМС.

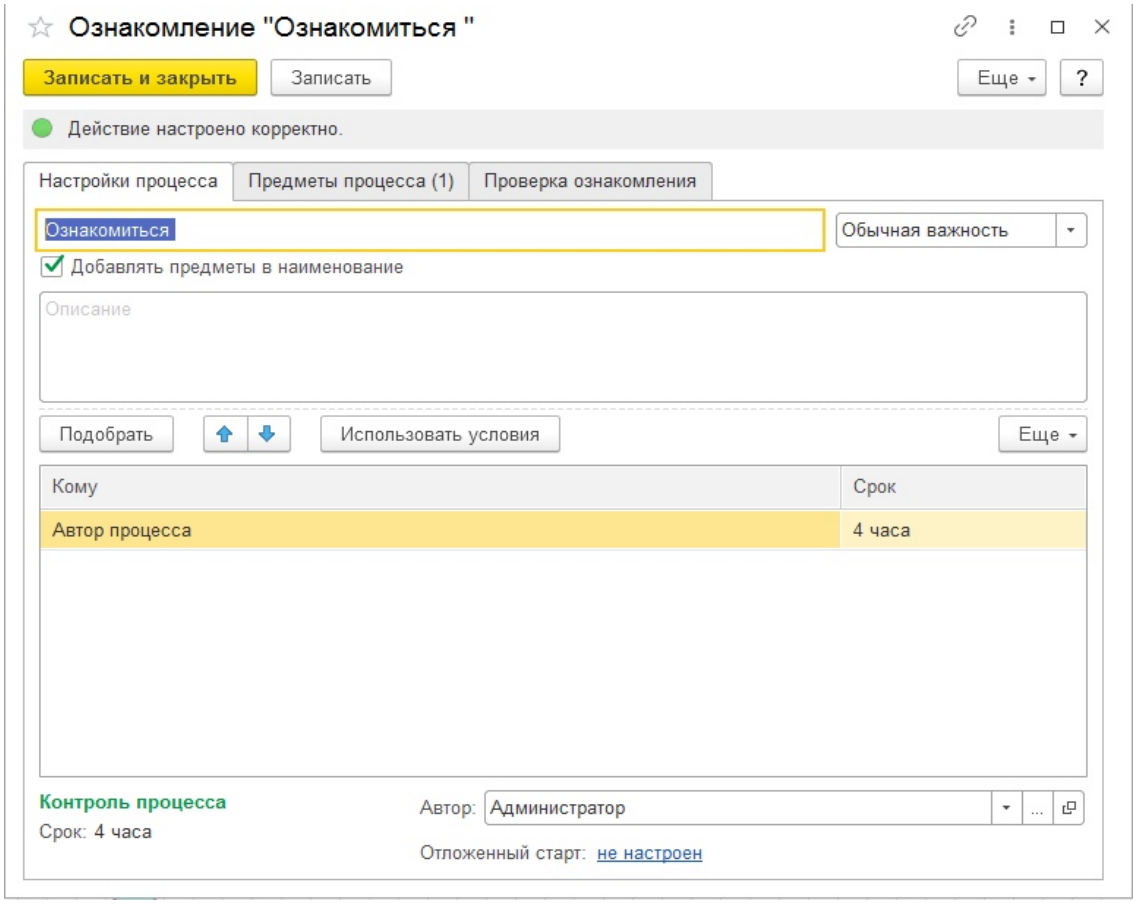


Рис. 3. Этап «Ознакомление»

Для того, чтобы реализовать «Обращение в техническую поддержку ДО», необходимо разработать нормативно-справочную информацию (рис. 4), которая содержит в себе:

1) разработанную схему движения документа с участниками процесса и условиями;

2) созданный вид документа в нормативно-справочной информации с указанием:

– названия документа и количества полей;
– автозаполняемого шаблона файла;
– названия документа и комментарий;
– нормативного срока исполнения заявки;
– ответственного лица и подразделения;
– регистрационного номера документа и многого другого.

3) назначенную роль и группу пользователей.

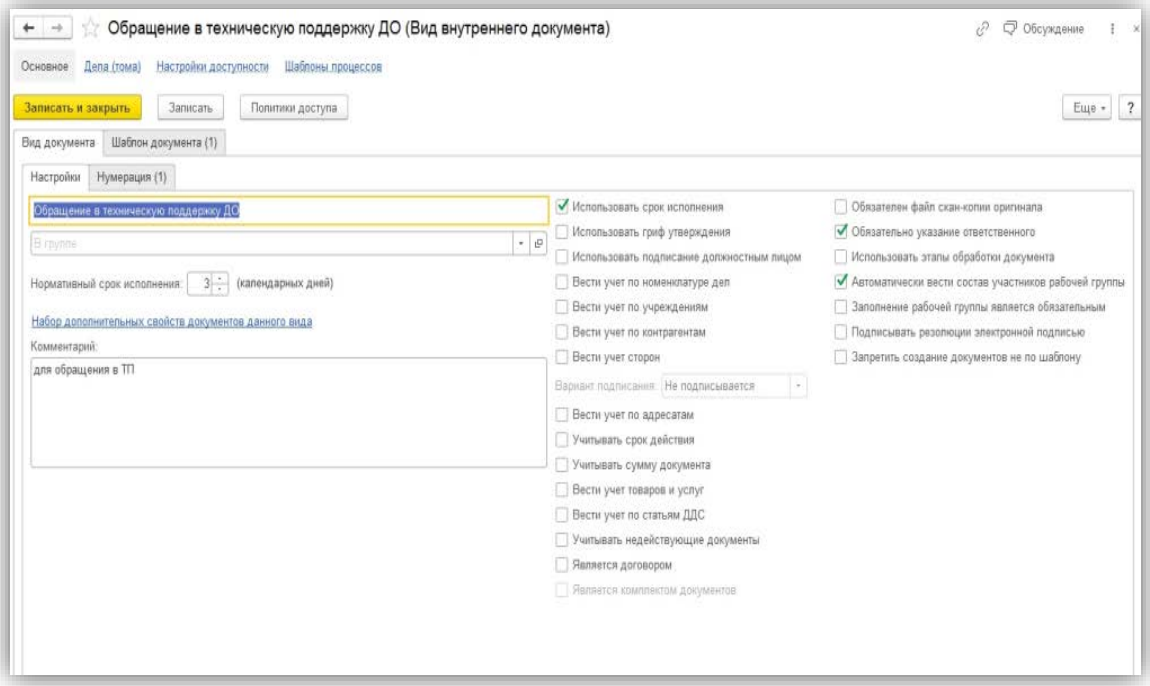


Рис. 4. «Нормативно-справочная информация»

Итогами разработки модели автоматизации электронного документооборота в университете стали:

1. автоматизация процесса обращения сотрудника в техническую поддержку;
2. обеспечение экономии рабочего времени сотрудников;
3. внедрение прозрачной процедуры согласования;
4. снижение влияния человеческого фактора на исполнительность;
5. увеличение скорости обработки информации;
6. укрепление исполнительской дисциплины.

Разработка модели автоматизации бизнес-процессов на базе СЭД привело к повышению качества управленческих решений.

Список используемых источников

1. Ульянцева С. Э. Управление документами: быстро, эффективно, своими силами. М. : 1С-Паблишинг, 2015. 148 с.ISBN 978-5-9677-2360-5.
2. Лушников В. В., Бондарев А. В. 1С:Документооборот. 200 вопросов и ответов. М. : 1С-Паблишинг, 2014. 293 с. ISBN 978-5-9677-2046-

Статья представлена заведующим кафедрой ИКС СПбГУТ, кандидатом технических наук, доцентом А. А. Зарубиным.

УДК 621.391.63
ГРНТИ 49.44.31

ИССЛЕДОВАНИЕ ПРОЦЕССОВ РАСПРОСТРАНЕНИЯ ИМПУЛЬСОВ ГАУССОВСКОЙ И ПРЯМОУГОЛЬНОЙ ФОРМЫ ПО ОДНОМОДОВОМУ ОПТИЧЕСКОМУ ВОЛОКНУ БЕЗ ПОТЕРЬ С УЧЕТОМ ЛИНЕЙНЫХ И НЕЛИНЕЙНЫХ ЭФФЕКТОВ

С. Э. Доценко

Санкт-Петербургский государственный университет телекоммуникаций им. проф. М. А. Бонч-Бруевича

В одномодовых оптических волокнах на процессы распространения влияют линейная хроматическая дисперсия и затухание, а также нелинейная фазовая самомодуляция. Известно, что в ОМ ОВ без потерь с аномальной ХД могут распространяться без искажений на бесконечно большие расстояния оптические импульсы, имеющие форму гиперболического секанса (фундаментальные солитоны) с определенным соотношением длительности и пиковой мощности. Свойства солитонов объясняются полной компенсацией ХД за счет ФСМ. В данной работе рассмотрены возможности компенсации ХД за счет ФСМ для импульсов гауссовской и прямоугольной формы. Теоретические расчеты сопоставлялись с результатами имитационного моделирования процессов распространения импульсов по ОМ ОВ.

волоконно-оптические системы связи, одномодовое оптическое волокно, хроматическая дисперсия, фазовая самомодуляция, импульсы гауссовской и прямоугольной формы.

В первой части работы рассмотрены процессы распространения гауссовских и прямоугольных импульсов по одномодовым оптическим волокнам (ОМ ОВ) без потерь и без учета нелинейных явлений. Для исследования процессов распространения, спектрально ограниченных гауссовских импульсов, использовались аналитические выражения [1] и имитационное моделирование на основе уравнений Шредингера [2, 3]. Для исследования процессов распространения прямоугольных импульсов использовалось только моделирование. Во второй части работы те же процессы рассматривались с учетом нелинейной фазовой самомодуляции (ФСМ). При исследованиях в программе OptiSystem [3] моделировалась схема волоконно-оптической системы связи (ВОСС) со скоростью B = 10 Гбит/с с амплитудной модуляцией (АМ) и кодированием без возврата к нулю (NRZ), состоящая из передатчика, исследуемого ОМ ОВ и фотоприемного устройства (ФПУ). Контролировались сигналы на входе и выходе ОМ ОВ (пиковая мощность

и длительность импульсов на уровне половины амплитуды). Качество связи при моделировании оценивалось максимальным значением *Q*-фактора.

1. Процессы распространения оптических импульсов без учета потерь и нелинейных явлений

В исследованиях использовалось ОМ ОВ со смещенной дисперсией типа DSF со следующими параметрами на длине волны λ_0 = 1550 нм: площадь основной моды A_{nm} = 41 мкм^2, коэффициент нелинейности γ = 2,5 1/(Вт км), параметр хроматической дисперсии (ХД) D_x = 2,7 пс/(нм км), наклон дисперсионной характеристики S_x = 0,085 пс/(нм^2 км), дисперсия групповых скоростей (ДГС) β_2 = – 3,5 пс^2/км [1]. Это же волокно будет иметь D_x = –2,7 пс/(нм км) и β_2 = 3,5 пс^2/км на длине волны λ = 1490 нм в соответствии с выражениями для $D_x(\lambda)$ и $\beta_2(\lambda)$ [2]:

$$D_x(\lambda) = D_x(\lambda_0) + S_x \cdot (\lambda - \lambda_0) \qquad \beta_2(\lambda) = -D_x(\lambda) \cdot \lambda_0^2 / (2\pi \cdot c) \ ,$$

где c – скорость света в вакууме.

Исследование проводилось для гауссовского и прямоугольного импульсов со скважностью $q = 5$ на уровне половины амплитуды $t_u = 1/(B \cdot q) = 20$ пс (0,2 бита).

Запишем выражение для зависимости амплитуды напряженности электрического поля от времени в спектрально ограниченном (без чирпинга) оптическом гауссовском импульсе на входе ОМ ОВ [1, 2]:

$$U_m(t) = U_{m0} \cdot \exp\left(-t^2 / \left(2T_0^2\right)\right) \ ,$$

где U_{m0} – пиковая амплитуда в середине гауссовского импульса и его полуширина T_0, которая связана с шириной импульса t_u на уровне половины амплитуды выражением $T_0 = t_u / 1{,}665$ = 12 пс.

Рассчитанное значение дисперсионной длины для этого импульса $L_D = T_0^2 / |\beta_2| = 41{,}1$ км, будет одинаковым для двух выбранных волн (λ = 1550 и 1490 нм).

Рассмотрим процесс распространения гауссовского импульса без начального чирпинга по ОМ ОВ без потерь и без учета нелинейных явлений (ФСМ). Для модулей комплексных амплитуд и фаз напряженности электрического поля на расстоянии z можно записать [1, 2]:

$$U(z,T) = \frac{U_m}{\sqrt[4]{1+z^2/L_D^2}} \cdot \exp\left(-\frac{T^2}{2T_0^2 \cdot (1+z^2/L_D^2)}\right), \qquad (1)$$

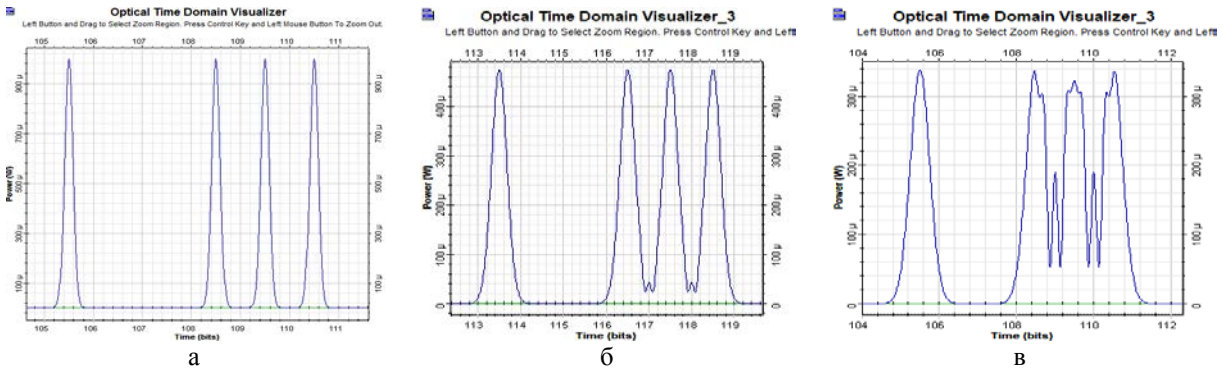
$$\varphi(z,T) = \frac{T^2 \cdot \mathrm{sign}(\beta_2)}{2T_0^2 \cdot (1+z^2/L_D^2)} + \mathrm{arctg}(\mathrm{sign}(\beta_2) \cdot z/L_D), \qquad (2)$$

где $T = t - z/V_g$ – внутриимпульсное время, отсчитываемое от вершины гауссовского импульса, sign(β_2) – функция знака, которая равняется 1 при $\beta_2 > 0$, или –1 при $\beta_2 < 0$, $V_g = c / n_g$ – групповая скорость распространения гауссовского импульса.

Из выражения (1) видно, что импульс на расстоянии z сохраняет гауссовскую форму, его амплитуда уменьшается, а длительность возрастает в $\sqrt{1+(z/L_D)^2}$ раз. Анализируя выражение (2) следует, что гауссовский импульс на расстоянии z приобретает чирпинг [1, 2].

Для повышения информативности результатов моделирования на вход в ОМ ОВ подавалась битовая периодическая последовательность гауссовских импульсов 00100111, которая позволяла измерять расширение одиночного импульса 00100 и наблюдать интерференцию трех рядом расположенных импульсов 01110.

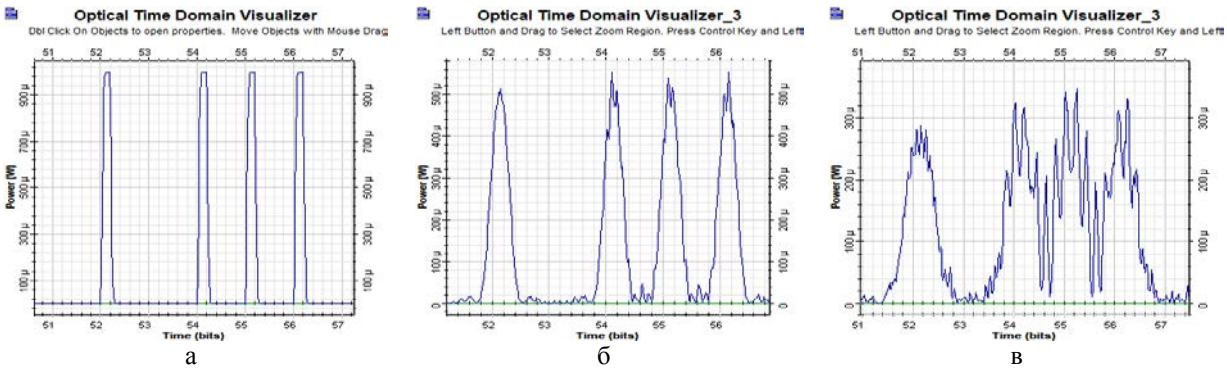
На рис. 1 показаны осциллограммы мощности гауссовских оптических импульсов на входе в ОМ ОВ (рис. 1а) и на расстояниях L равных $2L_D$ (рис. 1б) и 3 L_D (рис. 1в). При небольшой пиковой мощности P_{0m} = 1 мВт можно пренебречь ФСМ. Приведенные результаты моделирования в первом приближении справедливы для излучения с длинами волн $\lambda = 1550$ и 1490 нм, т. к. на этих длинах волн модули параметров ХД одинаковы.



а б в

Рис. 1. Осциллограммы оптической мощности гауссовских импульсов на выходе из ОМ ОВ DSF без потерь при учете ХД длиной 0 км (а), $2L_D$ = 82,2 км (б) и $3L_D$ = 123,3 км (в)

На рис. 2 показаны осциллограммы мощности прямоугольных испульсов на входе в ОМ ОВ (рис. 2а) и на расстояниях L равных L_D (рис. 2б) и $2L_D$ (рис. 2в) на длине волны 1550 нм (рис. 2в) при P_{0m} = 1 мВт. Результаты моделирования и расчетов для гауссовских импульсов приведены в таблице 1. Видно, что прямоугольные импульсы значительно сильнее искажаются, и обеспечивают значительное ухудшение качества связи, по сравнению с гауссовскими импульсами той же длительности. Результаты аналитических расчетов параметров гауссовских импульсов на выходе ОМ ОВ удовлетворительно согласуются с результатами моделирования (табл. 1 и рис. 1).



а б в

Рис. 2. Осциллограммы оптической мощности прямоугольных импульсов на выходе из ОМ ОВ DSF без потерь при учете ХД длиной 0 км (а), L_D = 41,1 км (б) и $2L_D$ = 82,2 км (в)

ТАБЛИЦА 1. Результаты исследований ВОСС на длине волны 1550 нм без учета ФСМ

	Прямоугольный импульс			Гауссовский импульс				
	Моделирование			Моделирование			Расчет	
L/L_D	P_{lm}, мВт	t_{ul}, бит	Q_{max}	P_{lm}, мВт	t_{ul}, бит	Q_{max}	P_{lm}, мВт	t_{ul}, бит
0	1	0,2	3614	1	0,2	3321	1	0,2
1	0,51	0,36	269	0,73	0,28	2864	0,707	0,28
2	0,28	0,68	73	0,48	0,40	2014	0,45	0,44
3	0,24	0,82	15	0,34	0,58	233	0,316	0,63

2. Процессы распространения оптических импульсов без учета потерь, но с учетом нелинейных явлений

Нелинейная длина ОМ ОВ определяется пиковой мощностью P_{m0} импульса и коэффициентом нелинейности γ:

$$L_{NL} = 1/\left(\gamma \cdot P_{0m}\right).$$

Полагая, что для компенсации ХД в ОМ ОВ с аномальной дисперсией с помощью ФСМ в волокнах с аномальной дисперсией ($\beta_2 < 0$) необходимо выполнение условия равенства дисперсионной и нелинейной длин ОМ ОВ, определим требуемую для этого пиковую мощность:

$$P_{0mtr} = -\beta_2 / \left(\gamma \cdot T_0^2\right) = 10 \text{ мВт}.$$

На рис. 3 показаны осциллограммы мощности оптических сигналов на выходе ОМ ОВ DSF длиной 82,2 км для входной пиковой мощности 10 мВт для гауссовского (рис. 3а) и прямоугольного (рис. 3б) импульсов. Видно, что пиковой мощности 10 мВт для сохранения начальной длительности (0,2 бит) и амплитуды импульсов (10 мВт) на выходе ОМ ОВ недостаточно. Наилучшие результаты получены для мощности

14 мВт (рис. 3в) и 20 мВт (рис. 3г) для гауссовского и прямоугольного импульсов, соответственно. Результаты моделирования, приведенные в таблице 2 и на рис. 3, показывают, что выбор оптимальной входной мощности позволяет сохранить амплитуду и длительность гауссовского импульса на больших расстояниях. Для прямоугольных импульсов при оптимизации входной мощности, в принципе, можно обеспечить сохранение длительности выходного импульса, но ценой его искажений и ухудшения качества связи.

Предполагается продолжить эти исследования, учесть реальные потери в ОМ ОВ и использовать оптические усилители.

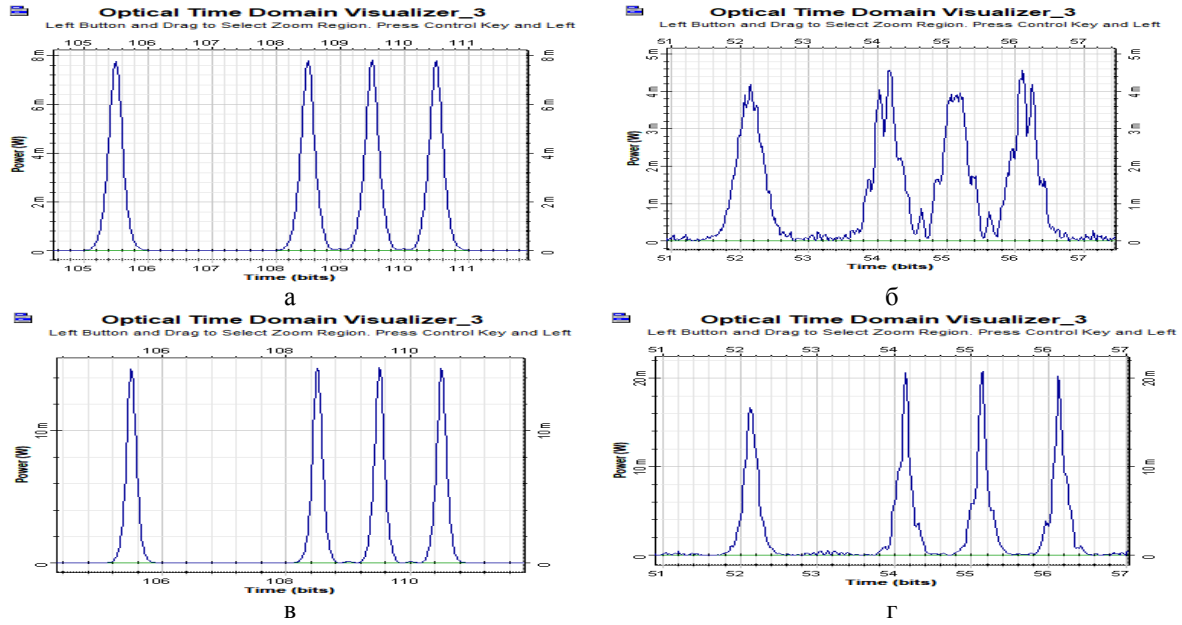


Рис. 3. Осциллограммы оптической мощности на выходе из ОМ ОВ DSF длиной 82,2 км без потерь для гауссовского (а и в) и прямоугольного (б и г) импульсов при входной пиковой мощности 10 мВт (а и б), 15 мВт (в) и 20 мВт (г)

ТАБЛИЦА 2. Результаты исследований ОМ ОВ длиной 82 км с учетом ХД и ФСМ

	Прямоугольный импульс			Гауссовский импульс					
λ, нм	1550			1550			1490		
P_{0m}, мВт	P_{lm}, мВт	t_{ul}, бит	Q_{max}	P_{lm}, мВт	t_{ul}, бит	Q_{max}	P_{lm}, мВт	t_{ul}, бит	Q_{max}
1	0,28	0,68	73	0,48	0,4	2014	0,42	0,48	1852
10	4,2	0,4	53	7,7	0,24	6823	3,2	0,64	4065
14	7,2	0,3	46	15	0,17	13255	4,1	0,72	1548
20	17	0,2	48	32	0,12	7133	5,2	0,8	512

Список используемых источников

1. Былина М. С., Глаголев С. Ф. Распространение гауссовских импульсов по ОМ ОВ в линейном приближении // Фотон-экспресс-наука 2019. 2019. № 6. С. 176–177.
2. Govind P. Agrawal. Nonlinear Fiber Optics Fifth Edition. M.: Academic Press is an imprint of Elsevier, 2013. 629 c.
3. Андреева Е. И., Былина М. С., Глаголев С. Ф., Доценко С. Э., Чаймарданов П. А. Свойства временных оптических солитонов в оптических волокнах и возможность их использования в телекоммуникациях. Часть 4 // Труды учебных заведений связи. 2019. Т. 5. № 1. С. 15–24.

Статья представлена заведующим кафедрой ФиЛС СПбГУТ, кандидатом технических наук, доцентом М. С. Былиной.

УДК 004.77
ГРНТИ 49.33.29

АНАЛИЗ ПРИМЕНЕНИЯ ТЕХНОЛОГИЙ LBS В МОБИЛЬНЫХ ПРИЛОЖЕНИЯХ

В. С. Елагин, Д. А. Истомин

Санкт-Петербургский государственный университет телекоммуникаций им. проф. М. А. Бонч-Бруевича

В современном мире трудно переоценить значение определения местоположения пользователя. Благодаря стремительному развитию LBS у людей открываются новые возможности. Ситуации, когда нужно быстро и точно определить местонахождение человека, встречаются постоянно. Современные люди не могут представить свою жизнь без использования навигатора, цифровых карт с информацией о зданиях и компаниях, расположенных в них, и многих других мобильных программ, которым требуется функция определения местоположения. Но у приложений разные требования к сервисам распознавания геолокации. Некоторым программам требуется более точное определение местоположения пользователя, другие могут пожертвовать точностью ради скорости и экономии производительности. В этой статье проводится анализ технологий LBS, их сравнение и применение в мобильных приложениях.

LBS (Location Based Servise), позиционирование, indoor-навигация.

Введение

Мобильные телефоны и Интернет произвели революцию в общении, а вместе с ним, и в образе жизни людей. Растущее число мобильных телефонов и персональных цифровых помощников позволяет людям получать доступ к Интернету, где бы они ни находились и когда бы они ни пожелали.

Из интернета можно получать как информацию о событиях (кино, концерты, вечеринки), так и информацию о местах (городские карты, рестораны, музеи, больницы). Такие виды поиска относительно местоположения абонента могут быть выполнены с использованием Location Based Service (LBS). Таким образом, можно определить, что LBS – это программный сервис, использующий данные о локации для управления какими-либо функциями.

Методы позиционирования можно разделить на три группы:

1. Сетевое позиционирование.
2. Терминальное позиционирование.
3. Комбинации сетевых и терминальных методов позиционирования.

Обзор технологий определения местоположения

В настоящее время существует несколько сотовых технологий определения местоположения, которые были изобретены и реализованы последовательно, повышая точность определения геопозиции. Эти технологии разрабатываются и используются параллельно, в зависимости от требований точности, которые предъявляет услуга, реализованная на основе технологии.

Методы, основанные на СОО

Cell ID исторически было первым и самым неточным способом определения местоположения абонента. Зная идентификатор соты (Cell ID), полученный от абонентского терминала или из сети, можно определить «точку» местоположения абонента в виде определенной геометрической фигуры с известным положением на карте. В Cell ID+ используется не только идентификатор ячейки (Cell ID), но и параметр TA (*Time Advance*). TA – значение, соответствующее времени, которое требуется, чтобы добраться до абонентской станции с мобильного телефона. Этот параметр позволяет выбрать область абонента в уже ранее определенной ячейке, тем самым увеличивая точность определения местоположения абонента. Enhanced Cell ID (E-CID) – метод, основанный на Cell of Origin, для оценки положения в сетях LTE. С помощью СОО положение устройства оценивается с использованием знания географических координат его обслуживающей базовой станции, в терминах LTE eNB.

Методы триангуляции

Определение местоположения с помощью метода UL-TOA (*UpLink Time Of Arrival*) основано на измерении времени прихода сигнала от мобильной станции до нескольких БС и вычислении местоположения абонента на основе этих данных. Для этого каждая БС должна быть оснащена

LMU (*Location Measurement Unit*), который записывает информацию о расстоянии от БС и передает ее в измерительный центр. Позиционирование E-OTD (*Enhanced Observed Time Difference*) аналогично UL-TOA, но абонентский терминал участвует в процессе позиционирования. OTDOA – UE-ассистированный метод, основанный на измерениях разности времени опорного сигнала (RSTD), проводимых на нисходящих опорных сигналах позиционирования, полученных из нескольких мест, где местоположение пользователя вычисляется путем мультилатерации.

Global Positioning System

GPS-позиционирование основано на измерении расстояния от спутников до приемника GPS, расположенного на поверхности Земли. Это расстояние до каждого спутника может быть определено приемником GPS. Основная идея – это решение обратной засечки, которое многие геодезисты используют в своей повседневной работе. Если вы знаете расстояние до трех точек относительно вашего собственного положения, вы можете определить координаты точки стояния относительно этих точек.

Совместное использование GPS и методов определения местоположения через мобильные сети

Такие методы, как A-GPS и A-GNSS, используют глобальную систему позиционирования, которая поддерживает сетевую инфраструктуру. Координаты вычисляются следующим образом: сигнал GPS передается на мобильный телефон, затем он передается на БС, которая вычисляет координаты телефона и отправляет их обратно.

Применение технологий LBS в мобильных приложениях

С быстрым развитием технологий мобильного интернета, многие мобильные телефоны уже имеют «доступ» к сети. Разнообразные приложения в мобильном Интернете кардинально меняют жизнь людей в информационную эпоху, а службы на основе местоположения (LBS) и мобильные сетевые прикладные системы «встроены» в повседневную жизнь людей. LBS позволяет маркетологам лучше понять группу клиентов, которые с большей вероятностью отдадут предпочтение их продукции. В настоящее время определение местоположения используется в качестве дополнительной функции практически во всех областях промышленности.

Естественно, что для разных задач определения местоположения требования разные. Некоторым программам требуется более точное определение местоположения пользователя, другие могут пожертвовать точностью ради скорости и экономии производительности.

В таблице представлены основные методы позиционирования, доступные в мобильных сетях. Эти методы имеют различные типичные диапазоны точности, и все они могут быть использованы с гибридной техникой. Каждый метод вычисляет позиции, используя различные измерения и сигналы из различных источников.

ТАБЛИЦА. Основные методы позиционирования

Метод нахождения местоположения	Ограничения окружающей среды	Влияние производительности устройства (Perf)	Влияние производительности системы	Затраченное время (Time)	Точность определения (Loc)
Cell ID	нет	незначительное	минимальное	минимальное	от 150 м до 35 км
Cell ID+	нет	незначительное	незначительное	незначительное	около 550 м
E-CID	нет	незначительное	среднее	незначительное	около 150 м
E-OTD	вне города	среднее	среднее	среднее	от 50 до 125 м
UL-TOA	вне города	незначительное	среднее	среднее	около 100 м
OTDOA	вне города	среднее	среднее	среднее	< 100 м
A-GPS	помещения	незначительное	среднее	среднее/ значительное	около 10–15 м
A-GNSS	помещения	значительное	среднее	среднее/ значительное	< 5 м
GPS	помещения	незначительное	среднее	значительное	около 1–5 м

Для более наглядного примера попробуем проанализировать использование методов определения местоположения в разных программах: приложение для определения прогноза погоды, приложение «Мобильные сотрудники» и приложение «Навигация по Торговому Центру».

Для удобного пользования мобильное приложение по определению прогноза погоды предлагает пользователю автоматически определять его местоположение. Для определения геопозиции в этих приложениях зачастую используются такие методы, как E-CID, CellID и CellID+. Они основаны на Cell of Origin (COO). С помощью COO положение устройства оценивается с использованием знания географических координат его обслуживающей базовой станции.

Для отличной работы мобильному приложению по определению погоды не нужна информация о местоположении пользователя с точностью

до нескольких метров. Ему вполне хватает качества обслуживания, предложенного методами определения местонахождения по индикатору сети (Cell ID). Данные методы затрачивают маленькое время для своей работы и не требуют высокой производительности как базовой станции, так и самого мобильного устройства. Конечно, надо понимать, что если пользователю требуется более точное определение его локации, например, с точностью до дома, то мобильному приложению потребуются другие методы нахождения местоположения. Работу приложения можно описать данными формулами:

$$Serv1 = f(Loc, Perf, Time),$$

где x > 0 y >2,

$$Serv1 = f_{Loc}(1/x^y) \qquad Serv1 = f_{Perf}(1/x) \qquad Serv1 = f_{Time}(1/x^y).$$

Одним из способов контроля и организации деятельности крупных компаний является сервис «Мобильные сотрудники», который позволяет руководителю осуществлять контроль местоположения и перемещения сотрудника в режиме онлайн. Так как работодателю важно получить конкретное местоположение своего сотрудника на карте для соблюдения контроля, мобильное приложение должно использовать точное определение местонахождения. Для данного качества обслуживания подходит либо метод, основанный на определение местоположения по GPS, либо метод триангуляции (E-OTD и OTDOA). Но из-за временного отклика при запуске приложения использовать чистое определение по GPS спутникам не совсем рационально, так что применяются технологии совместного использования GPS и методов определения местоположения через мобильные сети, такие как A-GPS и A-GNSS. Работу приложения можно описать данными формулами:

$$Serv2 = f(Loc, Perf, Time),$$

где z > 0 y > 2,

$$Serv2 = f_{Loc}(z) \qquad Serv2 = f_{Perf}(1/z) \qquad Serv2 = f_{Time}(1/z).$$

Несколько тысяч посетителей приходят в торговый центр каждый день. С помощью приложения «Навигация по Торговому Центру» люди могут перемещаться по обширному зданию по интерактивной карте. Программа предлагает идеальный маршрут до выбранного магазина, а также может принимать во внимание его доступность.

Навигация в закрытом помещении – это сложная задача из-за отсутствия прямой видимости, ослабления и рассеяния сигнала, из-за препятствий и многолучевого распространения при отражениях сигнала от стен и других препятствий. Поэтому навигация по спутникам GPS в большинстве случаев невозможна. А позиционирование по сотовым сетям попросту

не соответствует требуемой точности определения местоположения пользователя (5–10 метров).

В indoor-навигации есть несколько решений для определения местоположения пользователя. Мы остановимся на навигации по Wi-Fi из-за возможности использования на уже существующей сетевой инфраструктуре и простоты определения координат. Методика определение координат следующая – устройство пользователя сканирует доступные Wi-Fi-точки доступа, затем информацию о них отправляет на сервер, где эти данные по базе данных сопоставляются с координатами этих точек доступа, по которым и вычисляются координаты пользователя. Большим преимуществом является то, что позиционирование Wi-Fi позволяет определять этаж помещения, на котором находится покупатель. Благодаря использованию данного метода определение абонента происходит с точностью до 5 метров, что является приемлемым для работоспособности приложения «Навигация по Торговому Центру». Работу приложения можно описать данными формулами:

$$Serv3 = f(Loc, Perf, Time),$$

где m > 0 y > 2,

$$Serv3 = f_{Loc}(m^y) \qquad Serv3 = f_{perf}(m) \qquad Serv3 = f_{Time}(1/m).$$

Вывод

Таким образом, становится понятно, что для наиболее рационального использования ресурсов устройства и сети необходимо знать требуемые цели и условия работы мобильного приложения. У программ разные требования к сервисам позиционирования, поэтому для некоторых приложений требуется более точное определение местоположения пользователя, другие могут пожертвовать точностью ради скорости и экономии производительности мобильного устройства. Также важно понимать влияние окружающей среды на методы определения местоположения.

Например, спутниковые измерения обеспечивают наилучшую производительность для терминалов с приемниками, поддерживающими GNSS, в пригородных и сельских районах. Методы, основанные на разнице во времени прибытия (TDOA), такие как E-OTD, UL-TOA и OTDOA, могут быть лучшим выбором для внутренних помещений и городских каньонов, в то время как методы, основанные на идентификации ячейки (Cell ID, Cell ID+, ECID) хорошо подходят для всех сред и особенно удобны для терминалов, которые не оснащены приемниками GNSS.

Список используемых источников

1. Киреев А. В., Фокин Г. А. Оценка точности локального позиционирования мобильных устройств с помощью радиокарт и инерциальной навигационной системы // Труды учебных заведений связи. 2017. Т. 3. № 4. С. 54–62.

2. Ивакин Я. А., Подкользин А. Я. Реализация информационной технологии геохронологического трекинга на базе объектно-ориентированной ГИС // Информационные технологии и телекоммуникации. 2017. Т. 5. № 2. С. 45–55.

3. Киреев А. В., Фокин Г. А. Измерение времени прихода сигнала в задачах позиционирования в мобильных сетях при отсутствии прямой видимости // Информационные технологии и телекоммуникации. 2017. Т. 5. № 4. С. 36–41.

4. Лебедева Н. А., Олейникова О. В., Дунайцев Р. А. Исследование особенностей работы Wi-Fi на улице и внутри помещений // Информационные технологии и телекоммуникации. 2019. Т. 7. № 2. С. 34–45.

УДК 004.414
ГРНТИ 49.33.35

АНАЛИЗ ОБНОВЛЕННЫХ ТРЕБОВАНИЙ НПА И ИХ РЕАЛИЗАЦИЯ В СИСТЕМАХ ЗАКОННОГО ПЕРЕХВАТА

В. С. Елагин, Л. М. Лобанова

Санкт-Петербургский государственный университет телекоммуникаций им. проф. М. А. Бонч-Бруевича

В настоящее время в СОРМ существует проблема с реализацией требований в соответствии с внесением правок в федеральный закон №374-ФЗ. В данной статье рассматриваются новые требования для разработки программного обеспечения СОРМ. А также рассмотрение архитектуры одного варианта реализации требований и необходимые расчеты для реализации ПО.

СОРМ, Закон Яровой, законный перехват, хранение данных.

В связи с принятием федерального закона №374-ФЗ, собранным депутатом Госдумы Ириной Яровой, так называемый «Пакет Яровой» от 06.07.2016, в соответствии с которым были внесены правки в закон № 126-ФЗ от 07.07.2003, где сказано, что операторы связи обязаны хранить на территории Российской Федерации [1, 2]:

1. информацию о фактах приема, передачи, доставки и (или) обработки голосовой информации, текстовых сообщений, изображений, звуков, видео- или иных сообщений пользователей услугами связи – в течение трех лет с момента окончания осуществления таких действий;

2. текстовые сообщения пользователей услугами связи, голосовую информацию, изображения, звуки, видео-, иные сообщения пользователей услугами связи – до шести месяцев с момента окончания их приема, пере-

дачи, доставки и (или) обработки. Порядок, сроки и объем хранения указанной в настоящем подпункте информации устанавливаются Правительством Российской Федерации.

В настоящее время в целях изготовления и проведения работ по сертификации технических средств накопления информации, входящих в состав оборудования средств связи, включая программное обеспечение, обеспечивающего выполнение установленных действий при проведении оперативно-розыскных мероприятий, издан и зарегистрирован Минюстом России приказ Минкомсвязи России от 26.02.2018 № 86 [3].

Общие требования к Техническим средствам накопления голосовой информации (далее ТС ОРМ) предусматривают необходимость накопления и хранения, в том числе статистической информации, текстовых сообщений, голосовой информации (звуков), видеовызовов. Информационные системы, содержащие базы данных об абонентах оператора связи и оказанных им услугах связи, обеспечивающие выполнение установленных действий при проведении оперативно-розыскных мероприятий (далее ИС БД ОРМ), должны подключаться к ТС ОРМ накопления Голоса как дополнительные ПУ ОРМ. ТС ОРМ должны обеспечивать подключение **до 100 ПУ ОРМ** [3].

ТС ОРМ также должны обеспечивать [3]:

– пассивное подключение к сети связи посредством интерфейсов Ethernet, SDH, PDH;

– возможность определения территории, являющейся зоной ответственности пульта управления (далее ПУ ОРМ), и исключение взаимного влияния ПУ ОРМ между собой при проведении ОРМ;

– возможность **одновременного** приема, обработки и накопления информации одними техническими средствами ОРМ;

– возможность доступа с ПУ ОРМ к информации о соединениях и их содержании не позднее чем через 10 секунд после завершения соединений;

– определение с точностью до секунды и хранение для каждого сохраненного соединения, даты, времени начала и длительности соединения;

– контроль собственного функционирования и передачу на подключенные ПУ ОРМ информации о состоянии ТС ОРМ;

– синхронизацию времени с ПУ ОРМ, при этом коррекция времени может осуществляться только с головного ПУ ОРМ;

– круглосуточный удаленный доступ со стороны ПУ ОРМ и ИС БД ОРМ, взаимодействие с ПУ ОРМ в соответствии с приложением № 3 к Правилам.

Пропускная способность выделенного канала до каждого ПУ ОРМ должна составлять – в соответствии с таблицей.

ТАБЛИЦА. Пропускная способность на сети связи

Емкость абонентской базы до (тыс. абонентов)	10	100	100 и больше
Скорость передачи данных не менее (Мбит/с)	4	10	100

Требования к скорости выборки данных определены в п. 18.4 приказа № 86 (стр. 9) [3].

На рис. представлена архитектура ТС ОРМ одного из вариантов реализации Приказа № 86 со всеми его требованиями. Архитектура состоит из следующих компонентов:

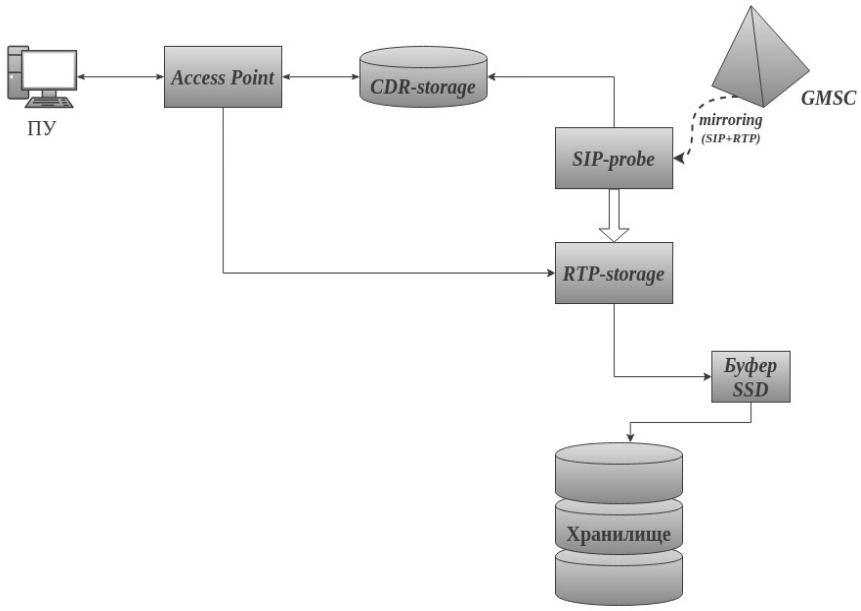


Рис. Архитектура технических средств ОРМ

SIP-probe – съёмник SIP и RTP трафика, а также ряда других протоколов, которые могут потребоваться для реализации требований приказа;

RTP-storage – компонента, обеспечивающего запись голоса (RTP-сессий);

Access point – точка доступа для ПУ – решение, реализующее интерфейс в сторону ПУ (86й приказ) и обеспечивающее выполнение команд обработки данных через формирование SQL-запросов к cdr-storage и запросов контента к rtp-storage;

CDR – storage – БД SQL, обеспечивающая хранение статистической информации о вызовах и возможность выборки вызовов по некоторым фильтрам.

Проходящий трафик через станцию, в данном случае GMSC, зеркалируется на SIP-probe, где информация по вызову: данные абонента А, данные абонента Б, время вызова и другие идентификаторы, перенаправляется в БД

CDR-storage, а RTP-трафик по выделенному каналу перенаправляется в RTP-storage, где, посредством добавления дополнительных заголовков, формируются cdr и отправляются в буфер SSD. Дальше в буфере накапливается объем данных за день, два, неделю и отправляется в хранилище.

Скорость выборки

При выборке **по MSISDN, IMSI или IMEI** требуется соблюдать следующие временные показатели:

на интервале до суток – **не более 3 секунд**;

на интервале до месяца – **не более 5 секунд**;

на интервале до 6 месяцев – **не более 15 секунд**.

При выборке **по номеру базовой** станции на интервале до суток – **не более 7 минут** [1]. При выборке по **иным критериям** время выполнения может быть выше (но не сказано, насколько выше).

Объём хранимой информации (в расчете на 1000 абонентов)

На данный момент, для любых сетей используем следующие статистические показатели:

– средняя продолжительность вызова – 60 секунд;

– каждый абонент разговаривает 18 минут в сутки или совершает 18 вызовов по 1 минуте (средняя продолжительность);

– в час наибольшей нагрузки каждый абонент разговаривает не более 6-ти минут;

– по каждому вызову создаётся 2 SIP плеча или 4 RTP-потока;

– средняя продолжительность вызова = 60 секунд;

– битрейт будет равен 64 Kb/сек. * 2 дорожки * 2 плеча = 256 Kb/сек. = 32 KB/сек.

Считаем, что на каждый вызов требуется генерировать 1 CDR-запись размером в 1 KB. Каждый абонент генерирует в сутки 18 мин * 32 KB/сек. * 60 сек. = 34560 KB = 35 MB. Таким образом, на каждые 1000 абонентов требуется:

– 1000 аб. * 35 MB * 30 сут. * 6 мес. = 6300000 MB = **6,3 TB** контента;

– 1000 аб. * 18 выз. *30 сут. * 6 мес. * 1 KB = 3240000 KB ~ **3,2 GB** CDR или 3,24 млн записей.

Т. е. на сети в 10000 абонентов получаем, что необходимо хранить 62 ТБ контента и 32 ГБ CDR. Судя по объёму CDR-записей, можно рассмотреть вариант размещения БД на SSD + дублирование базы целиком в оперативной памяти.

Из-за большого объёма хранимой информации, для хранения контента будет задействовано несколько десятков или сотен дисков. Хранение можно организовать двумя способами:

1. каждая сессия – это pcap-файл в файловой системе;

2. диск рассматривается как блочное устройство и каждая сессия – это одна или несколько страниц, причём:

– страницы одной сессии могут быть расположены строго последовательно – такой подход возможен, если есть возможность хранить всю сессию в оперативной памяти до её завершения;

– страницы одной сессии могут быть разделены страницами других сессий – такой подход используется, если нет возможности хранить всю сессию в оперативной памяти.

Исходя из предварительных расчётов, приведённых выше, на каждую 1000 абонентов потребуется хранить 6,12 ТБ информации. Соответственно, если речь идёт о десятках тысячах абонентов, то вполне возможно организовать хранилище непосредственно на той же машине, на которой будет запущен съёмник SIP-PROBE. Однако, если говорить о сотнях тысячах абонентов, то потребуется подключить сотни жёстких дисков. Поэтому следует сразу задуматься о возможности установки около съёмника нескольких независимых хранилищ, по которым будет равномерно распределяться поступающий RTP-трафик. Таким образом, возникает необходимость реализовать хранилище как отдельное приложение. Назовём его **RTP-storage**. В его задачи будет входить:

1. распределение RTP по дискам;

2. запись RTP на диски;

3. доступ к контенту с возможностью перекодирования (с использованием MCU);

4. управление контентом (удаление устаревших сессий).

Сложно разработать архитектуру, в которой бы не столкнулись с проблемами. Так и в данном решении есть ряд проблем, которые тормозят разработку. Сложность работы с SIP-сообщениями, а именно: сложность в обнаружении окончания вызова. Работа с файловой системой (именования cdr-файлов, иерархия, вложенность). При работе с большим количеством информации необходимо корректно организовать механизм записи/передачи cdr-файлов в основное хранилище, так как любая система хранения данных: жесткие диски, твердотельные диски (SSD) и сетевые хранилища данных (SAN), имеют ограниченное значение IOPS – количество операций ввода/вывода информаций.

Список используемых источников

1. Статья 13 Федерального закона от 06.07.2016 г. № 374-ФЗ О внесении изменений в Федеральный закон «О противодействии терроризму» и отдельные законодательные акты Российской Федерации в части установления дополнительных мер противодействия терроризму и обеспечения общественной безопасности: Принят Государственной Думой 24 июня 2016 г. Одобрен Советом Федерации 29 июня 2016 г. Москва. 33 с. [Электронный ресурс] / URL: http://www.kremlin.ru/acts/bank/41108/

2. Статья 64 Федерального закона РФ от 07.07.2003 г. №126-ФЗ «О связи»: Принят Госдумой 18.06.2003г. Одобрен Советом Федерации 25.06.2003 г. (последняя редакция) [Электронный ресурс] /URL: http://docs.cntd.ru/document/901867280/

3. Приказ Минкомсвязи России №86 от 26.02.2018 «Об утверждении Правил применения оборудования систем коммутации, включая программное обеспечение, обеспечивающего выполнение установленных действий при проведении оперативно-розыскных мероприятий. Часть IV. Правила применения оборудования систем коммутации, включая программное обеспечение и технические средства накопления голосовой информации, обеспечивающего выполнение установленных действий при проведении оперативно-розыскных мероприятий». Зарегистрирован в Минюсте РФ 28.03.2018 №50536: Москва. 78 с. [Электронный ресурс] / URL: https://digital.gov.ru/ru/documents/6006/

УДК 65.01
ГРНТИ 20.15.05

НОВАЯ ПАРАДИГМА ПРЕДОСТАВЛЕНИЯ ИНФОКОММУНИКАЦИОННЫХ УСЛУГ НА БАЗЕ БЛОКЧЕЙН-ПЛАТФОРМ

К. Э. Есалов, А. В. Помогалова, С. А. Родионов

Санкт-Петербургский государственный университет телекоммуникаций им. проф. М. А. Бонч-Бруевича

На сегодняшний день существует большое количество различных способов и средств предоставления инфокоммуникационных услуг. Но, как в любых подобных сервисах и системах, наиболее актуальным до сих пор остается вопрос безопасности и удобства предоставления услуг. Одним из решений данной проблемы является возможность использования технологии блокчейн. В данной работе рассматривается блокчейн-платформа, которая позволяет предоставлять инфокоммуникационные услуги безопасно, сохраняя информацию о произведенных действиях в блокчейн-сети. Также рассматривается архитектура данного решения и акцент производится на разбор умных контрактов, которые отвечают за автоматизацию и безопасность оказываемых услуг, относясь к части взаимодействия с блокчейн-сетью Ethereum.

Blockchain, Singularity, распределенный реестр, умные контракты, Ethereum, искусственный интеллект.

Введение

На сегодняшний день на рынке представлено множество различных решений для сферы предоставления различных инфокоммуникационных услуг, улучшения качества предоставления услуг. Одним из таких решений и является, рассматриваемая в рамках данной статьи, децентрализованная блокчейн-платформа SingularityNET.

Одной из особенностей данной платформы является использование технологии блокчейн. Блокчейн (*blockchain*) – в дословном переводе «цепь блоков», это технология организации информации в, криптографически защищенные и последовательно связанные, блоки. Обычно эта технология применяется для обеспечения децентрализованности, то есть распределенности и защищенности данных, их неизменяемости. Стоит учитывать, что данная технология также обеспечивает высокую сложность для атаки и расшифровки данных [1].

Обычно для обеспечения взаимодействия между каким-либо решением и блокчейн-сетью используются умные контракты. Умный контракт (*smart contract*) – это самоисполняемый компьютерный алгоритм, представленный в виде программного кода в блокчейн-сети, который не требует дополнительной активации после загрузки программного кода в блокчейн-сеть. Умные контракты позволяют проводить транзакции без участия в них третей стороны, согласно логике, прописанной в коде умного контракта.

Благодаря умным контрактам становится возможным простое и удобное внедрение технологии блокчейн в уже существующие решения и платформы. Таким примером может служить рассматриваемая платформа.

Децентрализованная платформа SingularityNET

SingularityNET – это децентрализованная платформа, ориентированная на предоставление услуг искусственного интеллекта по всему миру. Главной концепцией данного проекта является возможность поиска и использования услуг искусственного интеллекта в рамках данной платформы, реализованной на базе Ethereum [2].

Впервые проект был представлен в 2017 году, а идея проекта зародилась при осознании отсутствия способов и сервисов поиска и использования, а также продвижения услуг искусственного интеллекта. Данная платформа призвана облегчить и сделать более простым и удобным использование услуг искусственного интеллекта.

Другим определением SingularityNet может служить следующая формулировка: это децентрализованный рынок, такой же как Apple Store и Google Play, который специализируется на продаже вызовов к сервисам на базе искусственного интеллекта.

При этом владелец сервиса, работающего на базе искусственного интеллекта, может зарегистрировать свой сервис на платформе и тем самым позволит любому человеку найти сервис и воспользоваться им. Единственным условием является наличие вычислительных мощностей для полноценного запуска сервиса у его владельца.

Организация взаимодействия платформы с блокчейн-сетью

В рамках рынка SingularityNET реализовано 3 умных контракта, которые работают на базе платформы. Начнем с первого.

Первый смарт-контракт отвечает за реализацию токена платформы AGI (*Artificial General Intelligence*), созданного по стандарту ERC20. Эмиссия данного токена ограничена в количестве 1.000.000.000. Все единицы токена были единовременно выпущены и распределены среди участников ICO и команды разработчиков. Данный токен предназначен для работы в качестве внутренней валюты платформы и для проведения транзакций в рамках действий на децентрализованном рынке.

Второй умный контракт – Registry. Этот контракт служит для регистрации сервисов, которые предоставляют услуги искусственного интеллекта. Данный контракт содержит в себе минимальную необходимую информацию о сервисе, а конкретнее – его идентификационный номер и ссылку на его метаданные. Сервисы в Registry сгруппированы в организации. Каждый человек может зарегистрировать организацию и создавать сервисы внутри этой организации.

Третий смарт-контракт – MultiPartyEscrow, в свою очередь, отвечает за упрощение оплаты сервисов с использованием однонаправленных каналов. Для понимания, такие каналы представляют из себя значительно упрощенный, но более быстрый аналог Lightning Network. Каждая транзакция в Ethereum имеет определенные комиссионные сборы, а время записи транзакции достаточно длительное, поскольку зависит от комиссии, назначенной за транзакцию, но также от времени, необходимого на валидацию транзакции, и подтверждения ее нахождения в основной цепи блоков, что опять же занимает время. В целом, транзакция происходит в течении нескольких минут. Именно поэтому оплата транзакций в случае такого децентрализованного рынка выглядит не практичной. В смарт-контракте MultiPartyEscrow пользователь создаёт платежный канал с организацией, предоставляющей сервисы, и резервирует в этом канале определенную сумму AGI токенов [3]. Эта операция требует одной транзакции в рамках платформы Ethereum. После этого клиент может оплачивать любой сервис организации с помощью внутренних транзакций в рамках зарезервированной суммы токенов. При этом владелец организации может в любой момент забрать токены, уже оплаченные клиентом, не закрывая канал (то есть клиент сможет продолжить использовать сервис). Платежный канал устроен таким образом, что он безопасен как для клиента (сервис сможет потребовать не более фактически потраченной клиентом суммы), так и для сервис-провайдера (клиент не сможет забрать деньги из канала или иным другим способом воспрепятствовать переводу сервис-провайдеру фактически потраченной суммы).

В рамках проекта SingularityNET реализовано децентрализованное приложение SNET DApp, которое позволяет ознакомиться со списком доступных служб ИИ и взаимодействовать с ними через веб-интерфейс, где и функционируем рассмотренные умные контракты.

Отразим структурно как происходит взаимодействие при реализации 3 различных сценариев.

В случае регистрации сервиса, поставщик использует консольную утилиту SNet CLI (рис. 1). Она производит вызов контракта Registry, который, в свою очередь, добавляет полную информацию описания данных сервиса в IPFS базу данных, а контракт Registry содержит очень краткую информацию о сервисе. Файловая система IPFS содержит полное описание сервиса, данные о стоимости его использования и другие необходимые данные.

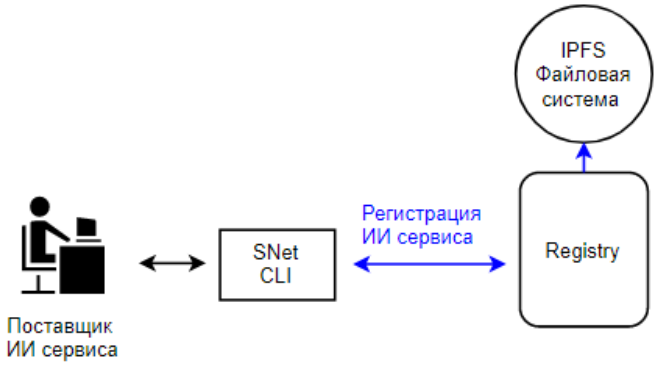


Рис. 1. Схема взаимодействия в рамках первого сценария

Когда речь идет о вызове услуг сервиса клиентом, то клиент использует web-интерфейс децентрализованного приложения. Далее происходит открытие платежного канала с обращением к умному контракту MultiParty Escrow (рис. 2, см. ниже). Далее вызов самого сервиса после его оплаты происходит с помощью демона SNet, который взаимодействует с блокчейн-сетью для упрощения авторизации и оплаты услуг, а также выступает в качестве промежуточного звена для выполнения вызовов к услугам сервиса. Демон – это утилита-шлюз, позволяющий контролировать доступ к службе поставщика услуг ИИ.

Если пользователю необходимо узнать описание сервиса, то обращение происходит к файловой системе IPFS, где хранится полная информация о сервисе (рис. 3, см. ниже). Сервисы, которые публикуются в сети SingularityNET, также называют агентами. Доступ к сервису осуществляется с использованием токена AGI [3].

Таким образом, данная разработка позволяет наладить коммуникацию между поставщиками и потребителями услуг искусственного интеллекта [4]. Теперь поставщикам интеллектуальных сервисов необходимо заниматься только разработкой на базе искусственного интеллекта и регистрировать разработанные сервисы на платформе SingularityNET, поскольку децентрализованное приложение платформы уже позволяет производить поиск и использование подобных сервисов.

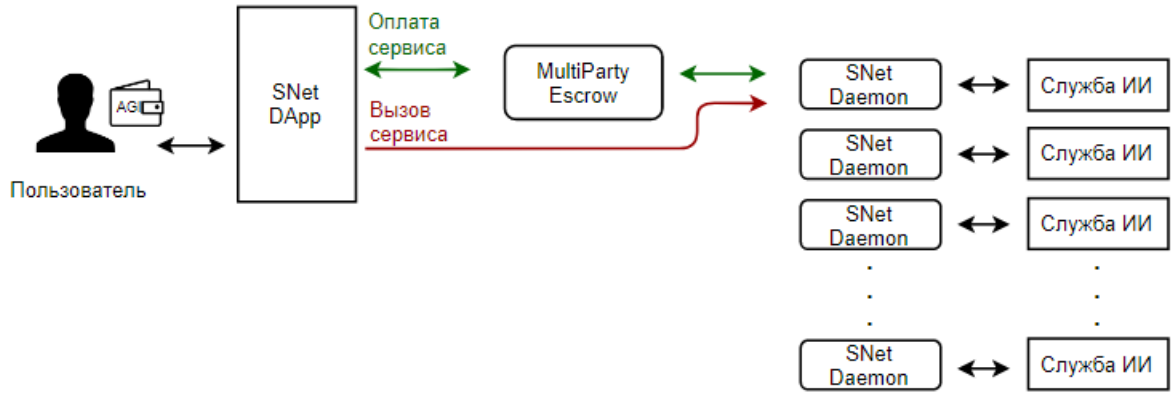


Рис. 2. Схема взаимодействия в рамках второго сценария

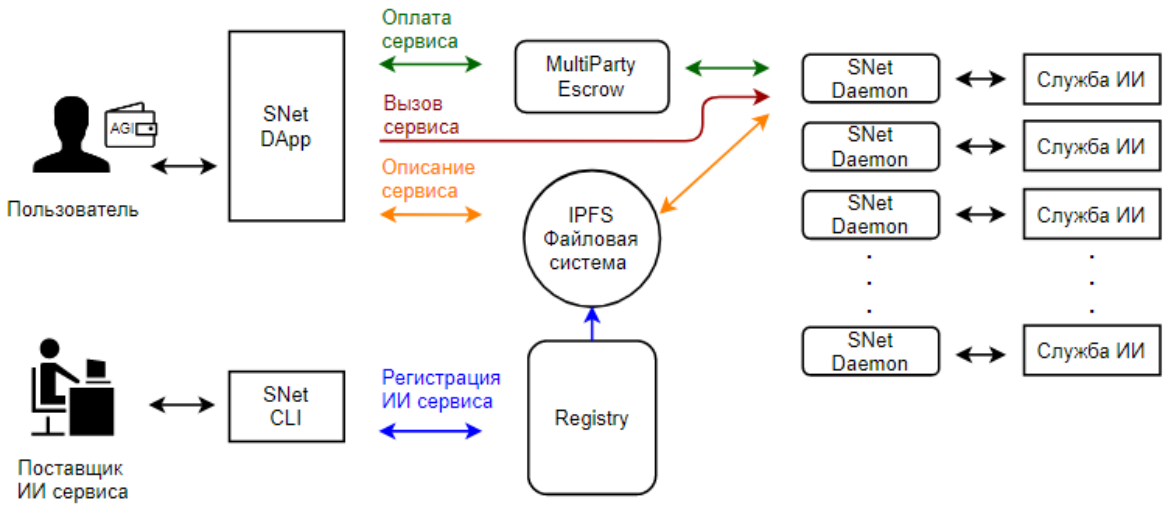


Рис. 3. Схема взаимодействия в рамках третьего сценария

Список используемых источников

1. Tapscott D., Tapscott A. Blockchain Revolution: How the Technology Behind Bitcoin is Changing Money, Business, and the World. M., 2017. 324 с.

2. Любимова О. Создатель Ethereum: «Блокчейн поможет искоренить коррупцию» [Электронный ресурс] // Inc. 2017. URL: https://incrussia.ru/understand/sozdatel-ethereum-vitalik-buterin-blokcheyn-pomozhet-iskorenit-korruptsiyu/ (дата обращения 15.03.2020).

3. Jesus Rodriguez, The Launch of SingularityNet Beta and the Day Decentralized AI Became Real [Электронный ресурс] // Medium. URL: https://towardsdatascience.com/the-launch-of-singularitynet-beta-and-the-day-decentralized-ai-became-real-b12b8163211 (дата обращения 17.02.2020).

4. A. Potapov, S. Rodionov, M. Peterson, O. Scherbakov, I Zhdanov, N. Skorobogatko. Vision System for AGI: Problems and Directions [Электронный ресурс]. URL: https://arxiv.org/ftp/arxiv/papers/1807/1807.03887.pdf (дата обращения 25.02.2020).

УДК 004.51
ГРНТИ 81.93.29

ВИРТУАЛЬНАЯ РЕАЛЬНОСТЬ В ВИЗУАЛЬНОЙ АНАЛИТИКЕ ГРАФОВ

К. Н. Жернова, М. В. Коломеец

Санкт-Петербургский институт информатики и автоматизации Российской академии наук

Анализ графовых структур данных является распространенной задачей во множестве областей информатики: анализ социальных сетей, компьютерных сетей, файловых систем, зависимостей сервисов и т.д. Данная работа посвящена визуальной аналитике графовых структур с использованием виртуальной реальности. Исследуется вопрос эффективности восприятия информации оператором при анализе графов с различной степенью связности и размера. При этом эффективность оценивается по объективным показателям (скорость принятия решений и точность выполнения задачи при визуальном анализе) и субъективным показателям (удобство использования виртуальной реальности в визуальной аналитике). Оценка производится двойным рандомизированным методом в сравнении с использованием экрана компьютера, клавиатуры и мыши.

виртуальная реальность, пользовательские интерфейсы, информационная безопасность, визуализация данных, оценка эффективности.

Визуальная аналитика часто используются в системах поддержки принятия решений в различных областях. При этом, для аналитика наиболее сложным в представлении являются данные, которые имеют графовую структуру. Одним из способов улучшения восприятия оператором таких данных (и как следствие, повышение скорости и качества принимаемых решений) является использование новых средств человеко-машинного взаимодействия, таких как сенсорные экраны, виртуальная и дополненная реальность [1].

В данной работе мы рассматриваем вопрос эффективности использования виртуальной реальности для представления графовых структур в сравнении с их представлением посредством LCD экрана. Для этого был разработан программный прототип тестирования восприятия оператора.

Программный прототип был разработан на UNITY и включает в себя две программы:

– VR тестирование, предназначенное для запуска на ПК с подключенными VR очками HTC Vive [2].

– LCD тестирование, предназначенное для запуска на ПК с подключенным LCD монитором.

В данных программах последовательно отображаются 10 графов, которые являются представлением графов друзей социальной сети [3]. Графы варьируются в размере от 500 до 10000 вершин и одинаковы для обеих программ.

Также, для обеих программ для расчета координат вершин используются силовой метод отрисовки [4] с одинаковыми параметрами. Таким образом, достигается одинаковое изображение для двух тестов.

Единственным отличием в программных прототипах является метод управления.

Для VR прототипа перемещение камеры и масштабирование изображения реализуется посредством VR очков – пользователь перемещается по комнате и, для того, чтобы рассмотреть часть графа, ему необходимо подойти к ней. Переключение между графами происходит при нажатии на тачпад контроллера, который дается пользователю в руку.

Для LCD прототипа перемещение камеры реализуется посредством клавиатуры (на манер компьютерных игр), а масштабирование – посредством прокрутки колесика мыши. Переключение между графами происходит при нажатии на клавишу Enter.

Примеры отображения первых двух графов тестирования в VR прототипе изображена на рис. 1 и 2.

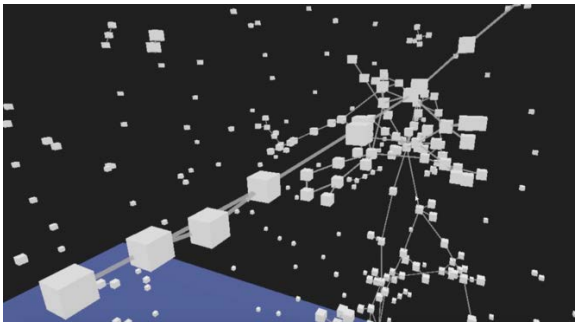


Рис. 1. Изображение графа № 1 в VR прототипе

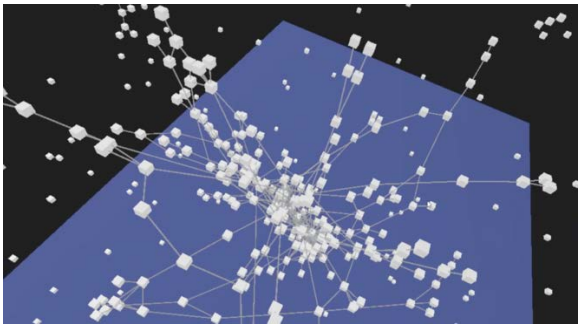


Рис. 2. Изображение графа № 2 в VR прототипе

Оценка эффективности восприятия производится по критерию скорости и точности. Для этого пользователю могут даваться определенные наблюдателем задания. Например, оценить количество вершин, оценить количество связей, оценить количество вершин, которые имеют больше двух связей и т. д. Ключевым условием в формировании задания является возможность определить правильный результат в численном выражении для того, чтобы сравнить его с ответом пользователя. Так как пользователь может переключаться между графами путем нажатия на кнопку контроллера или клавиатуры, программа фиксирует время отображения графа. Таким образом, становится возможным определить скорость и точность.

Скорость – время выполнения задания. Фиксируется программой, как разница во времени, когда начал отображаться граф и когда пользователь переключил граф на следующий.

Точность – отношение между правильным ответом и ответом пользователя. Фиксируется наблюдателем, который получает ответ на задание от пользователя.

Оценка субъективных показателей производится посредством анкетирования пользователей, прошедших тест. Анкета является классическим SUS тестом [5] из 10-ти вопросов, применяемым для оценки удобства использования программы.

Таким образом, в результате тестирования можно получить три оценки: скорость, точность и субъективную оценку удобства.

Данный подход и программный прототип можно использовать для оценки восприятия пользователя. В будущем планируется провести тесты на группах студентов для того, чтобы получить распределения оценок, по которым можно будет получить средние значения эффективности.

Выводы

Данная работа содержит описание подхода к оценке эффективности VR для визуальной аналитики графовых структур. Предложена оценка по трем показателям скорости, точности и субъективной оценки удобства методом двойного рандомизированного тестирования. Был разработан прототип системы оценки, который работает с VR и LCD, и позволяет получить, и после сравнить, оценки эффективности.

Работа выполнена при частичной финансовой поддержке РФФИ (проект 18-37-20047-мол_а_вед).

Список используемых источников

1. Коломеец М. В., Чечулин А. А., Котенко И. В. Использование виртуальной и дополненной реальности для визуализации данных кибербезопасности // Защита информации. Инсайд. 2017. Т. 5. № 77. С. 58–63.

2. Borrego A. et al. Comparison of Oculus Rift and HTC Vive: feasibility for virtual reality-based exploration, navigation, exergaming, and rehabilitation //Games for health journal. 2018. Т. 7. N 3. PP. 151–156.

3. Kolomeets M., Chechulin A., Kotenko I. Social networks analysis by graph algorithms on the example of the V Kontakte social network // J. Wirel. Mob. Networks, Ubiquitous Comput. Dependable Appl. 2019. Т. 10. N 2. PP. 55–75.

4. Kalameyets M., Chechulin A., Kotenko I. The technique of structuring social network graphs for visual analysis of user groups to counter inappropriate, dubious and harmful information // CEUR Workshop Proc. 2018. Т. 2258. PP. 87–95.

5. Saco M., Thigpen J. A quick and dirty usability scale // J. Drugs Dermatology. 2014. Т. 13. N 5. PP. 531–536.

Статья представлена научным руководителем, канд. техн. наук А. А. Чечулиным.

УДК 004.51
ГРНТИ 81.93.29

ОБЗОР МЕТОДИК ОЦЕНКИ ЭФФЕКТИВНОСТИ СИСТЕМ ВИЗУАЛЬНОЙ АНАЛИТИКИ

К. Н. Жернова, М. В. Коломеец

Санкт-Петербургский институт информатики и автоматизации Российской академии наук

В современных средствах компьютерной безопасности применяются разнообразные модели визуализации. Эти модели могут различаться по уровню сложности, и по этой причине требуется разработка моделей человеко-компьютерного взаимодействия, наиболее подходящих для каждой конкретной модели визуализации. Однако сложность модели не должна снижать эффективность взаимодействия с этой моделью. В данном докладе предлагается методика экспериментальной оценки эффективности человеко-компьютерного взаимодействия с приложениями компьютерной безопасности.

человеко-компьютерное взаимодействие, информационная безопасность, пользовательские интерфейсы, визуализация данных, оценка эффективности.

В настоящее время, по мере развития компьютерных сетей и систем, возрастает количество инцидентов компьютерной безопасности. Таким образом, возрастает важность визуальной аналитики этих инцидентов. Разрабатываются новые модели визуализации, которые позволяют более качественно анализировать поступающую информацию, касающуюся безопасности сети [1]. Однако, прежде чем начинать использовать ту или иную модель визуализации в системах визуальной аналитики, требуется провести оценку этой модели.

При оценке эффективности моделей визуализации для систем визуальной аналитики используются различные методики оценки. Подобные методики основываются на различных данных. Для более эффективного комбинирования методик оценки требуется их классифицировать по способу получения этих данных.

Классификация методик оценки по признаку формализации

Существуют методы оценки с участием пользователя или без участия пользователя, при этом они могут быть формализованы (используются какие-то формальные показатели, например, время, скорость, точность и т. д.) или не формализованы (представлены в виде мнений пользователей, экспертов и т. д.). Таким образом, получаются следующие группы методов оценки:

1) формализованные без участия пользователя;

2) формализованные с участием пользователя;
3) не формализованные с участием пользователя;
4) не формализованные без участия пользователя.

Очевидно, что не формализованных методов без участия пользователя получить нельзя, поэтому остаются три группы методов оценки [2]:

1) сильные (формализованные, без участия пользователя);
2) относительно сильные (формализованные, с участием пользователя);
3) слабые (не формализованные, с участием пользователя).

Различные методы оценки [3, 4, 5], применяющиеся к моделям визуализации, приведены в таблицах ниже. Методы оценки можно разделить по степени формализации (табл. 1) на сильные методы (используется формальная оценка), относительно сильные (используются формализованные мнения пользователей) и слабые (мнения пользователей не формализованы).

ТАБЛИЦА 1. Способы оценки визуализации в зависимости от степени формализации

Сильные	Относительно сильные	Слабые
Контекстное исследование	Эвристические оценки	Опросы
Формирующие и суммирующие юзабилити-тесты	Когнитивные пошаговые решения задач	Фокус-группы
Веб/Поисковая аналитика	Обратная связь экспертов юзабилити, которые выполняли реальные задачи	Экспертные оценки
А/Б тестирование	Построение маршрутов пользователей	Мнение друзей, коллег и т. д.
Многофакторное тестирование	Исследования дневников	Интуиция
Контролируемые эксперименты	Карточная сортировка	Личный опыт
Анализ задач	Отслеживание взгляда	Немодерированное тестирование с комментированием вслух

В зависимости от стадии разработки, можно разделить методы оценки на оценки на этапе проектирования, оценки на этапе разработки и оценки на этапе тестирования (табл. 2, см. ниже).

Степень формализации метода оценки показана цветом заполнения ячейки. Наиболее формальные методы выделены голубым цветом, методы относительно формальные выделены жёлтым, не формализованные методы показаны красным.

ТАБЛИЦА 2. Способы оценки визуализации в зависимости от стадии разработки

Проектирование	Разработка	Тестирование
Интервью, мнения	Семинары по проектированию (групповые обсуждения)	Сеансы парного анализа
Наблюдение за пользователями	Бумажное прототипирование и макеты	Количественные тестирования
Контекстные запросы	Обратная связь экспертов юзабилити, которые выполняли реальные задачи	Экспертные оценки
Анкетирование (опросы)	Выделенные юзабилити-тесты	Немодерированное тестирование с комментированием вслух
Фокус-группы	Эвристические оценки	Формирующие и суммирующие юзабилити-тесты

Из таблицы 2 видно, что на различных этапах проектирования визуализации используются методы разной степени формализации.

Выводы

Данный обзор методик оценки эффективности визуализаций даёт простую классификацию способов оценки на основе степени формализации оценки. На разных этапах проектирования могут быть использованы методы каждой из представленных групп.

На разных этапах разработки следует использовать как сильные, так и слабые методы оценки, поскольку, несмотря на хорошие формальные показатели, созданная визуализация может оказаться неудобной для пользователя и, следовательно, менее эффективной.

Работа выполнена при частичной финансовой поддержке РФФИ (проект 19-17-50173).

Список используемых источников

1. Коломеец М. В., Чечулин А. А., Котенко И. В. Обзор методологических примитивов для поэтапного построения модели визуализации данных // Труды СПИИРАН. 2015. Т. 5. № 42. С. 232–257.

2. Travis D., Hodgson P. Think Like a UX Researcher: How to Observe Users, Influence Design, and Shape Business Strategy. CRC Press, 2019.

3. Sedlmair M. et al. Information visualization evaluation in large companies: Challenges, experiences and recommendations // Information Visualization. 2011. Т. 10. N 3. PP. 248–266.

4. Lam H. et al. Seven guiding scenarios for information visualization evaluation. 2011.

5. Plaisant C. The challenge of information visualization evaluation // Proceedings of the working conference on Advanced visual interfaces. 2004. PP.109–116.

Статья представлена научным руководителем, кандидатом технических наук А. А. Чечулиным.

УДК 004.51
ГРНТИ 81.93.29

МОДЕЛИ ВИЗУАЛЬНОГО ЧЕЛОВЕКО-КОМПЬЮТЕРНОГО ВЗАИМОДЕЙСТВИЯ С СЕТЬЮ УСТРОЙСТВ ИНТЕРНЕТА ВЕЩЕЙ

К. Н. Жернова, Н. А. Комашинский, И. В. Котенко

Санкт-Петербургский институт информатики и автоматизации Российской академии наук

Технология Интернета вещей постоянно развивается, при этом, число устройств, подключённых к Интернету вещей, со временем увеличивается. Для управления подобной сетью с большим количеством устройств и отслеживания её состояния используются сложные модели визуализации, например, графы. Так, по мере усложнения сети, возникает необходимость разрабатывать новые более эффективные модели человеко-компьютерного взаимодействия с визуализацией сети Интернета вещей. Данная работа представляет возможные решения для человеко-компьютерного взаимодействия с сетью устройств.

человеко-компьютерное взаимодействие, информационная безопасность, пользовательские интерфейсы, визуализация данных, Интернет вещей, сенсорные экраны.

Введение

В настоящее время управление сетью Интернета вещей становится доступным на мобильных вычислительных устройствах. Многие мобильные устройства имеют сенсорный экран, что подразумевает появление новых

способов взаимодействия с такими сетями. Сети Интернета вещей постоянно расширяются, получая применение в различных областях, таких как «умные» дома/города, беспилотный транспорт, мониторинг безопасности и т. п. Данная тенденция обуславливает увеличение количества обрабатываемой информации, передающейся в таких сетях.

Однако сети Интернета вещей не лишены проблем в области информационной безопасности. При мониторинге безопасности такой сети требуется обрабатывать огромное количество различных данных об инцидентах безопасности, затем требуется анализировать эти данные и принимать решения о дальнейших мерах противодействия угрозам [1]. Все эти задачи усложняют взаимодействие оператора с системой, таким образом, требуется разработать модель человеко-компьютерного взаимодействия, которая повысит эффективность работы с сетью Интернета вещей.

Модели взаимодействия с сетью Интернета вещей

Поскольку к сети Интернета вещей может быть подключено большое количество устройств, которые могут быть связаны как в централизованную иерархическую сеть, так и в децентрализованную, удобнее всего представлять данную сеть в виде графа.

Граф сам по себе является довольно сложной моделью визуализации. Кроме того, по мере увеличения количества устройств, подключенных к сети Интернета вещей, требуются специальные модели человеко-компьютерного взаимодействия для управления сетями устройств и инцидентами безопасности, возникающими в данных сетях.

В настоящее время довольно распространённым способом человеко-компьютерного взаимодействия являются сенсорные экраны, кроме того, они достаточно изучены с точки зрения юзабилити [2]. Также разрабатываются различные модели взаимодействия именно с сенсорными экранами, подходящие именно для управления компьютерной безопасностью [2, 3]. Модель человеко-компьютерного взаимодействия с сетью включает в себя компонент взаимодействия и компонент визуализации.

Компонент визуализации сети Интернета вещей

На рисунках ниже представлены примеры визуализированных сетей Интернета вещей. Рис. 1 (см. ниже) показывает модель визуализации с точным отображением устройств, участвующих в построении сети. На рис. 2 (см. ниже) изображена аналогичная сеть, однако различные виды устройств представлены в виде условных обозначений, максимально отличающихся друг от друга цветом и формой. Предполагается, что при большом количестве устройств в сети условные обозначения позволят лучше различать виды устройств между собой.

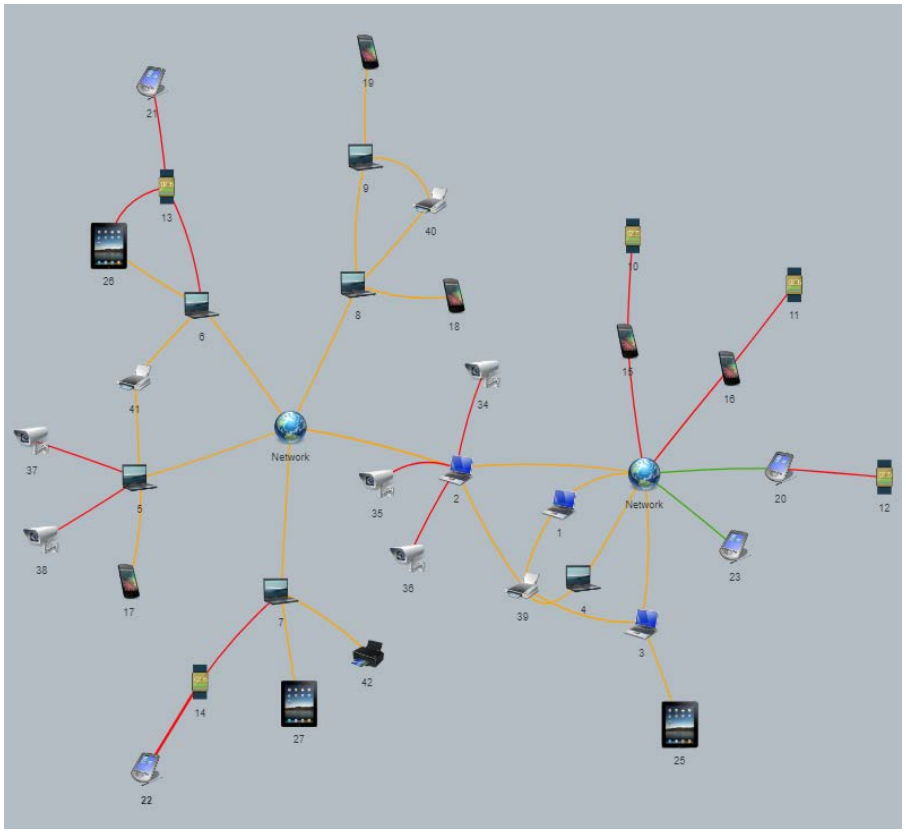


Рис. 1. Визуализация сети устройств Интернета вещей

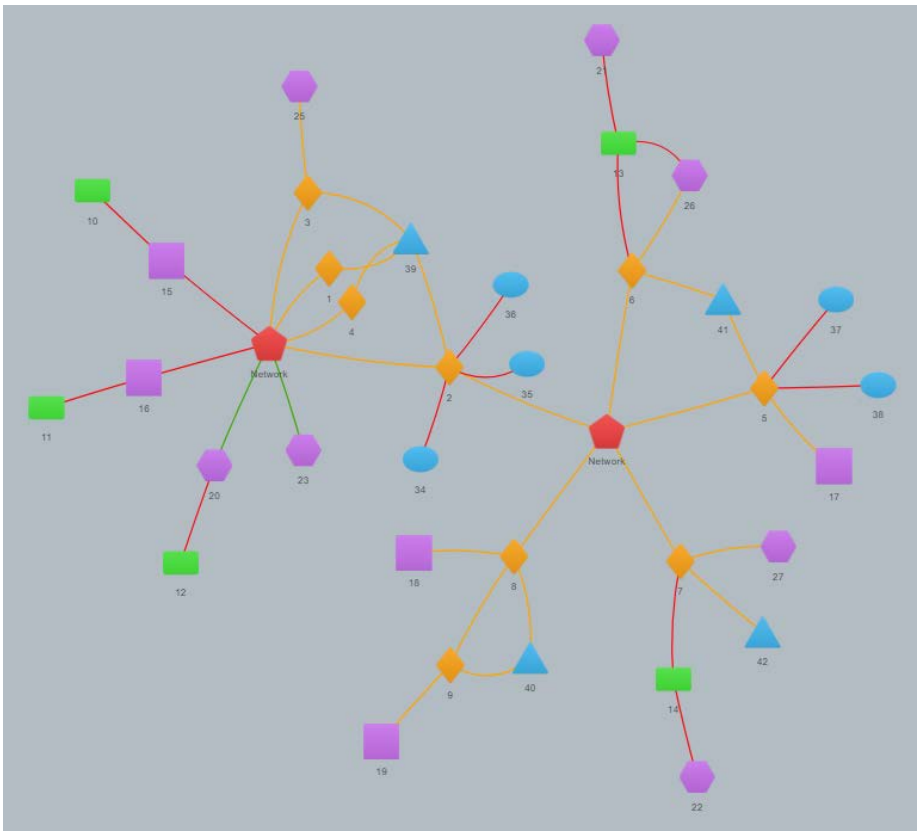


Рис. 2. Визуализация аналогичной сети при помощи простых фигур

Компонент взаимодействия с сетью Интернета вещей

Для управления сетью устройств Интернета вещей требуются следующие действия:

1) управление устройствами (вершины графа);
2) масштабирование (изменение вида графа сети устройств);
3) фильтрация (отбор устройств по определённому признаку);
4) выделение;
5) перемещение между уровнями сети устройств.

Управлять устройствами можно с помощью жеста drag&drop, т. е., выбирая вершину графа с изображением устройства и перетягивая её в нужное место.

Фильтрация может осуществляться с помощью выбора определённого устройства и выбора нужной опции в контекстном меню.

Для выделения нужного участка сети может использоваться жест разведения двух пальцев в разные стороны с появлением квадратной области.

Сведение/разведение несколькими пальцами может использоваться для перемещения между уровнями сети или изменения её отображения.

Также для графов больших сетей актуален вызов информации по требованию, так как при большом количестве информации модель визуализации окажется перегруженной. Дополнительную информацию можно вызывать с помощью быстрого двойного прикосновения (*double tap*), при этом убрать информацию можно, сделав «стирающий» жест рукой (*swipe* несколькими пальцами влево или вправо).

Выводы

Для улучшения эффективности управления сетью устройств Интернета вещей можно применять различные жесты взаимодействия с сенсорным экраном. Граф сети Интернета вещей может быть представлен разными способами, как с помощью точного отображения участвующих устройств, так и с помощью условных обозначений. В дальнейшем планируется провести исследование об эффективности того или иного способа представления графа, а также способов взаимодействия с ним с помощью жестов на сенсорных экранах.

Работа выполнена при частичной финансовой поддержке РФФИ (проект 18-07-01488-а).

Список используемых источников

1. Kotenko I., Saenko I., Branitskiy A. Framework for mobile Internet of Things security monitoring based on big data processing and machine learning // IEEE Access. 2018. Т. 6. PP. 72714–72723.

2. Котенко И. В. и др. Модель человеко-машинного взаимодействия на основе сенсорных экранов для мониторинга безопасности компьютерных сетей // Региональная информатика (РИ-2018). XVI Санкт-Петербургская. 2018. С. 149.

3. Котенко И. В. и др. Методы человеко-машинного взаимодействия на основе сенсорных экранов в ситуационных центрах безопасности // Информационные технологии в управлении (ИТУ-2018). 2018. С. 554–558.

УДК 004.716
ГРНТИ 49.33.29

СТРУКТУРА ВЗАИМОДЕЙСТВИЯ БЕСПИЛОТНЫХ АВТОМОБИЛЕЙ С СЕТЕВОЙ ИНФРАСТРУКТУРОЙ

А. А. Задорожняя, Р. В. Киричек, Д. О. Реутова

Санкт-Петербургский государственный университет телекоммуникаций им. проф. М. А. Бонч-Бруевича

Технологии реализации беспилотного автотранспорта стремительно развиваются и в ближайшем будущем станут неотъемлемой частью человеческой жизни. Но для удобства использования таких технологий необходимо разработать новую структуру взаимодействия БПА с сетевой инфраструктурой на основе первого поколения беспилотного автотранспорта. Это, так называемая, «концепция второго поколения беспилотного автотранспорта», которая сейчас активно изучается, в связи с чем, перед научным сообществом стоит ряд задач, среди которых создание архитектуры и разработка требований построения сетевой инфраструктуры БПА.

беспилотный автомобиль (БПА), сетевая инфраструктура, датчики, лидары, сканеры радаров.

Многие концерны, такие как Yandex, Tesla, КАМАЗ, General Motors [1, 2, 3] активно разрабатывают беспилотные автомобили, а также тестируют их на своих полигонах. Но в марте 2018 года в США произошел случай, который привел к фатальным последствиям. Велосипедист неожиданно выскочил на дорогу и камера, расположенная на беспилотном автомобиле (БПА), не успела своевременно распознать движущийся объект, и автомобиль не успел затормозить [4, 5]. В результате, многие люди стали относить БПА к критической инфраструктуре, способной нанести вред здоровью человека. На сегодняшний день актуален вопрос о необходимости дублирования функций принятия решения БПА на сторонние средства.

Можно предложить несколько вариантов дублирования таких функций.

В военных структурах существуют системы дублирования на каждом устройстве (резервные устройства). Например, в космосе втройне дублируются команды. Поэтому изначально было предложено поставить второй бортовой компьютер в автомобиль, который также дублировал действия первого и «подхватывал» действия в случае отказа работы первого. Но фактически этот вариант не решает вопрос с точки зрения обработки данных.

Поэтому была предложена концепция сетевой поддержки, которая предполагает расположение вдоль автодорог микрооблаков, которые будут принимать данные от автомобиля (данные со сканеров радаров, лидаров и датчиков), обрабатывать и «подтягивать» информацию о том, что происходит вокруг, и передавать в виде управляющих команд на автомобиль. То есть, эти микрооблака, фактически, есть сетевая поддержка для БПА.

Эта, так называемая, концепция второго поколения беспилотного автотранспорта (БПА) сейчас активно развивается. На данном этапе развития этой концепции придумана референсная (т. е. эталонная) архитектура. В современном мире есть примеры её внедрения, например, концерны General Motors и Tesla перешли на второе поколение.

Использование высокоскоростных каналов передачи – необходимое условие, потому что по расчетам компании Huawei круговая сетевая задержка для БПА должна составлять 20 мс [6]. За это время данные должны считаться с автомобиля, должны быть доставлены в облако, обработаны в облаке и вернуться обратно в виде управляющей команды.

Возникает интересная расчетная задача: а через какое расстояние ставить эти микрооблака и через какое расстояние ставить придорожные базовые станции (БС), которые будут принимать радиосигнал?

Таким образом, задачи на 2021–2024 год: создание архитектуры и разработка требований построения сетевой инфраструктуры БПА.

Как уже говорилось ранее, Международный союз электросвязи (МСЭ) представил эталонную модель сети: вдоль дороги расположены придорожные БС, есть микрооблака, есть миниоблака, есть высокоуровневые облака, которые собирают данные о том, что происходит вокруг [7]. Например, если рядом с БПА движется человек с телефоном, автомобиль или велосипедист, то БПА будет его «видеть», получив данные из этого облака.

Второе поколение беспилотного автотранспорта заключается во взаимодействии беспилотного автомобиля и сетевой инфраструктуры (рис., см. ниже).

Например, по дороге едет автомобиль, вдоль которой стоят базовые станции. Автомобиль связывается с базовой станцией для того, чтобы просчитать правильность маршрута. В случае, если на дороге возникает препятствие, тогда автомобиль должен либо остановиться, либо объехать его, все вычисления делаются в придорожном блоке.

Рис. Архитектура взаимодействия беспилотного автомобиля и сетевой инфраструктуры

Сетевая инфраструктура включает в себя 3 основных уровня:

– первый – базовая станция (*MEC Host*). MEC host состоит из вычислительного элемента, блока планирования, блока управления и блока синхронизации данных. Базовая станция собирает информацию с транспортных средств, светофоров, камер, размещенных на обочине дороги, и радаров, обрабатывает эти данные и строит маршрут для автотранспорта;

– второй – промежуточное облако хранения и обработки информации;

– третий – глобальное облако, которое состоит из блока хранения, блока планирования, базы данных карт, и блока контроля трафика.

Автомобиль оснащен средствами сбора информации (например, камерой сбора данных, радаром, лидаром). После начала движения автотранспорта данные об окружающей обстановке фиксируются и отправляются на ближайшую базовую станцию, которая расположена вдоль дороги. Данные, полученные из автомобиля, анализируются вычислительным элементом и дополняются информацией с базовой станции. Результат передается блоку управления, который строит маршрут с учетом всех возможных препятствий. После чего данные о безопасном маршруте передаются встроенному компьютеру беспилотного автомобиля, и он продолжает движение. Такая архитектура обеспечивает постоянный мониторинг обстановки на дороге и, тем самым, способствует предотвращению аварий.

Для реализации данной технологии требуется рассчитать сетевую задержку, которая возникает с момента передачи данных беспилотного автомобиля на базовую станцию и до возврата обработанной информации обратно автомобилю. Сетевая задержка зависит от следующих параметров:

– оптимальное расстояние между базовыми станциями;

– максимальное расстояние между автомобилем и базовой станцией;

– допустимая скорость автомобиля;

– расстояние между базовой станцией и глобальным облаком.

Следовательно, требуется рассчитать эти параметры для определения требований к сетевой задержке.

Что касается поведения БПА, в настоящее время на его борту находится большое количество устройств для считывания и его позиционирования – это лидары, радары, датчики. Во-первых, каждый из них генерирует большой объём трафика, во-вторых, каждый из них требует определенной скорости передачи данных, так как разные объёмы передаваемых данных.

Результат анализа компании Huawei – в сутки БПА генерирует 1,5 Тб данных, которые надо обрабатывать. В связи с этим, возникает вопрос, касающийся задач обработки данных и задач взаимодействия.

Соответственно, возможно создание различных приложений: удаленная диагностика, возможность мониторинга дорожной сети в целом, аналитика предсказаний дорожно-транспортных происшествий.

В заключении, хочется отметить, что подходы, которые сейчас используются:

1. БПА с сетевой поддержкой;

2. использование «привязных мультикоптеров», как базовой основы для ретрансляции данных, организации связи там, где она не предусмотрена (в труднодоступных районах, где нет традиционных БС);

3. организация каналов связи между инфраструктурой и БПА.

Список используемых источников

1. Fabian Kröger. Automated Driving in Its Social, Historical and Cultural Contexts // Autonomous Driving. Technical, Legal and Social Aspects. Markus Maurer, J. Christian Gerdes, Barbara Lenz, Hermann Winner (ed.). PP. 41–68. URL: https://link.springer.com/content/pdf/10.1007%2F978-3-662-48847-8_3.pdf

2. Дитмар П., Меллер Роланд Ф., Хаас Е. Руководство по техническому подключению и кибербезопасности // Компьютерные коммуникации и сети. Springer International Publishing AG, 2019, 30 с.

3. Гамби А., Мюллер М., Фрастер Г. Неисправность: Испытания программного обеспечения самоуправляемых автомобилей с использованием процедурной генерации контента на основе поиска // IEEE/ACM. 41-я Международная конференция по программной инженерии: сопутствующие издания научного учреждения (Международная конференция по разработке программного обеспечения – компаньон). 2019. 27–30 с.

4. Авария со смертельным исходом в Uber: внедорожник видел водителя, не тормозил: федералы", май 2018. URL: https://zen.yandex.ru/media/id/5aafcccb7ddde8eebb3eadf4/uber-ubral-svoi-samohodnye-avtomobili-s-dorog-posle-avarii-so-smertelnym-ishodom-5ab10249799d9d49e9574320?utm_source=serp

5. Левин С. Тесла со смертельным исходом: В отчете говорится, что режим «автопилот» ускорил автомобиль, прежде чем водитель погиб // The Guardian, июнь 2018.

6. 3GPP. Изучение поддержки LTE для услуг Vehicle-to-Everything (V2X) // TR 22.885 V.

7. ITU-T SG 20. Рекомендация Y.NDA-arch «Функциональная архитектура».

УДК 004.056.53
ГРНТИ 81.93.29

НЕЙРОННЫЕ СЕТИ ДЛЯ МОНИТОРИНГА И ПРОТИВОДЕЙСТВИЯ НЕЖЕЛАТЕЛЬНОЙ ИНФОРМАЦИИ В СЕТИ ИНТЕРНЕТ

П. М. Залесова[1], И. Б. Саенко[2]

[1]Санкт-Петербургский государственный университет телекоммуникаций им. проф. М. А. Бонч-Бруевича
[2]Санкт-Петербургский институт информатики и автоматизации Российской академии наук

Проблема противодействия распространению нежелательной информации в общем, и кибербуллингу, в частности, в сети Интернет является острой для современного общества. Современные системы мониторинга сети Интернет все чаще разрабатываются с использованием алгоритмов глубокого обучения нейронных сетей. В работе исследуются методы, модели и алгоритмы глубокого обучения, предлагаются возможные реализации и подходы, направленные на непосредственный анализ информации. Отдельно предложена классификация мер противодействия распространению нежелательной информации, основанная на распределении зон ответственности среди распространителей.

нежелательная информация, кибербуллинг, противодействие, Интернет, социальные сети, нейронные сети.

В связи с быстрым развитием Интернет-технологий, люди все больше погружаются в сеть. Отличным способом для коммуникаций являются социальные сети. Взаимодействие в сети становится причиной совершения различных видов киберпреступлений, таких как фишинг, спам, распространение вредоносных программ. Серьезной проблемой для пользователей стал кибербуллинг [1].

Кибербуллинг относится к агрессивному, преднамеренному акту, совершаемому группой или отдельным лицом в киберпространстве с использованием информационных и коммуникационных технологий неоднократно или в течение длительного времени против жертв, которые не могу защитить себя [1, 2]. Кибербуллинг или киберзапугивание является серьезной национальной проблемой здравоохранения.

В России, на сегодняшний день, самая популярная социальная сеть – «ВКонтакте». По текущим данным «ВКонтакте» содержит 585 млн зарегестрированных пользователей (без учета удаленных страниц, неактивных профилей, фейковых аккаунтов). Ежедневно сайт посещает около 85 млн человек.

4 ноября 2019 года в «ВКонтакте» начали эксперимент по защите от кибербуллинга, запустив функцию по борьбе с оскорблениями. Функция заключается во введении новых алгоритмов, которые при наборе комментария определяют, есть ли в нем признаки оскорбления. В случае их выявления, автор получает совет отказаться от обидного фрагмента и не тратить время на агрессию [3]. Также в июле 2019 функцию защиты от оскорблений запустил Instagram.

Для борьбы с кибербуллингом используются различные методы, например, интеллектуальный анализ данных или построение модели машинного обучения с набором функций, которая включает в себя информацию о сети, информацию об активности пользователей, также информацию о самих пользователях, и всю информацию по контенту [4].

В 2015 году Игорь Сантос провел исследование по созданию модели машинного обучения, которая обнаруживает профили, так называемых, «тролей». Используя алгоритмы машинного обучения, авторы анализировали различную информацию, содержащуюся в профиле, например, данные соединения и текст постов, чтобы можно было связать троллинг-аккаунты с соответствующими реальными профилями пользователей [5].

Для обнаружения кибербуллинга было применено несколько различных подходов. Например, несколько лет назад для обнаружения оскорбительных выражений был введен лексико-синтаксический словарь, состоящий из различных оскорбительных выражений, что поспособствовало более точному определению кибербуллинга. Для большей вероятности определения киберзапугивания был разработан подход, основанный на гендерном уровне, который использовал гендерный признак для повышения, способности классификатора к дискриминации [6]. Добавление возраста и пола в качестве характеристики также повлияло на эффективность обнаружения травли в Интернете, но как показала практика, лишь немногие пользователи сети предоставляют полную и достоверную информацию о себе.

Чаван и Шиладжа включили местоимения, Skip-gram, TF-IDF и N-грамму [7]. Однако этих характеристик было недостаточно для анализа динамики данных в Интернете. Кроме того, после появления социальных сетей появились и новые наборы аббревиатур. Это тоже приходится учитывать для решения задачи обнаружения травли.

Не все исследования учитывали поведение и личность человека. Эти факторы также могут быть использованы в качестве признаков, которые увеличивают вероятность обнаружения. Давид Миллер проанализировал места киберзапугивания, используя модель «bagofwords» или мешка слов, чтобы найти наиболее распространенные термины, используемые киберпреступниками [8].

В 2017 году Анна Шмидт и Майкл Виганд провели исследование по выявлению речевых проявлений агрессии с использованием обработки естественного языка [9]. Что касается обнаружения кибербуллинга с использованием глубокой нейронной сети, также проводилось множество исследований.

В октябре 2017 года на хакатоне «ВКонтакте» был представлен проект PyTidor [10]. Были созданы бот для диалогов в «Telegram» и бот-фильтр для сообществ «ВКонтакте». Эти боты взаимодействуют с обученной нейронной сетью, которая распознает, является ли текст агрессивным. Помимо этого, боты могут предупреждать пользователя об агрессивном поведении против него или с его стороны.

В 2019 году на Международной конференции по современным вычислительным и коммуникационным системам был представлен доклад об использовании сверточной нейронной сети [11]. В докладе был представлен новый подход к выявлению травли в Интернете. Это подход использует алгоритм свертки нейронной сети, который работает через несколько слоев и дает более точную классификацию.

В таблице приведены результаты различных существующих систем обнаружения киберзапугивания, основанных на интеллектуальном анализе данных, машинном обучении и системе глубокого обучения на основе нейронных сетей.

ТАБЛИЦА. Сравнение методов обнаружения кибербуллинга

Название статьи	Используемые методы	Точность обнаружения, %
Оптимизированное обнаружение кибербуллинга Twitter на основе глубокого обучения [12]	RNN GloVe	81,60
Обнаружение кибербуллинга и агрессии в социальных комментариях [13]	Обработка естественного языка и машинного обучения	75
Обнаружение кибербуллинга в социальных сетях с использованием методов интеллектуального анализа данных [14]	Интеллектуальный анализ данных	75
Обнаружение кибербуллинга с использованием глубокой нейронной сети [11]	CNN (Convolution Neural Network)	93,97

В данной работе были описаны существующие исследования по распознаванию кибербуллинга в сети Интернет. Проведен сравнительный анализ таких методов как глубокое машинное обучение, интеллектуальный анализ данных и нейронные сети. На основании одного из исследований можно

сказать, что система с использованием глубокой нейронной сети дает лучшие результаты по обнаружению кибербуллинга.

Работа выполнена при частичной финансовой поддержке Российского научного фонда (проект № 18-11-00302) в СПИИРАН.

Список используемых источников

1. Андрианов В. И., Виткова Л.А., Волкогонов В.Н. Вопросы информационной безопасности с точки зрения психологии и виктимологии // Актуальные проблемы инфотелекоммуникаций в науке и образовании. IV Международная научно-техническая и научно-методическая конференция: сб. науч. ст. в 2-х т. СПб. : СПбГУТ, 2015. Т. 1. С. 190–193.

2. Сахаров Ю. А., Жувикин А. Г., Виткова Л. А. Проблема автоматизированного мониторинга графических изображений в сети Интернет // Защита информации. Инсайд. 2017. № 2(74). С. 64–67.

3. Головлева Ю. А., Виткова Л. А., Ковцур М. М., Дмитриева Е. В. Конвергенция информационных технологий для повышения эффективности управления информационным пространством Санкт-Петербурга // Информационная безопасность регионов России (ИБРР-2017): материалы X межрег. конф., Санкт-Петербург, 01–03 нояб. 2017 г. М. : СПОИСУ, 2017. С. 510–512.

4. Пресс-служба ВКонтакте [Электронный ресурс]. URL: https://vk.com/press/no-abuse (дата обращения 25.02.2020).

5. Galán-García P., de la Puerta J. G., Gómez C. L., Santos I., Bringas P. G. (2016) Supervised machine learning for the detection of troll profiles in Twitter social network: Application to a real case of cyberbullying // Logic J. IGPL 24(1):42–53.

6. Ritesh Kumar, Atul Kr. Ojha, Shervin Malmasi, and Marcos Zampieri. 2018a. Benchmarking Aggression Identification in Social Media // In Proceedings of the First Workshop on Trolling, Aggression and Cyberbulling (TRAC), Santa Fe, USA.

7. Chavan V.S., S SS. Machine learning approach for detection of cyber-aggressive comments by peers on social media network // In: 2015 International Conference on Advances in Computing, Communications and Informatics (ICACCI); 2015. PP. 2354–2358.

8. Haoti Zhong, Hao Li, Anna Squicciarini, Sarah Rajtmajer, Christopher Griffin, David Miller, Cornelia Caragea. Content-Driven Detection of Cyberbullying on the Instagram Social Network // Proceedings of the Twenty-Fifth International Joint Conference on Artificial Intelligence (IJCAI-16), 2016. PP. 3952–3958.

9. A. Schmidt and M. Wiegand. A survey on hate speech detection using natural language processing // In: International Workshop on Natural Language Processing for Social Media, Association for Computational Linguistics, 2017, PP. 1–10.

10. PyTidor [Электронный ресурс]. URL: https://thevyshka.ru/15015-hakathon/ (дата обращения 25.02.2020).

11. Banerjee, V., Telavane, J., Gaikwad, P., &Vartak, P. Detection of Cyberbullying Using Deep Neural Network // 2019 5th International Conference on Advanced Computing & Communication Systems (ICACCS); 2019. PP. 604–607.

12. Monirah A. Al-Ajlan, Mourad Ykhlef. Optimized Twitter Cyberbullying Detection based on Deep Learning, 978-1-5386-4110-1, IEEE-2018.

13. Kahitiz Sahay, Harsimran Singh Khaira, Prince Kukreja, Nishchay Shukla. Detecting Cyberbullying and Aggression in Social Commentary using NLP and Machine Learning // International Journal of Engineering Technology Science and Research, Vol. 5, Iss. 1, January 2018.

14. Hariani, Imam Raid. Detection of Cyberbullying on Social Media using Data Mining Techniques // International Journal of Computer Science and Information Security, Vol. 15, No. 3, March 2017.

УДК 004.725.7
ГРНТИ 49.33.29

АНАЛИЗ ЛЕКАРСТВЕННЫХ СРЕДСТВ НА БАЗЕ ССОП С ПРИМЕНЕНИЕМ МЕТОДОВ ИНФРАКРАСНОЙ МИКРОСПЕКТРОСКОПИИ

М. В. Захаров, Р. В. Киричек

Санкт-Петербургский государственный университет телекоммуникаций им. проф. М. А. Бонч-Бруевича

Все более актуальной становится задача анализа состава лекарственных средств с целью проверки их качества в «полевых условиях», что исключает возможность использовать традиционные лабораторные методы. Для проведения подобного анализа авторами предлагается использовать портативный инфракрасный микроспектрометр, подключенный к сети связи общего пользования, что обеспечивает возможность передачи результатов анализа по назначению или проведение удаленного анализа по запросу, но и возможность удаленной обработки и хранения данных анализа с использованием облачных технологий и Edge Computing.

микроспектрометр, молекулярный анализ, инфракрасная спектроскопия, сети связи общего пользования, e-health, Cloud Computing, Edge Computing.

Электронное здоровье (*e-health*) сегодня во всем мире является одной из наиболее важных и, динамично развивающихся, областей на стыке медицины, вычислительной техники и телекоммуникационных технологий [1, 2]. Сегодня осуществляется коренной перелом – переход от использования носимой портативной e-health электроники отдельными «продвинутыми» пользователями к системной цифровизации области здравоохранения и регулярному использованию устройств e-health медицинскими работниками в своей профессиональной деятельности [3].

Данные процессы подкрепляются с одной стороны общемировыми трендами, такими как повсеместная цифровизация и информатизация, использование облачных сервисов, ведение здорового образа жизни и т. д.,

а с другой стороны – техническими инновационными предложениями, которые выдвигает международное научное сообщество, в том числе и в области e-health. В качестве примера можно рассмотреть новые неинвазивные методы анализа крови [4, 5], а также методы анализа лекарственных препаратов [6], которые основаны на применении инфракрасной спектроскопии. Эти методы призваны ускорить и упростить процесс проведения анализа, заменив традиционные лабораторные исследования. Однако до недавнего времени не существовало устройств, технические характеристики которых позволяли бы применять методы инфракрасной спектроскопии в «полевых» условиях. К счастью, в настоящее время появился ряд портативных носимых устройств, которые позволят осуществить подобный анализ [7, 8, 9].

Настоящие устройства позиционируются производителями как персональные носимые инфракрасные микроспектрометры общего назначения, которые предназначены, в основном, для анализа состава продуктов питания. Однако производители не исключают и применение в области анализа лекарственных средств.

Рассмотрим подробнее схему взаимодействия (рис.) при анализе лекарственных средств или при проведении исследований (анализ крови и т. д.).

Рис. Схема взаимодействия

Врач с помощью спектрометра проводит исследование вещества. Первичные данные передаются на планшет в специализированное приложение, в котором отображаются персональные данные пациента и другая необходимая информация. С целью повышения качества обслуживания приложение на планшете должно иметь возможность предварительного анализа полученных данных с целью отсечения явных ошибок сканирования и т. д. В случае если сканирование выполнено успешно, врач отправляет данные через специальный гетерогенный шлюз, расположенный в карете скорой помощи. Этот шлюз должен обеспечивать конвертацию данных в формат, пригодный для дальнейшей передачи с максимальным доступным качеством обслуживания (что актуально, например, в местности, где затруднен доступ в сеть Интернет) [10].

Такой гетерогенный шлюз также может обеспечить самостоятельную обработку данных (без передачи их в медицинское учреждение), а также может выступать как граничный шлюз (*Edge Gateway*), обеспечивая несложную обработку данных при высокой нагрузке в случае повышенной интенсивности поступления данных (например, в случае эпидемий) [11, 12, 13].

Далее, с помощью сети Интернет происходит передача данных в медицинское учреждение, где происходит их накопление, хранение и систематизация. Данные могут быть переданы на дополнительную обработку для выявления корреляционных зависимостей. Результат вместе с рекомендациями передается пациенту для ознакомления.

Рассмотренная схема взаимодействия может быть использована для моделирования или экспериментов в ходе дальнейших исследований.

Исследование выполнено при финансовой поддержке РФФИ в рамках научного проекта № 19-37-90140.

Список используемых источников

1. Ахмед А. А., Блинников М. А., Пирмагомедов Р. Я., Глушаков Р. И., Кучерявый А. Е. Обзор современного состояния e-health // Информационные технологии и телекоммуникации. 2017. Т. 5, № 3. С. 1–13.

2. Кучерявый А. Е., Бородин А. С., Киричек Р. В. Сети связи 2030 // Электросвязь. 2018. № 11. С. 52–56.

3. Смышляев А. В., Мельников Ю. Ю., Садовская М. А. Распространение интернета и электронных технологий среди медицинских организаций, оказывающих первичную медико-санитарную помощь в российской федерации // Главный врач юга России. 2020. № 1. С. 7–11.

4. Manurung B. E., Munggaran H. R., Ramadhan G. F., Koesoema A. P. Non-Invasive Blood Glucose Monitoring using Near-Infrared Spectroscopy based on Internet of Things using Machine Learning // 2019 IEEE R10 Humanitarian Technology Conference, pp. 2524–2527, March 2020.

5. Лыкина А. А., Черепанов К. В., Артемьев Д. Н., Смолянская О. А. Исследование альбумина человеческого методом ИК Фурье спектроскопии // Сборник трудов XI международной конференции «Фундаментальные проблемы оптики – 2019» / Под ред. С. А. Козлова, 2019. С. 387–388.

6. Baik K.-J., Lee J. H., Kim Y., Jang B.-J. Pharmaceutical tablet classification using a portable spectrometer with combinations of visible and near-infrared spectra // 2017 Ninth International Conference on Ubiquitous and Future Networks (ICUFN), pp. 1011–1014, July 2017.

7. SCiO – The World's First Pocket Sized Molecular Sensor [Электронный ресурс] // Consumer Physics, 2020. URL: https://www.consumerphysics.com (дата обращения 03.05.2020).

8. Tellspec scanner [Электронный ресурс] // Tellspec Inc, 2020. URL: https://www.tellspec.com (дата обращения 03.05.2020).

9. LinkSquare [Электронный ресурс] // Stratio Inc., 2020. URL: https://linksquare.io (дата обращени: 03.05.2020).

10. Kulik, V., Kirichek R. The heterogeneous gateways in the Industrial Internet of Things // 2018 10th International congress on ultra modern telecommunications and control systems and workshops (ICUMT). 2018. PP. 210–215.

11. Атея А. А., Выборнова А. И., Кучерявый А. Е. Многоуровневая облачная архитектура для услуг Тактильного Интернета // Электросвязь. 2017. № 2. С. 26–30.

12. Recommendation ITU-T Q.5001 (2018), Signalling requirements and architecture of intelligent edge computing.

13. Pham V. D., Hoang T., Kirichek R., Makolkina M., Koucheryavy A. Minimizing the IoT System Delay with the Edge Gateways // In: Vishnevskiy V., Samouylov K., Kozyrev D. (eds) Distributed Computer and Communication Networks. DCCN 2019. Lecture Notes in Computer Science, vol. 11965. Springer, Cham.

УДК 654.027.1
ГРНТИ 49.33.29

РАЗРАБОТКА МЕТОДОВ ДИСТАНЦИОННОГО ТЕСТИРОВАНИЯ ПАРАМЕТРОВ СЕТИ НА БАЗЕ РЕКОМЕНДАЦИИ Q.3056 МСЭ-Т С ИСПОЛЬЗОВАНИЕМ ПРОГРАММНЫХ ЗОНДОВ

В. В. Зеленов[1,2], Р. В. Киричек[1], Н. И. Шустов[1,3]

[1]Санкт-Петербургский государственный университет телекоммуникаций им. проф. М. А. Бонч-Бруевича
[2]ООО «НТЦ АРГУС»
[3]ООО «НТЦ СевенТест»

Постоянный рост числа пользователей сети интернет создает всё большую нагрузку на сетевое оборудование операторов, предоставляющих услуги доступа, что впоследствии влечёт за собой снижение показателей качества обслуживания.

Это может повлиять на качество доступа к сети у определенных пользователей или организаций, которые пользуются этой услугой. В настоящий момент не существует стандартизованного метода измерения таких показателей. В связи с этим, целесообразно реализовать метод дистанционного тестирования параметров сети на базе рекомендации Q.3056 МСЭ-Т с использованием программных зондов, что позволит в режиме реального времени постоянно собирать и хранить информацию о показателях качества обслуживания сети.

качество обслуживания, QoS, тестирование сети оператора, Рекомендация Q.3056 МСЭ-Т, клиент-сервер.

Большинство операторов имеют частные технические решения для оценки эффективности своих сетей, и пользователи не имеют альтернативных средств для обоснования любых претензий относительно надлежащего обеспечения услуг доступа к сети интернет.

Решение этой проблемы включает в себя создание алгоритма/протокола, который может быть использован зондами, измерения которых могут являться доверенными для всех заинтересованных сторон. Использование такого доверенного протокола исключит возможность влияния внутренних сервисов оператора на результаты системы мониторинга и, таким образом, обеспечить пользователям достоверность данных о технических характеристиках предоставляемых услуг.

Система дистанционного тестирования параметров сетевого и коммуникационного обслуживания – распределенный программно-аппаратный комплекс для тестирования параметров сетевого и коммуникационного обслуживания. Система дистанционного тестирования параметров сетевого и коммуникационного обслуживания имеет клиент-серверную архитектуру и включает в себя описанные далее элементы [1].

Одним из таких элементов является зонд. Зонд – клиентская система мониторинга качества услуг связи, включающая в себя следующие подсистемы:

1. Узел тестирования приложения (SMP).
2. Интерфейс взаимодействия узла тестирования приложения (SMP CI).

Другим элементом является сервер для удаленного тестирования параметров сетевого и коммуникационного обслуживания (RTNP *Server*). Сервер состоит из следующих подсистем:

1. Подсистема мониторинга (MCS).
2. Система сбора, анализа и вывода данных (DCAOS).
3. База данных тестов (MDB).
4. База данных узлов (PDB).

Архитектура системы проиллюстрирована на рис. 1.

Зонд – отдельный элемент системы дистанционного тестирования параметров сетевого и коммуникационного сервиса, включающий программно-аппаратное устройство с функциями тестового узла приложения и взаимодействия с узловой тестирования приложения. Зонд является отдельным элементом системы RTNP [2]. Это может быть реализовано в виде аппаратного и/или программного обеспечения.

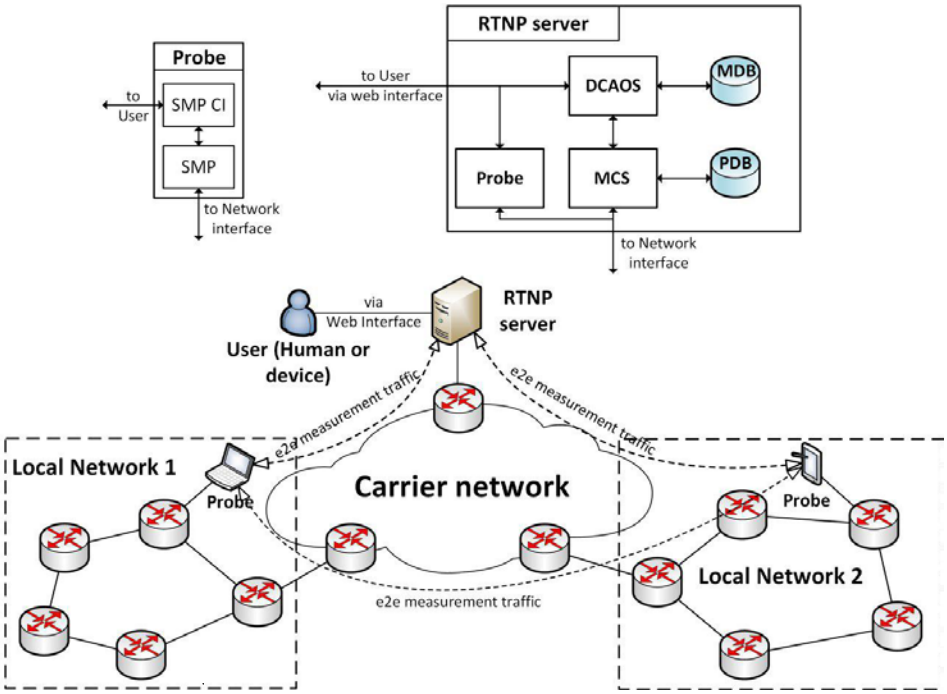


Рис. 1. Архитектура системы дистанционного тестирования параметров сетевого и коммуникационного обслуживания

Тестовый узел приложения (SMP) – программное обеспечение, работающее в фоновом режиме, реализующее сценарии тестирования, использующее тестовые конфигурации, полученные из подсистемы мониторинга. Этот узел проводит сбор, сохранение и передачу измерений и формирует на основе полученных тестовых конфигураций транспортные потоки с использованием выбранного протокола уровней 3–7 в соответствии с моделью OSI [3].

SMP выполняет следующие функции:

1. Принимает и передает информацию от/в SMP CI.

2. Реализация тестовых сценариев в соответствии с тестовыми конфигурациями, полученными от SMP CI.

3. Генерирует транспортные потоки на основе тестовых конфигураций, полученных от SMP CI.

SMP CI – приложение, выполняющее функцию взаимодействия с тестовым узлом приложения. Это может быть графический интерфейс, кон-

сольный интерфейс, сетевой интерфейс или интерфейс приложения. Приложение может выполнять функции одного из вышеупомянутых интерфейсов или нескольких одновременно, в зависимости от задачи.

SMP CI выполняет следующие функции:

1. Прием и передача информации от/к SMP.

2. Ввод и вывод начальной конфигурации SMP (адрес сервера, порт, тип аппаратной платформы, PUID).

3. Выбор, начальной конфигурации и запуск тестового сценария.

4. Ввод и вывод текущей тестовой конфигурации (сценарии тестирования, PUID, IP-адрес, порт SMP, MUID).

5. Отправка промежуточных и окончательных результатов тестов.

6. Обновление программного обеспечения зонда.

Сервер системы дистанционного тестирования должен управлять выполнением сеансов тестирования. Функциональность сервера образуется из подсистем следующим образом.

Подсистема мониторинга – это серверная программа, которая отслеживает реализацию сценариев тестирования. Она выполняет следующие функции:

1. Регистрация зондов в системе, выделение уникального идентификационного номера узла (PUID).

2. Генерация тестовых конфигураций для зондов, включая уникальный идентификационный номер теста (MUID).

3. Получение тестовых конфигураций от зондов их уникальных тестовых идентификационных номеров (MUID).

4. Повторное получение и передача тестовых конфигураций от/к зондам.

5. Получение и передача промежуточной и окончательной тестовой информации от/к зондам.

6. Взаимодействие с системой сбора данных, анализа и вывода данных.

7. Запись и чтение данных о зондах из базы данных узла с помощью PUID.

8. Постоянный мониторинг показателей качества обслуживания (QoS) для зондов, зарегистрированных в базе данных узлов.

Подсистема сбора, анализа и вывода данных – подсистема серверной программы, осуществляющая сбор, анализ и вывод данных, полученных в результате реализации данного сценария тестирования. Она выполняет следующие функции:

1. Взаимодействие с подсистемой мониторинга.

2. Ввод и выход информации о завершенных тестах.

3. Анализ информации, полученной по завершенным тестам.

4. Вывод полезной информации о завершенных тестах для пользователя, с помощью веб-интерфейса.

5. Запись и чтение информации о тестах из базы данных тестов с использованием MUID.

База данных тестов – подсистема серверного ПО, осуществляющая запись, чтение и хранение данных о завершенных тестах с помощью MUID.

База данных узлов – подсистема серверного ПО, осуществляющая запись, чтение и хранение данных, касающихся зарегистрированных зондов на сервере RTNP, используя PUID.

Далее, описан процесс тестирования. Общая логика процедуры тестирования представлена на рис. 2.

Дистанционное тестирование опирается на распределенную систему проверенных зондов. Каждый зонд включает встроенный аппаратный уникальный идентификатор. Идентификатор является устойчивым к фальсификации программными методами.

Точки тестирования готовы после установки зондов. Сервер RTNP обеспечивает аутентификацию и авторизацию зондов для тестирования. Перед запуском теста сервер RTNP может проверить, готовы ли все тестовые компоненты, участвующие в тесте.

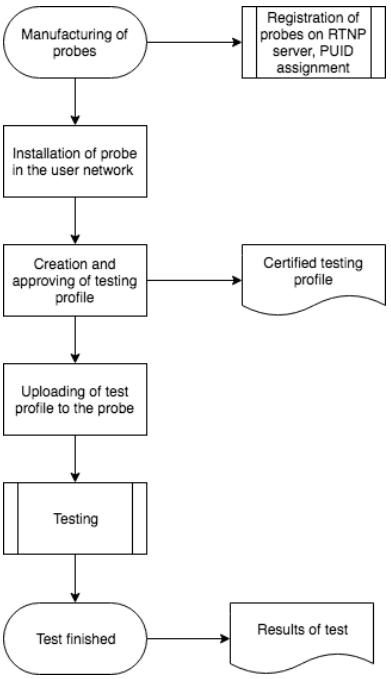


Рис. 2. Общая логика тестирования с использованием зондов

Конкретные подходы, используемые сервером RTNP для проверки подлинности и авторизации зондов, не входят в область настоящей Рекомендации.

Процесс тестирования может включать активный и/или пассивный режим зондов. В пассивном режиме зонды измеряют параметры производительности сети с заранее установленной скоростью. В этом режиме процесс тестирования не оказывает существенного влияния на текущие операции в замедленной сети. В активном режиме зонды имитируют трафик определенного приложения, что может повлиять на работу, характерную для сети, или даже прервать текущие процессы [4, 5].

В конце теста результаты доступны на сервере RTNP. Результаты хранятся в соответствии с политикой, принятой пользователем, и доступны через веб-интерфейс на сервере RTNP.

Подводя итог, в данной работе рассмотрена Рекомендация Q.3056 МСЭ-Т, позволяющая реализовать методы дистанционного тестирования параметров сети оператора с использованием программных зондов. В дальнейшем будет представлена система измерения параметров сети на основе данной Рекомендации.

Список используемых источников

1. Recommendation Q.3059 ITU-T. Signalling procedures of the probes to be used for remote testing of network parameters: International Telecommunication Union – Telecommunication Standardization Sector, 2017. 11 p.

2. Гольдштейн Б. С., Соколов Н. А., Яновский Г. Г. Сети связи : учебник. СПб. : БХВ-Петербург, 2014. 401 с. ISBN 978-5-9775-2798-9.

3. Recommendation Q.3960 ITU-T. Framework of Internet related performance measurements: International Telecommunication Union – Telecommunication Standardization Sector, 2016. 20 p.

4. Кожанов Ю. Ф. Качество обслуживания в сетях связи. СПб. : СПбГУТ, 2014. 160 с.

5. Олифер В., Олифер Н. Компьютерные сети. Принципы, технологии, протоколы : учебник для вузов. 5-е изд. СПб. : Питер, 2016. 992 с.: ил. ISBN 978-5-496-01967-5.

УДК 654.027.1
ГРНТИ 49.33.29

РАЗРАБОТКА МЕТОДОВ ИЗМЕРЕНИЯ СКОРОСТИ ИНТЕРНЕТ В СЕТЯХ ФИКСИРОВАННОЙ И МОБИЛЬНОЙ СВЯЗИ НА БАЗЕ РЕКОМЕНДАЦИИ Q.3961 МСЭ-Т

В. В. Зеленов[1,2], Р. В. Киричек[1], Н. И. Шустов[1,3]

[1]Санкт-Петербургский государственный университет телекоммуникаций им. проф. М. А. Бонч-Бруевича
[2]ООО «НТЦ АРГУС»
[3]ООО «НТЦ СевенТест»

На сегодняшний день работа множества организаций напрямую зависит от качества интернет-соединения. Использование метода измерения скорости сети интернет на базе Рекомендации Q.3961 МСЭ-Т позволит контролировать качество предоставляемых услуг. Существуют решения для измерения пропускной способности интернет-соединения, такие как Speedtest, 2ip, Fast, но они не основаны на стандарте или рекомендации. Следовательно, измерения данных систем нельзя считать доверенными. Таким образом, чтобы контролировать качество интернет-соединения при помощи доверенного источника, необходим доверенный метод, который рассмотрен в данной статье.

пропускная способность, качество сети, Рекомендация МСЭ-Т.

Каждый день растет количество пользователей сети интернет, что напрямую влияет на качество предоставляемых услуг, т. к. чем больше

пользователей, тем больше требуется ресурсов для предоставления этих услуг и поддержания качества обслуживания сети.

На данный момент не существует единого стандарта измерения скорости в Сети Связи Общего Пользования. Вследствие чего, невозможно определить, что качество предоставляемых услуг [1, 2, 3], а именно, скорость доступа к сети интернет, соответствует заявленному. Из-за этого растет количество случаев мошенничества, а также это приводит к проблемам, связанным с качеством сети у отдельных организаций, использующих услуги таких операторов связи.

Существуют общедоступные методы для измерения скорости интернет, но они не являются гарантом качества, так как они не основаны на общепринятом стандарте.

Таким образом, возникает актуальная задача сократить случаи мошенничества, а также предоставить возможность измерения скорости сети интернет при помощи доверенного метода на основе принятой рекомендации.

Данный метод, представленный на рис. 1, предназначен для точного измерения максимальной пропускной способности [3], которую может предоставить данное интернет-соединение. Точность достигается при помощи отправки данных по нескольким параллельным потокам с использованием отдельных соединений TCP [4] в течение предопределенного периода времени. Передаваемые данные в потоках генерируются с высокой степенью случайности. В этом методе используемый псевдогенератор случайных чисел может не соответствовать криптографическим требованиям, однако при этом он не должен сжимать данные во время передачи. Для того, чтобы увеличить вероятность того, что тест может быть выполнен даже в сетях, защищенных брандмауэрами и прокси-серверами, данные должны быть переданы через HTTP или HTTPS (TLS или SSL) [5].

Рис. 1. Метод измерения скорости сети интернет на базе Рекомендации Q.3961 МСЭ-Т

Далее рассмотрим архитектуру данного метода.

Controller FE – это функциональный элемент, предназначенный для контроля механизмов тестирования на определенном терминальном оборудовании (*Measurement Agent*). Контроллер отвечает за определение тестовых скриптов и инициирование их на данном терминальном оборудовании. Процесс определения тестовых скриптов может потребовать от Collector FE получения существующих данных.

Кроме того, Controller FE предоставляет пользователю среду измерения и инструменты для выполнения теста на веб-странице HTTP/s. Он принимает и выполняет необходимые скрипты, которые будут использоваться во время теста. Кроме того, он предоставит пользователям интерфейс, чтобы получить доступ к измеренным результатам.

В случае применения на измерительном агенте доступ к web-интерфейсу может быть предоставлен по различным каналам.

Collector FE – это функциональный элемент, предназначенный для сбора, обработки и хранения результатов измерений и других статистических данных, полученных от агентов измерений, подключенных к Controller FE.

Агент измерения (MA) – это функциональный элемент, который имеет функциональность для выполнения тестовых скриптов, которые определены в Controller FE, и для получения результатов тестов и загрузки соответствующих данных в Collector FE.

Агент измерения имеет две различные конфигурации:

Вариант 1) включает в себя терминальное оборудование (компьютер, смартфон, планшет и т. д.), которое контролируется физически и, как правило, принадлежит пользователю:

– Это терминальное оборудование должно иметь активное подключение к сети Интернет и веб-браузеру для того, чтобы получить доступ к вебсайту, размещенному на контроллере, или иметь предустановленное приложение для доступа к тестам в случае портативного устройства.

– Терминальное оборудование должно быть также способно обеспечивать связь с коллектором для передачи результатов и других статистических данных.

Вариант 2) включает в себя терминальное оборудование и наличие агента измерения в виде промежуточного (зонд) или дополнительного оборудования, интегрированного в терминальное оборудование.

6.2.4. Пир измерений FE – это функциональный элемент, который способен отвечать на сообщения от тестов, отправленные из агента измерений, и имеет возможность собирать данные измерений, которые будут загружены в Collector FE. Кроме того, он также предоставляет возможность мониторинга используемых ресурсов, чтобы Controller FE мог запланировать

тесты таким образом, чтобы предотвратить любые прогнозируемые помехи, влияющие на результаты тестов.

Рабочий процесс/выполнение/реализация/процедура системы тестирования показана на рис. 2.

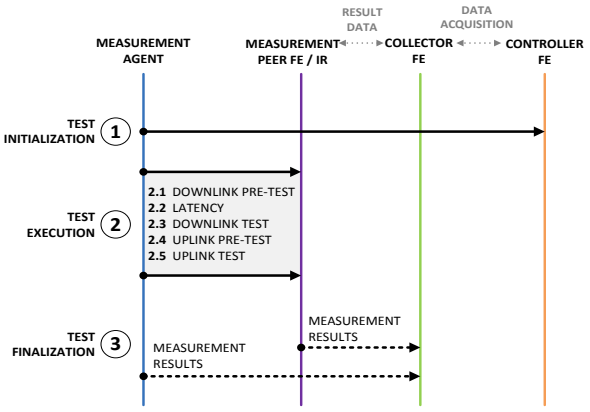


Рис. 2. Рабочий процесс системы тестирования

Процедуры, описанные ниже, действительны только для TCP.

Далее определены основные этапы процедуры тестирования, как только агент по измерению получил тестовый код от Controller FE, а также местоположение или расположение узлов измерения.

Пир измерений (MP) выбирается в контроллере в зависимости от местоположения агента измерений (MA). Также при измерении скорости интернет есть возможность выбора пира по умолчанию или одного из доступных пиров.

Тест состоит из семи фаз, которые выполняются одна за другой, то есть фаза m начинается после завершения фазы $m-1$ без какой-либо паузы между ними. Это означает, что фазы не пересекаются.

Чтобы обеспечить сопоставимые условия тестирования скорости передачи данных в мобильных сетях, следует инициировать предварительную загрузку [6].

Если процедуры предварительного тестирования загрузки и отдачи не реализованы (фазы 2 и 5), то агент измерения (терминальное оборудование) должен открыть соединение TCP на загрузку и отдачу. Для теста загрузки контроллер отправляет блок данных размера N, для теста отдачи агент измерения отправляет блок данных того же размера.

Методология тестирования определяет набор переменных и констант, которые должны быть назначены до выполнения алгоритма тестирования или во время выполнения теста. Некоторые из этих значений открыты для выбора в пределах диапазона, в соответствии с конкретными соображениями каждой реализации или текущих сетевых условий на момент выполнения теста.

Значения, перечисленные в таблице (см. ниже), действительны только для TCP.

Фазы тестирования:

1. Инициализация.
2. Предварительный тест скорости загрузки.

3. Тест на задержку.
4. Тест скорости загрузки.
5. Предварительное тестирование скорости отдачи (необязательно).
6. Тест скорости отдачи.
7. Завершение.

ТАБЛИЦА. Используемые параметры измерений

	Параметр	Единица измерения	Интервал	Значение по умолчанию
n	Количество параллельных соединений	№	$1 \le n \le 10$	$n = 3$
Tp	Длительность предварительного теста	с	$0 \le Tp \le 5$	$Tp = 2$
Td	Длительность предварительного теста загрузки	с	$5 \le Td \le 15$	$Td = 7$
Tu	Длительность предварительного теста отдачи	с	$5 \le Tu \le 15$	$Td = 7$
To	Таймаут	с	$5 \le To \le 10$	$To = 5$
p	Количество сигналов ‘ping’ в течение предварительного теста задержки	№	$5 \le p \le 20$	$p = 10$
T_l	Максимальное пройденное время до отправки первого сигнала ‘ping’	мс	$200 \le T_l \le 1000$	$Tl = 500$
z	Размер блока данных (размер куска)	КБ	Минимум 1 КБ	$z = 4$

Предполагается, что узлы обмениваются информацией с устройством управления тестированием через протокол HTTP, в формате представления данных JSON.

Когда узел зарегистрирован на тестовом устройстве, каждый узел отправляет следующую информацию:

– тип сообщения (*setup*);
– пропускная способность канала записи для пира измерения;
– пропускная способность канала чтения для пира измерения;
– адрес пира измерения;
– порт пира измерения.

После регистрации узла механизм управления тестированием возвращает узлам следующую информацию:

– тип сообщения (*setupACK*);
– адрес пира измерения;
– порт пира измерения;
– UID пира измерения.

Когда тест инициализирован, следующая информация отправляется на тестовый сервер из источника пира измерения:

– тип теста;
– тип сообщения;
– тайм-аут;
– продолжительность теста;
– пропускная способность канала записи для пира измерения;
– пропускная способность канала чтения для пира измерения;
– количество потоков;
– количество пакетов – для отложенных тестов или в качестве альтернативы параметру «продолжительность теста» (необязательно);
– размер тела тестового сообщения – для теста скорости отдачи и загрузки (необязательно);
– использованное шифрование: HTTPS через SSL/TLS, HTTP (без шифрования);
– метод шифрования/расшифровки: RSA. NTRUEncrypt и др.;
– адрес пира назначения;
– порт пира sназначения.

Таким образом, в данной работе рассмотрена архитектура метода измерения скорости на базе рекомендации Q.3961 МСЭ-Т. Показана возможность реализации данного метода. В дальнейшем планируется реализация данного метода в рамках стенда.

Список используемых источников

1. Recommendation Q.3961 ITU-T. Testing methodologies of Internet related performance measurements including e2e bit rate within the fixed and mobile operator’s networks: International Telecommunication Union – Telecommunication Standardization Sector, 2017. 23 p.

2. Kulik V., Muthanna A., Pham V. D., Hakimov A., Kirichek R., Pirmagomedov R. The study of semantic gateway performance // Электросвязь. 2017. № 6. С. 69–73.

3. Кучеряевый А. Е., Кучеряевый Е. А., Харью Я. Качество обслуживания в сети Интернет // Электросвязь. 2002. № 1. С. 9–14.

4. Таненбаум Э., Уэзеролл. Д. Компьютерные сети, 5-е изд. СПб. : Питер, 2012. 384 с.

5. Гольдштейн Б. С., Кучерявый А. Е. Сети связи пост-NGN. СПб. : БХВ-Петербург, 2013. 160 с. ISBN 978-5-9775-0900-8.

6. Вегешна Ш. Качество обслуживания в сетях IP. М. : Вильямс, 2003. 368 с.

УДК 004.056
ГРНТИ 19.31

РАЗРАБОТКА МЕТОДИКИ ПРОВЕДЕНИЯ ИСПЫТАНИЙ IPS МОДУЛЕЙ

И. П. Зуев, П. В. Карельский, М. М. Ковцур, Д. В. Юркин

Санкт-Петербургский государственный университет телекоммуникаций им. проф. М. А. Бонч-Бруевича

Защита конфиденциальной информации и технологических процессов ее обработки в локальной вычислительной сети – приоритетная задача любой организации, попадающей под федеральное регулирование. Одним из распространенных методов обеспечения управления информационными потоками при взаимодействии с сетями общего пользования, в том числе и с сетью Интернет, является установка на границе локальной вычислительной сети межсетевого экрана. Однако современные подходы к обеспечению безопасности межсетевого взаимодействия требуют совместной с межсетевыми экранами установки средств обнаружения и предотвращения вторжений (IPS систем). Работа посвящена обзору IPS систем, разработке тестового стенда для проведения испытаний и его проверки посредством тестирования одного из решений по обнаружению и предотвращению вторжений.

СПВ, СОПВ, IPS, корпоративная сеть, предотвращение вторжений, защита периметра сети.

Установка и использование систем межсетевого экранирования на границе контролируемых зон локальной вычислительной сети (ЛВС) различных организаций – неотъемлемая часть обеспечения безопасности сети и внутренних корпоративных ресурсов, будь то терминальные фермы, центры обработки данных, или пользователи автоматизированных рабочих мест (АРМ). Однако обеспечить простой запрет прохождения как межсетевого трафика внутренних сегментов сети, так и информационного обмена с сетью Интернет, в сегодняшних реалиях оказывается недостаточным. Хакерские атаки уже не являются чем-то необычным и выходящим за грань фантастики, данные инциденты приобрели повсеместный характер и пользуются небывалой популярностью среди нарушителей периметра контролируемой зоны. Только за февраль 2020 года было зафиксировано около 4 млн сетевых атак на каждый день месяца [1, 2]. Отсюда следует, что для обеспечения безопасности ЛВС, защиты конфиденциальной информации и технологических процессов организации необходимо применение дополнительных мер защиты. Одной из таких мер является использование систем обнаружения и предотвращения вторжений – IPS систем.

Система обнаружения и предотвращения вторжений – система, позволяющая в реальном времени определять атаки на подконтрольную систему,

предотвращать их, и вести статистику для последующего анализа администраторами информационной безопасности (ИБ). Такие системы можно считать эволюцией систем обнаружения вторжений (IDS систем), которые позволяли только определять атаки и сигнализировать о них администраторам, которым, в свою очередь, приходилось самостоятельно предпринимать меры по предотвращению инцидентов ИБ.

IPS модули подразделяются на две категории – хостовые (или их еще называют узловыми) и сетевые. Хостовые IPS модули предназначены для анализа трафика, контроля сетевой активности в пределах АРМ пользователя. Такие системы являются программными комплексами и устанавливаются непосредственно на АРМ. Сетевые системы предназначены для анализа трафика, выявления угроз и их предотвращения, направленного в контролируемую зону, т. е. защищаемую ЛВС организации. Такие IPS могут быть только программными решениями или программно-аппаратными комплексами, представляющими из себя отдельные сетевые устройства на ряду с межсетевыми экранами, прокси-серверами и т. п. Наиболее популярными на сегодняшний день решениями являются именно программные варианты IPS систем, поскольку такой вариант позволяет приобрести межсетевой экран типа Next Generation Firewall (сокр. NGFW), реализующий одновременно межсетевое экранирование и, анализ и предотвращение инцидентов ИБ. Сетевые системы предотвращения вторжений устанавливаются в, так называемом, «Inline» режиме, т. е. в разрыв сети. Данный метод развертывания позволяет IPS пропускать весь трафик непосредственно через себя и, в отличие от систем IDS, снять дополнительную нагрузку с других сетевых устройств, поскольку задача обеспечения зеркалирования трафика отпадает.

Среди IPS систем есть модули с открытым исходным кодом. Наиболее востребованными можно выделить IPS системы Snort и Suricata. Среди коммерческих предложений для корпоративного использования представлены следующие варианты: Cisco Firepower, Check Point NGFW с программным модулем IPS Software Blade, FortiGate IPS от компании FortiNet. Среди отечественных продуктов и вендоров стоит упомянуть АПКШ (аппаратно-программный криптошлюз) Континент от компании Код Безопасности, а также ViPNet xFirewall от компании Infotecs.

В соответствии с приказами № 17 [3] и № 21 [4] ФСТЭК России, при эксплуатации средств защиты информации, в том числе и IPS модулей, на объектах информатизации необходимо осуществлять регулярный контроль эффективности применения систем защиты. Поэтому перед ответственной за эксплуатацию IPS систем организацией встает актуальный вопрос проведения испытаний и анализа защищенности средств защиты информации, что делает необходимым разработку и проведение различных

видов тестирования, включающих в себя проверку функций систем и проведение анализа уязвимостей.

Для разработки методики тестирования IPS модулей, а впоследствии и проведения самого тестирования, возникает необходимость в развертывании инфраструктуры, которая в целом будет отражать стандартную корпоративную сеть с присущими ей ресурсами типа корпоративной почты, контроллера домена, внутреннего центра сертификации и т. п. В соответствии с этими требованиями было виртуально развернуто подобие корпоративной сети, представленное на рис.

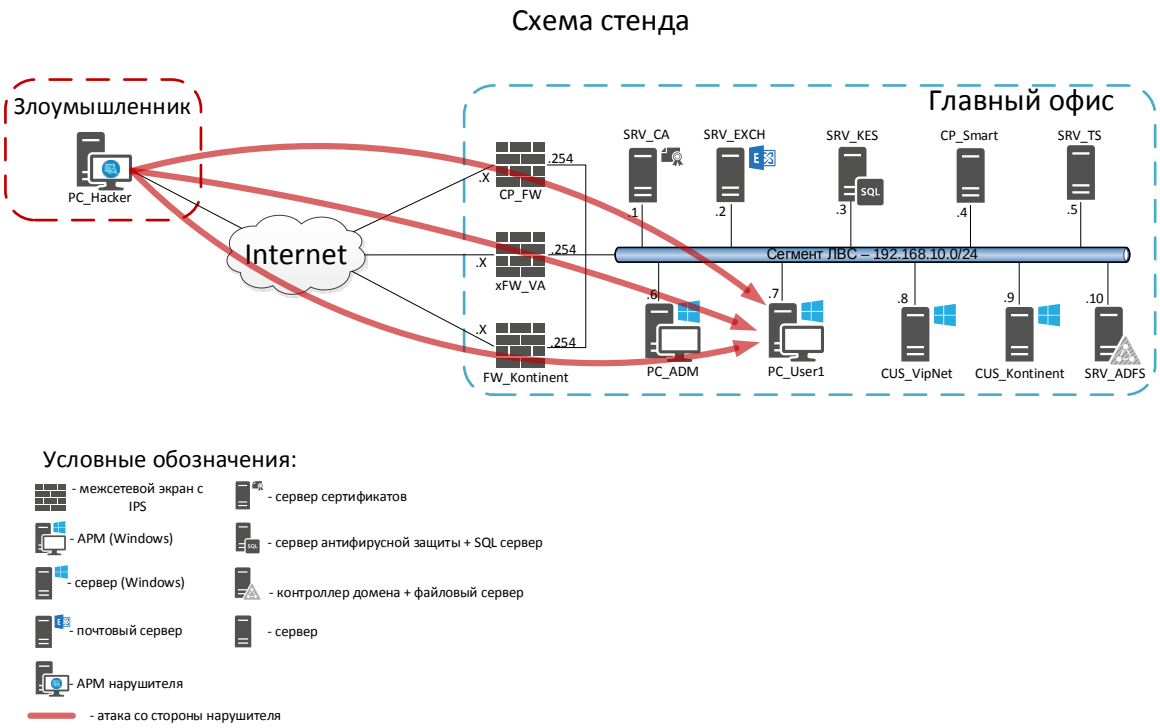


Рис. Схема тестового стенда

На границе ЛВС расположен межсетевой экран со встроенным модулем IPS защиты. Для тестирования был взят передовой продукт зарубежного производства – Check Point NGFW, а также два отечественных решения – АПКШ Континент и ViPNet xFirewall. Проверка именно этих продуктов соответствует требованиям, выдвинутыми заказчиком по возможности максимального использования отечественных разработок при организации защиты корпоративной ЛВС. Для воспроизведения действий возможного злоумышленника развернута виртуальная машина с ОС Kali Linux, что позволяет использовать широкий диапазон ПО, предназначенного для обнаружения уязвимостей корпоративной инфраструктуры и их использования.

Для проверки работоспособности тестового стенда было проведено предварительное тестирование межсетевого экрана Check Point с программ-

ным модулем IPS Software Blade. Для обнаружения уязвимостей и их эксплуатации использовалось ПО «metasploit». Было произведено сканирование открытых портов с определением ОС целевой машины (АРМ с предустановленной ОС Windows 7), после чего были произведены попытки эксплуатации найденных уязвимостей цели [5]. Следует отметить, что, поскольку речь идет о тестировании конкретно IPS модуля, использованного в составе представленного межсетевого экрана, то правила межсетевого экранирования описаны как «permit any any», т. е. разрешен весь трафик с включенным логированием по каждой попытке установления соединений или передаче трафика. В настройках IPS модуля использован профиль типа «Блокировать все», что значит предотвращение всех вторжений, найденных в процессе анализа трафика. Каждая попытка вторжения также подвержена логированию для упрощения последующего анализа работы модуля предотвращения вторжений.

В таблице представлены результаты предварительного тестирования. Стоит отметить следующее – каждая атака или вид сканирования, использующиеся в ПО «metasploit», генерирует *n* количество событий. Например, запуская сканирование открытых портов целевой системы, происходит перебор определенного количества портов, что в свою очередь приводит к *n* числу событий в соответствии с *n* количеством портов. На каждое событие идет реакция со стороны IPS модуля, т.е. на *n* число событий приходится *k* срабатываний. Каждое срабатывание сопровождается определенным действием со стороны IPS модуля [6].

ТАБЛИЦА. Результаты предварительного тестирования IPS модуля Check Point

Вид атаки	Кол-во событий в атаке	Кол-во срабатываний	Действие
msf scan	238	239	alert
dcerpc attack	1	1	blocked
Oracle	1	1	blocked
ipas_pipe	1	1	blocked
ms08_netapi	1	1	blocked
ms10_spoolss	1	1	blocked
timbuktu	1	1	blocked
https inspection	1	1	blocked
documents scanning	1	1	blocked

Работа IPS модуля характеризовалась профилем «Блокировать все», где определено предотвращение всех атак, направленных на внутреннюю

подконтрольную сеть. Поэтому каждое событие, генерируемое атакой злоумышленника, сопровождается действием «blocked». Также из таблицы видно, что при сканировании открытых портов количество срабатываний не соответствует числу событий в атаке – $k > n$. Данная «аномалия» объясняется тем, что в логах работы межсетевого экрана были зафиксированы все попытки сканирования по определенным портам, а также было выведено общее сообщение о том, что на систему ведется атака типа «сканирование портов».

Таким образом, сохраняется задача разработки методики тестирования в соответствии с корпоративными требованиями заказчика, выставляемыми к защите периметра контролируемой ЛВС, провести тестирование требуемых межсетевых экранов отечественной и зарубежной разработки, а также, по результатам тестирования, разработать математическую модель IPS модулей.

Список используемых источников

1. Интерактивная карта киберугроз [Электронный ресурс]. URL: https://cybermap.kaspersky.com/ru/stats/#country=213&type=ids&period=m (дата обращения 17.03.2020).

2. Ушаков И. А. Обнаружение инсайдеров в корпоративной компьютерной сети на основе технологий анализа больших данных // Вестник Санкт-Петербургского государственного университета технологии и дизайна. Серия 1: естественные и технические науки. 2019. № 4. С. 38–43.

3. Приказ от 11.02.2013 №17 ФСТЭК России «Об утверждении Требований о защите информации, не составляющей государственную тайну, содержащейся в государственных информационных системах» [Электронный ресурс]. URL: https://fstec.ru/component/attachments/download/566 (дата обращения 17.03.2020).

4. Приказ от 18.02.2013 № 21 ФСТЭК России «Об утверждении Состава и содержания организационных и технических мер по обеспечению безопасности персональных данных при их обработке в информационных системах персональных данных» [Электронный ресурс]. URL: https://fstec.ru/component/attachments/download/561 (дата обращения 17.03.2020).

5. Виткова Л. А., Дудникова М. Н., Петрова А. Н. Определение вероятности нарушения критических свойств информационного актива на основе CVSS метрик уязвимостей // Актуальные проблемы инфотелекоммуникаций в науке и образовании. VII международная научно-техническая и научно-методическая конференция: сб. науч. ст. в 2-х т. СПб. : СПбГУТ, 2018. С. 152–156.

6. Сахаров Д. В., Ковцур М. М., Бахтин Д. В. Модель защиты от эксплойтов и руткитов с последующим анализом и оценкой инцидентов // Наукоемкие технологии в космических исследованиях земли. 2019. Т. 11. № 5. С. 22–31.

УДК 004.457
ГРНТИ 49.33; 20.53

ПРЕИМУЩЕСТВА И НЕДОСТАТКИ ПРИМЕНЕНИЯ PLC-ТЕХНОЛОГИЙ ДЛЯ ОРГАНИЗАЦИИ УПРАВЛЕНИЯ УЗЛОМ СВЯЗИ С ИСПОЛЬЗОВАНИЕМ АВТОМАТИЗИРОВАННОЙ СИСТЕМЫ УПРАВЛЕНИЯ УЗЛОМ СВЯЗИ

В. Г. Иванов, А. Ю. Савицкий

Военная академия связи им. Маршала Советского союза С. М. Буденного

Организации управления и несению службы дежурной сменой на узлах связи уделяет большое внимание. Для реализации этих целей на узлах связи используются большое количество разнотипных оконечных устройств. В статье анализируется применение технологий PLC в составе универсального терминального устройства служебной связи и управления «Терминала».

управление, узел связи связь, PLC.

Управление узлом связи (УС) – постоянное и целенаправленное воздействии должностных лиц на элементы (боевые посты) узла связи по всесторонней подготовке и эффективному применению сил и средств связи для выполнения поставленной задачи. [1]. В настоящее время вся работа по организации управления УС производится только ручным способом, в лучшем случае при наличии ПЭВМ могут использоваться офисные приложения. Автоматизация процессов управления и создание автоматизированных систем управления узлом связи позволит сократить время на сбор и обработку информации о состоянии узлов связи и его элементов, уменьшить усилия, затрачиваемые на техническую и расчетно-информационную работу, а также доведение задач до подчиненных с одновременным их документированием, обеспечение циркулярной или выборочной передачи важных команд и распоряжений до всех инстанций [2] Имеющиеся средства связи и автоматизации в аппаратных и станциях не позволяет их использовать для управления УС без использования дополнительного оборудования.

Для решения вопросов развертывания автоматизированной системы управления полевым узлом связи в ходе научной работы разработано универсальное терминальное устройство служебной связи «Терминал» с написанием соответствующего программного обеспечения.

В состав «Терминал» включен программно-аппаратные средства, позволяющие реализовать IP АТС и обеспечить сопряжение с ПАК автоматизации процессов управления узлом связи. Структурно «Терминал» состоит из модулей, которые размещены в одном портативном устройстве (рис. 1).

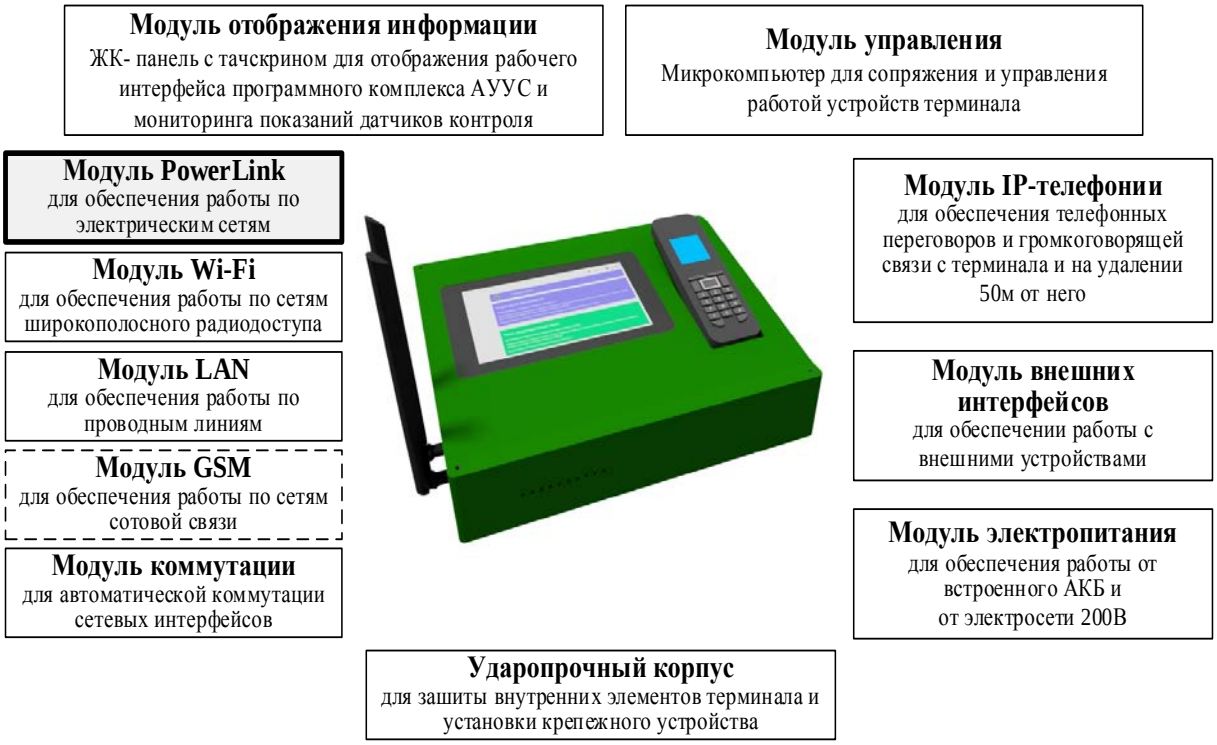


Рис. 1. Основные составляющие универсального терминального устройства служебной связи и управления «Терминала»

Универсальное терминального устройства служебной связи и управления при эксплуатации полевого узла связи пункта управления. устанавливаются и подключается к сети 220 В в каждой аппаратной. Аппаратные подключаются к сети электропитания от одной электропитающей станции.

Связь через линии электропередачи PLC (*Power Line Communication*) – термин, описывающий несколько разных систем для использования ЛЭП для передачи голосовой информации или данных [3]. Данная технология связи, позволяет отправлять данные по уже имеющимся силовым кабелям. Следовательно, при подключении только одного кабеля питания к электронному устройству можно включить его и одновременно управлять извлекать данные из него в полудуплексном режиме.

Сеть может передавать голос и данные, накладывая аналоговый сигнал поверх стандартного переменного тока частотой 50 или 60 Гц.

Можно выделить 2 класса PLC систем:

– NPL (*Narrowband over Power Lines*) узкополосная передача через ЛЭП, которая работает на более низких частотах, со значительно меньшими

скоростями передачи данных до 1 Мбит/с, имеет большую дальность (до нескольких километров), увеличивается за счет применения повторителей. NPL сейчас в основном применяется в устройствах управления уличным освещением, системах сигнализации, учета расхода и управления электроэнергии.

– BPL (*Broadband over Power Lines*) широкополосная передача через ЛЭП – работает на более высоких частотах, со скоростями передачи данных до 500 Мбит/с используется в приложениях с более коротким диапазоном. Данная технология сегодня используется для требующих высокой скорости приложений передачи данных, таких как Internet (интернет), High Definition Television (телевидение высокой четкости).

PLC похож на другие коммуникационные технологии, в которой отправитель формирует данные для отправки, которые должны быть отправлены через среду связи, а получатель извлекает данные для их чтения. Главное отличие состоит в том, что PLC не требует дополнительных кабелей, позволяет контролировать все подключенные устройства к ЛЭП, так как он повторно использует существующую проводку

В составе устройства «Терминала» применили PLC, который предназначен для автоматической организации ЛВС по технологии Fast Ethernet обеспечивающий скоростью до 100 Мбит/с с симметричным алгоритмом блочного шифрования соединения по технологии AES-128 с размером блока 128 бит, ключ 128/192/256 бит.

Технология передачи данных по ЛЭП состоит в наложении на электрический ток (50 Гц) сигнала высокой частоты (от 1 до 30 МГц) со слабой энергией (до 0,5 В) (рис. 2). Сигнал проходит через электрические провода и оборудование. После чего его можно принять и раскодировать на значительном расстоянии. Таким образом передача данных может осуществляться не просто по проводам, а по контактной сети питания.

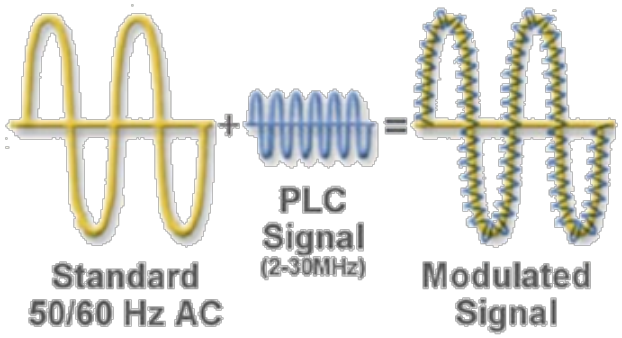


Рис. 2. Принцип технологии PLC

Исследования и разработки данного принципа начались еще в конце XIX века. Уже в XX веке осваивались системы передачи с частотным разделением каналов на высоковольтных линиях, в последующем на средних и низковольтных системах распределения. С появлением технологиями передачи данных по электрическим сетям 120/220 В – X–10 (коммуникационный протокол и основанный на нем инженерный стандарт, применяют в системах домашней автоматизации), CEBus и LonWorks, DPL1000 в 90-х

в интерес возрос еще более. Необходимо, было разработать систему, которая способна экономически эффективно конкурировать с беспроводными решениями.

За последние годы технология получила значительное развитие благодаря новым видам модуляций, методам контроля ошибок и коррекции: если в июне 2001 г. система передачи данных типа HomePlug 1.0 (название для различных спецификаций связи по линиям электропередачи) позволяла развивать скорость до 14 Мбит/сек, то сегодня выпускаются устройства с технологиями HomePlug AV2 поддерживающие скорости до 1 Гбит/сек. Но это теоретическая пропускная способность, реальная же пропускная способность может быть существенно меньше. Качество электропроводки, её неоднородность, скрутки в линии влияют и на пропускную способность, и на качество передачи данных. В ходе развертывания PLC сети устройства, включенные в одну сеть, будут работать стабильно, так как адаптеры работают на физическом уровне сетевой модели OSI, и при включенные в одну сеть питания синхронизируются между собой. Использование PLC технологий эффективно, где необходима оперативность, легкая расширяемость, простота реализации, мобильность устройств. При применении PLC технологии обычно используют готовые коммуникации, поэтому данная технология может быть использована в автоматизации технологических процессов, связывая блоки автоматизации по электропроводам или другим видам проводов.

Основные преимущества PLC:

– широкое применение: PLC может обеспечить связь в труднодоступных узлах связи, где радио и радиорелейный сигнал обладает высокой степенью затухания (здания с металлическими стенами, подземные сооружениях) или где применение радио и радиорелейной связи не допустимо (в ходе организации боя);

– низкая стоимость сокращение затрат на развертывание: PLC не требует установки новых проводов, в том числе и контактные сети;

– оперативность развертывания сети передачи данных – центр электропитания является одним из основных элементов узла связи;

– помехоустойчивость – PLC оборудование включает механизм подавления сигнала в заданном диапазоне, если есть влияние на какие-то частоты.

Основные недостатки PLC:

– создание помех для пользователей – проводка в технологии PLC неэкранирована поэтому излучает большое количество энергии так как используется та же полоса частот;

– при применении системы широкополосной передача через ЛЭП будут некоторые помехи от радиосигналов, излучаемых цепями PLC;

– скорость, качество и надёжность связи зависит от качества электропроводки, наличие скруток.

Таким образом, если сравнивать с Wi-Fi у PowerLine высокая стабильность соединения, ни включение силовых устройств, ни скачки напряжения, не мешают стабильности соединения. Кроме того, PowerLine является более защищенным. Систему защиты на Wi-Fi в определенных условиях возможно взломать в момент аутентификации пользователя, то при использовании PLC технологий соединение устанавливается при помощи предустановленного ключа, и взлом с теоретической точки зрения невозможен.

Применение PLC технологий в организации управления позволит повысить оперативность и устойчивость, расширить возможность применяемых средств управления, а также обеспечить сохранение в тайне от противника, мероприятий, проводимых командирами, штабами, начальниками родов войск, специальных войск в ходе подготовки и в период проведения боевых действий.

Список используемых источников

1. Симоненко И. В., Николаев Д. И., Иванов В. Г., Бажин М. И., Карев В. А. Программно-аппаратный комплекс автоматизированной системы управления узлом связи // Неделя науки СПбПУ: материалы научной конференции с международным участием. СПб. : ПИЛИТЕХ-ПРЕСС, 2019. С. 38–40.

2. Иванов В. Г., Корякин Д. Д., Панихидников С. А. Автоматизированные системы управления связью // Труды учебных заведений связи. СПб. : СПбГУТ, 2016. Т. 2. № 4. С. 56–62.

3. Связь по линиям электропередачи [Электронный ресурс]. URL: https://ru.wikipedia.org/wiki/Связь_по_ЛЭП (дата обращения 02.03.2020).

УДК 004.457
ГРНТИ 49.33; 20.53

СИСТЕМА МОНИТОРИНГА ПАРАМЕТРОВ ОБОРУДОВАНИЯ И СЕРВИСОВ УЗЛОВ СВЯЗИ С ИСПОЛЬЗОВАНИЕМ УНИВЕРСАЛЬНОГО ТЕРМИНАЛЬНОГО УСТРОЙСТВА СЛУЖЕБНОЙ СВЯЗИ

В. Г. Иванов, А. Ю. Савицкий

Военная академия связи им. Маршала Советского союза С.М. Буденного

Организации управления и несению службы дежурной сменой на узлах связи уделяют большое внимание. В статье рассматриваются организации управления на совре-

менном этапе развития средств технологического управления сетями. Показаны основные направления развития системы управления и возможности использования современных программных средств управления.

управление, узел связи, SNMP.

Управленческая составляющая обеспечивает до 40 % и более реализации боевого потенциала войск. Естественно, что при всех прочих равных условиях один из самых эффективных способов обеспечения общего превосходства в ходе вооруженного противоборства – это достижение превосходства в управлении. Несомненно, что это комплексная проблема, затрагивающая практически все сферы военного строительства. Но, пожалуй, наиболее чувствительным и наиболее проблемным на сегодня звеном является область организации системы управления.

На современном этапе в Вооруженных Силах Российской Федерации проводится внедрение высокоскоростных цифровых средств связи, обеспечивающих решение конкретных оперативных задач управления и повышения качества связи.

При этом значение технической основы пунктов управления (ПУ) не менее важно, чем оперативного состава, а зависимость должностных лиц от неё неуклонно растёт. Построение ПУ, их применение во всех видах деятельности войск, алгоритм работы должностных лиц во многом определяется именно её возможностями.

В настоящее время технической основой построения транспортных сетей связи (ТСС) являются гибридные телекоммуникационные системы передачи синхронной цифровой иерархии (СЦИ/SDH: STM-1, 4, 16, 64), но все большее значение принимает технология Ethernet транспортного уровня. ТСС включает не только системы передачи, но и, относящиеся к ним, средства контроля, оперативного переключения, резервирования, управления и синхронизации [1].

Среди протоколов для мониторинга устройств также используются протоколы SNMP, Telnet и SSH, с помощью которых происходит непосредственное подключение к оборудованию и получение данных при помощи системных команд, скриптов. Большинство существующих современных систем мониторинга IT-инфраструктуры используют одинаковый принцип: система мониторинга опрашивает оборудование или программное обеспечение, получает результат и сравнивает его либо с шаблоном, либо с заранее заданными, предельно допустимыми значениями.

SNMP (*Simple Network Management Protocol*) – протокол, который используется для управления сетевыми устройствами. С помощью протокола SNMP, программное обеспечение для управления сетевыми устройствами может получать доступ к информации, которая хранится на управляемых устройствах (например, на коммутаторе). На управляемых устройствах

SNMP хранит информацию об устройстве, на котором он работает, в базе данных, которая называется MIB [2].

SNMP был разработан для решения задач передачи данных в системах мониторинга, у каждой системы мониторинга существуют и собственные реализации протоколов обмена данными, но SNMP является наиболее популярным и востребованным за счет расширяемости и открытости интерфейса.

Для усовершенствования системы управления полевым узлом связи, в ходе научной работы, разработано универсальное терминальное устройство служебной связи «Терминал», и написано программное обеспечение автоматизированной системы управления узлом связи. Для организации управления средствами связи из состава аппаратных и станции УС с использованием «Терминала» в программно-аппаратном комплексе (ПАК) используется протокол SNMP (рис.).

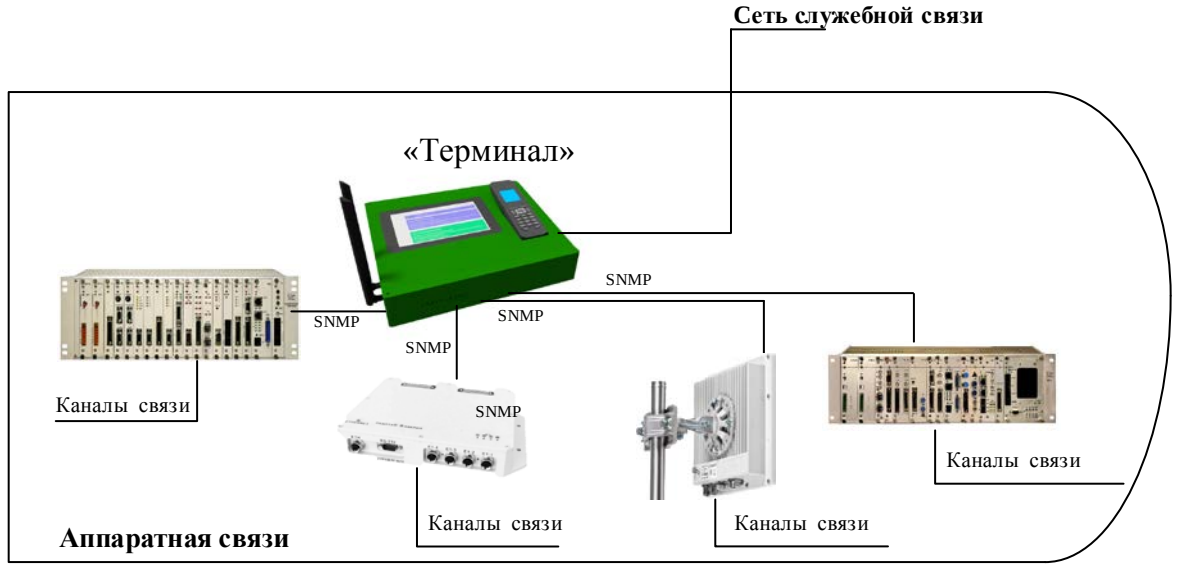


Рис. Схема подключения оборудования аппаратной для организации мониторинга и управления

При использовании SNMP один или более административных компьютеров (где функционируют программные средства, называемые менеджерами) выполняют отслеживание или управление группой хостов или устройств в компьютерной сети. На каждой управляемой системе есть постоянно запущенная программа, называемая агент, которая через SNMP передаёт информацию должностному лицу.

Модуль мониторинга ПАК построен с использованием основных принципов клиент-серверной архитектуры. Клиент представляет собой веб-приложение, доступное по определенному адресу в сети через браузер. Серверная часть состоит из трех сервисов. Цель разделения функционала системы на сервисы – распределение нагрузки и организация кэширования для часто

запрашиваемых клиентом ресурсов (например, изображения оборудования) [3].

Монитор непрерывно генерирует задания на опрос для зарегистрированного в системе оборудования. Каждое задание инкапсулирует в себе получение текущих параметров оборудования по протоколу SNMP, определение доступности оборудования в сети, сохранение результатов опроса в базу данных.

После каждого цикла опроса всего оборудования создается событие о том, что данные обновлены, и публикуется в шине событий.

Востребованность данной системы назрела уже давно, но без единства технических решений решить её сложно и практически невозможно, при этом, «Терминал» позволяет уже сегодня решать задачи управления узлами связи.

Структура ПАК позволяет развернуть его элементы с использованием «Терминала», а четкая структурированность и последовательность обрабатываемых данных на сервере ПАК, позволяет осуществлять бесперебойную работу средств в едином контуре управления узлом связи.

Структура программного комплекса ПАК разработана в соответствии с последовательностью работы должностных лиц органов управления связи и узлов связи по организации планирования и управления узлом связи.

Раздел ПАК, который запускается на «Терминале», позволяет лицам дежурной смены вести электронный журнал несения дежурства с автоматизированной фиксацией состояния каналов и связи боевого поста. Ключевой особенностью является обеспечение автоматизированного контроля состояния каналов и связи на основе подключения разработанного мини ЭВМ к средствам связи аппаратной, и ведения учета состояния запланированных связей, согласно таблицы-приказ, боевому посту. Получение информации об оборудовании осуществляется по протоколам SNMP. Структурное взаимодействие всех документов, разрабатываемых в ПАК с использованием единой базы данных, позволяет на всех уровнях управления узлом связи вести «стволовой» контроль учета состояния запланированных связей. При этом, в режиме реального времени дежурный по узлу связи сможет контролировать состояние каналов и средств связи, и своевременно принимать соответствующие решения.

Список используемых источников

1. Иванов В. Г., Панихидников С. А. Теория и практика построения технической основы системы управления специального назначения : монография. СПб. : СПбГУТ, 2016. 184 с.

2. Simple Network Management Protocol [Электронный ресурс]. URL: http://xgu.ru/wiki/SNMP (дата обращения 18.03.2020).

3. Симоненко И. В., Николаев Д. И., Иванов В. Г., Бажин М. И., Карев В. А. Программно-аппаратный комплекс автоматизированной системы управления узлом

связи // Неделя науки СПбПУ: материалы научной конференции с международным участием. СПб. : ПИЛИТЕХ-ПРЕСС, 2019. С. 38–40.

УДК 621.391.64
ГРНТИ 49.29.14

ОЦЕНКА ДЛИНЫ ДИСПЕРСИОННОГО РАЗБЕГАНИЯ ОПТИЧЕСКИХ СИГНАЛОВ В СТЕКЛАХ С РАЗНЫМ ХИМИЧЕСКИМ СОСТАВОМ

В. С. Иванов, Б. К. Резников, А. Н. Сергеев

Санкт-Петербургский государственный университет телекоммуникаций им. проф. М. А. Бонч-Бруевича

В связи с увеличением скорости и широким внедрением систем со спектральным разделением каналов появляются новые оптические волокна с разным химическим составом. При этом возникают новые влияющие факторы, которые нельзя не учитывать в инженерных расчетах проектируемой или реконструируемой линии связи. При выполнении расчётов нужно учитывать, помимо традиционных факторов, и скорость распространения разных длин волн, определяющую способность системы передавать максимально большие потоки информации. В связи с этим возникает необходимость знания о максимальном расхождении отельных оптических каналов при прохождении света по оптическому волокну с учетом химического состава стекла, из которого изготовлена сердцевина волокна. Это позволит оптимизировать систему передачи как по скорости, так и по максимальной длине элементарного кабельного участка или оптического тракта.

дисперсия, скорость передачи, химический состав стекол, спектральное разделение каналов, фазовая скорость.

Особенностью передачи сигналов, передаваемых по оптическому волокну в многоканальных системах, является то, что каждый из каналов переносится со своей скоростью. Это происходит из-за того, что для каждой длины волны существует свое собственное значение показателя преломления оптического волокна, из-за чего импульсы разных длин волн движутся с разными скоростями, что, в свою очередь, приводит к изменению расстояния между каналами и прохождению импульсов друг сквозь друга с последующим сложностями при демультиплексировании.

В режиме с нормальной дисперсией импульс с большей длиной волны движется быстрее, а в режиме с аномальной дисперсией наоборот.

Дисперсия определяется электромагнитным взаимодействием волны со связанными электронами материала среды, которое носит, как правило,

нелинейный (резонансный) характер и только вдали от резонансов может быть описано с приемлемой точностью уравнением Селмейера [1].

Для обычных оптических стекол показатель преломления, рассчитанный с помощью трехчленного уравнения Селмейера, отклоняется от фактического показателя преломления менее чем на 5×10^{-6} [2] в диапазоне длин волн от 365 нм до 2,3 мкм, что соответствует порядку однородности образца стекла [3]. В наиболее общем виде, уравнение Селмейера выглядит как [4]:

$$n^2(\lambda) = 1 + \sum_{j=1}^{3}\left(R_j \frac{\lambda^2}{\lambda^2-\omega_j^2}\right), \quad (1)$$

где ω_j и R_j – значения коэффициентов Селмейера, а суммирование по j для объемного кварцевого стекла ведется по первым трем резонансам [4]. Значение λ в формуле (1) измеряется в микрометрах (мкм).

Скорость распространения связана со значением показателя преломления соотношением:

$$v(\lambda) = \frac{C}{n(\lambda)}.$$

Тогда время распространения световой волны вдоль оптического волокна определенной длины будет определяться как:

$$t = \frac{z}{v(\lambda)}, \quad (2)$$

где z – длина оптического волокна.

Тогда расстояние, которое пройдет импульс, с той или иной длиной волны, будет определяться как:

$$L(n) = v_{\text{г}}(\lambda) * t = \frac{C*t}{\sqrt{1+\sum_{j=1}^{3}\left(R_j\frac{\lambda^2}{\lambda^2-\omega_j^2}\right)}}$$

Таким образом, разные длины волн в системах со спектральным разделением каналов имеют свою собственную скорость распространения. Эти скорости зависят только от состава стекла, длины волны и показателя преломления оптического волокна. Посмотрим, как показатель преломления влияет на скорость распространения сигналов. Для примера возьмем чистое кварцевое стекло SiO_2. Значения коэффициентов Селмейера (R_j и ω_j) для двуокиси кремния и некоторых других стекол приведены в таблице 1 (см. ниже).

Теперь можно рассчитать по формуле (2) скорость распространения импульса $v_{\text{г}}(t)$. В таблице 2 (см. ниже) приведены результаты расчета значений показателя преломления для стандартного частотного плана систем CWDM. Результаты расчета скорости приведены в таблице 3 (см. ниже).

ТАБЛИЦА 1. Значения коэффициентов Селлмейера для кварцевого стекла и некоторых других стекол с разным составом

Обозначение стекла	Состав стекла	Тип коэфф.	Значение коэффициента		
			1	2	3
А	SiO_2	R_j	0,6961663	0,4079426	0,8974794
		ω_j	0,0684043	0,1162414	9,8961610
Б	13,5 % GeO_2 86,5 % SiO_2	R_j	0,73454395	0,42710828	0,82103399
		ω_j	0,08697693	0,11195191	10,84654000
В	7,0 % GeO_2 93,0 % SiO_2	R_j	0,686982900	0,44479505	0,79073512
		ω_j	0,078087582	0,11551840	10,43662800

ТАБЛИЦА 2. Значение показателя преломления для длин волн стандартного частотного плана систем CWDM стекол А, В и С

λ, мкм		1,271	1,291	1,311	1,331	1,351	1,371	1,391	1,411	1,431
Показатель преломления для стекол	А	1,44725	1,447	1,44679	1,44657	1,44634	1,44611	1,44588	1,44565	1,44542
	Б	1,46868	1,4685	1,46829	1,46809	1,4679	1,4677	1,46751	1,46732	1,46713
	В	1,45814	1,4579	1,45775	1,45755	1,45735	1,45716	1,45696	1,45677	1,45657
λ, мкм		1,451	1,471	1,491	1,511	1,531	1,551	1,571	1,591	1,611
Показатель преломления для стекол	А	1,44519	1,4449	1,44472	1,4444	1,44425	1,44401	1,44377	1,44353	1,44328
	Б	1,46693	1,4667	1,46655	1,4663	1,46616	1,46597	1,46578	1,46558	1,46538
	В	1,45637	1,4561	1,45598	1,4557	1,45558	1,45539	1,45519	1,45498	1,45478

ТАБЛИЦА 3. Зависимость фазовых скоростей (в км/с) распространения в стекле от длины волны

λ, мкм	1,271	1,291	1,311	1,331	1,351	1,371	1,391	1,411	1,431
А	207289	207325	207355	207387	207420	207453	207486	207519	207552
Б	204265	204290	204319	204347	204373	204401	204427	204454	204480
В	205741	205775	205796	205824	205853	205879	205908	205935	205963
λ, мкм	1,451	1,471	1,491	1,511	1,531	1,551	1,571	1,591	1,611
А	207585	207626	207652	207698	207720	207754	207789	207823	207859
Б	204508	204540	204651	204596	204616	204642	204669	204697	204725
В	205991	205944	206046	206086	206103	206130	206158	206188	206216

На рис. 1 показана зависимость показателя преломления от длины волны для стекол, указанных в таблице 2.

Исходя из расчетов значений показателей преломления, приведенных в таблице 2 можно рассчитать фазовые скорости и время распространения света на участке 1 км. Результаты расчетов приведены в таблицах 3 и 4, а также на рис. 2.

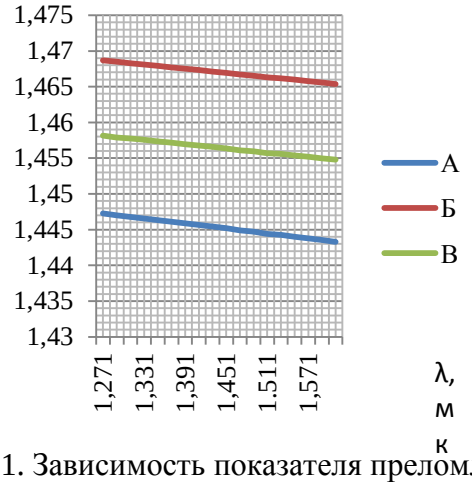


Рис. 1. Зависимость показателя преломления от длины волны у стекол А, Б и В

ТАБЛИЦА 4. Зависимость времени распространения световых волн в стекле типа А от длины волны на участке длиной 1 км

λ, мкм	**1,271**	**1,291**	**1,311**	**1,331**	**1,351**	**1,371**
t, мкс	4,82416	4,82333	4,82263	4,8219	4,82113	4,82036
λ, мкм	**1,391**	**1,411**	**1,431**	**1,451**	**1,471**	**1,491**
t, мкс	4,81959	4,81883	4,81806	4,81729	4,81633	4,81573
λ, мкм	**1,511**	**1,531**	**1,551**	**1,571**	**1,591**	**1,611**
t, мкс	4,81466	4,81416	4,81336	4,81256	4,81176	4,81093

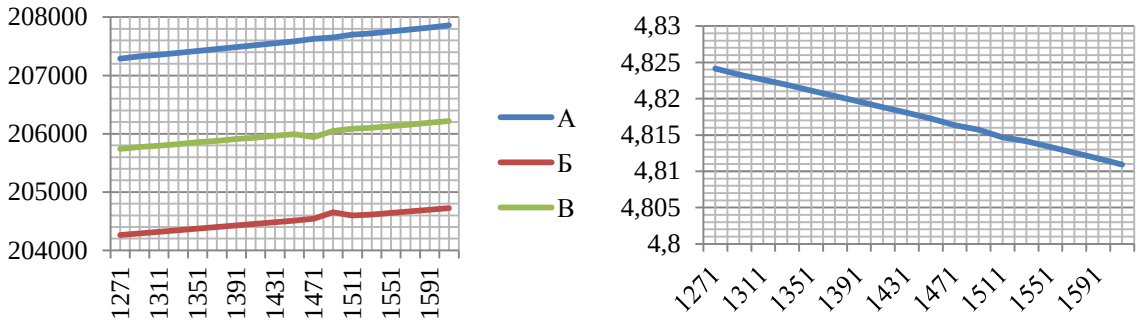


Рис. 2. Слева – фазовая скорость распространения света разных длин волн в стеклах с разным химическим составом сердцевины; справа – зависимость времени распространения разных длин волн в стекле типа А на участке длиной 1 км

Время t, за которое сигнал пройдет определенное расстояние L определяется по следующему выражению:

$$t = \frac{L}{C}\sqrt{\sum_{j=1}^{3}\left(R_j \frac{\lambda^2}{\lambda^2 - \omega_j^2}\right)}.$$

Таким образом, максимальная разность времени появления оптических сигналов в конце участка длиной 1 км составляет 13,23 нс при условии, что все каналы были введены в волокно одновременно.

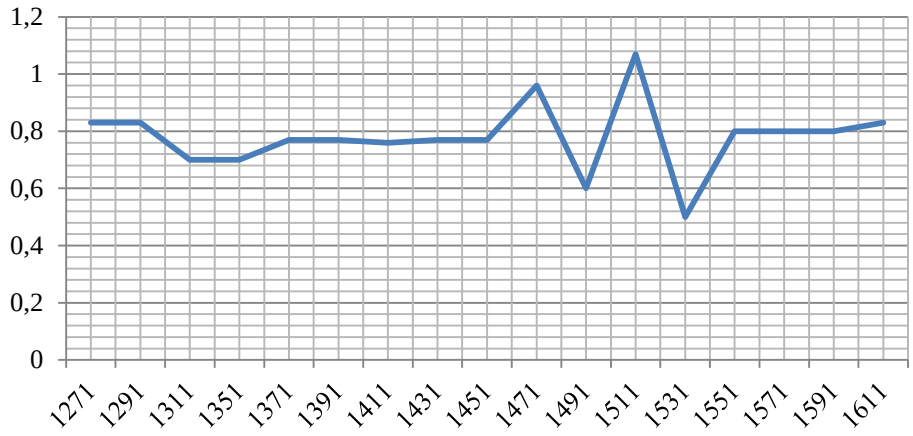


Рис. 3. Разброс времени распространения между соседними каналами на участке длиной 1 км находится в диапазоне от 0,5 до 1,07 нс

Таким образом, расстояния, на которые импульсы разных длин волн смещаются относительно друг друга, зависят от величины показателя преломления и значения длины волны (рис. 3). В системах CWDM в чистом кварцевом волокне разность времени распространения крайних каналов через один километр достигает величины 13,23 нс. В диапазоне 1291–1451 нм каналы имеют наименьший разброс во времени и имеют наилучшие дисперсионные параметры.

Список используемых источников

1. Агравал Г. Нелинейная волоконная оптика. М. : Мир, 1996.

2. Стекла для изготовления оптических волокон и кабелей [Электронный ресурс] // HyperLine Cabling System. URL: http://www.hyperline.ru/learn/teoriya-i-praktika-montazha-kabelnykh-sistem/stekla-dlya-izgotovleniya-opticheskikh-volokon-i-kabeley/ (дата обращения 12.02.2020).

3. Sellmeier equation [Electronic resourse] // Wikipedia – The Free Encyclopedia. URL: https://en.wikipedia.org/wiki/Sellmeier_equation (дата обращения 13.02.2020).

4. Optical Properties [Electronic resourse] // Ohara Corporation. URL: http://ohara-corp.com/o2.html (дата обращения 12.02.2020).

УДК 681.7.068.4
ГРНТИ 47.13.31

КОНВЕРГЕНЦИЯ ТЕХНОЛОГИЙ ФОТОНИКИ И РАДИОЭЛЕКТРОНИКИ ПРИ СОЗДАНИИ ВЫСОКОСКОРОСТНЫХ ШИН ПЕРЕДАЧИ ДАННЫХ

Н. Н. Иванов[1], Т. А. Радзиевская[2]

[1]Санкт-Петербургский государственный университет телекоммуникаций им. проф. М. А. Бонч-Бруевича
[2]Санкт-Петербургский государственный электротехнический университет «ЛЭТИ» им. В. И. Ульянова (Ленина)

Высокоскоростная передача данных на дистанции блок-блок и модуль-модуль может быть обеспечена оптическими методами за счёт применения полимерных оптических волноводов в сочетании с микрооптическими устройствами сопряжения волноводов с лазерными диодами и фотодиодами. Для изготовления такой оптической шины передачи данных предлагается базироваться на сумме аддитивных технологий, близких к 3D MID.

полимерный планарный оптический волновод, аддитивные технологии.

Проблема передачи данных на большие расстояния имеет достаточно высокий уровень решения путем успешного применения для этой цели традиционных стеклянных одномодовых и многомодовых волоконно-оптических соединений. Однако для межмодульных и межблочных соединений как ведущие компании мира (*Samsung*, IBM и др.) [1], так и ряд российских исследователей [2], предлагают использовать полимерные оптические волноводы. Преимуществом таких волноводов перед традиционным оптоволокном является согласованный с материалом стандартных печатных плат коэффициент температурного расширения волновода, что позволит защитить волноводы от растрескивания под действием различных температурных факторов. Полимерные волноводы можно формировать интегральным способом по всей поверхности, а также между слоями печатной платы. В состав оптического канала связи на печатной плате, в таком случае, входят:

– источник излучения, генерирующий модулированное оптическое излучение заданной длины волны;

– устройство ввода лазерного излучения в волновод;

– диэлектрический полимерный оптический волновод прямоугольного (канального) сечения;

– устройство вывода излучения из волновода в фотоприёмник;

– фотоприёмный диод.

В настоящее время стандарт технологии формирования полимерной оптической шины передачи данных отсутствует. В том числе, пока не определены общепринятые окна прозрачности волноводов из конкретных полимерных материалов, уровни потерь и перекрестных помех, уровни генерации шумов при изменении климатических и механических условий, требования к габаритно-присоединительным размерам составных частей оптического канала, знание которых необходимо для получения максимальной скорости передачи данных и разработки драйвера управления лазером. В интересах обеспечения последующей разработки образцов межмодульной и межблочной коммутации, создания серийной технологии производства коммутационных плат с интегрированными оптическими проводниками, необходимо выявить реальные параметры и обоснованные требования для ряда возможных материалов и технологий.

Одним из шагов в обозначенном направлении является выбор базовых технологий формирования полимерных оптических волноводов и устройств сопряжения (ввода/вывода излучения) волновода с полупроводниковыми оптическими компонентами.

В качестве базовой технологии формирования матрицы полимерных оптических волноводов прямоугольного сечения, представляется рациональным выбор технологии мягкой фотолитографии, особенности которой, применительно к рассматриваемым изделиям, нашли отражение в ряде публикаций [3, 4, 5]. В частности, для изготовления макета платы с полимерными оптическими волноводами прямоугольного сечения (оптико-электронной шиной передачи данных) была определена последовательность этапов создания оптико-электронной шины [5] с соответствующими параметрами и режимами обработки, которая представлена на рис. 1.

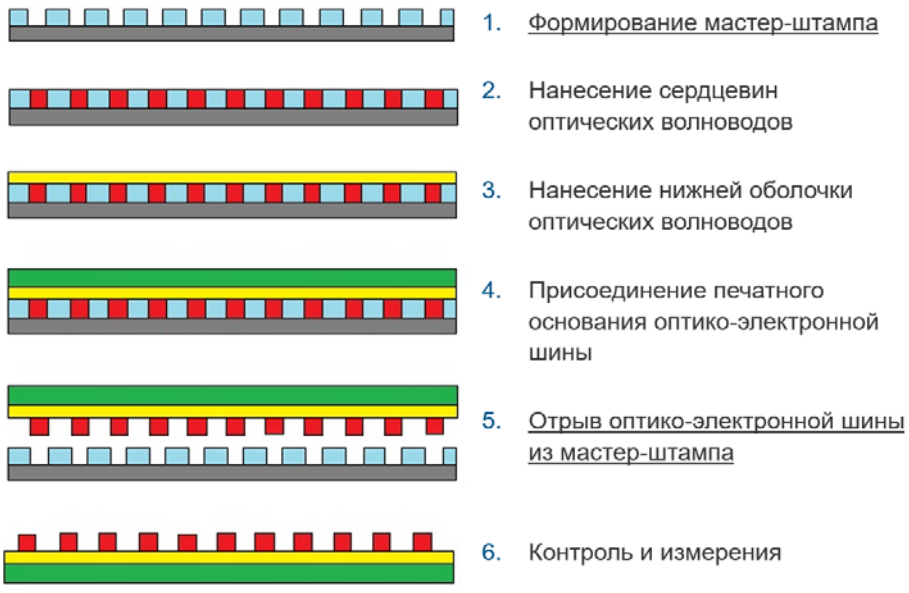


Рис. 1. Блок-схема технологического процесса формирования оптико-электронной шины передачи данных

Наиболее важными и лимитированными этапами являются изготовление мастер-штампа с помощью фотолитографии, проводимой в ЦМСТ ЗАО «НИТИ «Авангард» (Санкт-Петербург), и отрыв шины из мастер-штампа.

Следует отметить, что предложенный технологический процесс не имеет полного соответствия с традиционной технологией мягкой литографии, применяемой для изготовления микрофлюидных и микросистемных изделий. Вместо оттиска мастер-штампа, в полимерном слое происходит нанесение полимерного материала сердцевин оптических волноводов путем полива, с последующим удалением избыточного полимера с помощью ракеля. Кроме того, в дальнейшем отсутствует оттиск мягкого полимерного штампа, полученного из жесткого мастер-штампа, в честь которого была названа эта технология «мягкой». Следовательно, разработанный технологический процесс можно отнести к нетрадиционной технологии мягкой литографии, модифицированной под нужды изготовления печатных плат с оптико-электронными шинами передачи данных в виде полимерных оптических волноводов прямоугольного сечения.

Предлагаемая технология обладает рядом особенностей, которые обеспечивают гибкую адаптацию к различным конкретным условиям:

– для создания сердцевины волновода используется материал, обладающий широким окном прозрачности (от ИК до ближнего УФ), что может оказаться весьма полезным для его согласования с излучателем и фотоприёмником;

– получаемые функциональные слои хорошо согласуются с печатными платами по коэффициенту термического расширения, что обеспечит длительный ресурс работы устройства в условиях смены температур и энергоциклов;

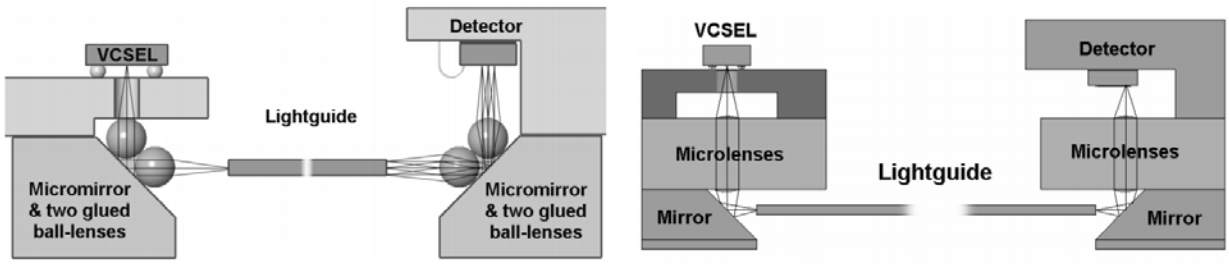
– необходимый набор технологических приёмов идентичен, либо близок к стандартным технологиям изготовления многослойных печатных плат современных радиоэлектронных модулей, и может быть освоен на серийных производственных предприятиях;

– возможность повторного применения жесткого мастер-штампа позволяет снизить расходы на изготовление подобных устройств, а также уменьшает требования к технологической среде, в которой производится конечное устройство, т. к. только при формировании мастер-штампа необходима среда чистых производственных помещений классов ISO 5-6.

При выборе базовой технологии изготовления устройств сопряжения волноводов с лазерным диодом и фотодиодом, следует принять во внимание особенности конструкции волновода, необходимость соответствия их геометрической формы и точности позиционирования устройств сопряжения во избежание увеличения потерь сигнала.

Дополнительной сложностью, на текущем этапе, является неопределённость с длиной волны используемого излучения (например, в силу неопределённости выбора температуры, около которой будет стабилизироваться режим лазерного диода). Диодный лазер, благодаря особенности своей конструкции, может генерировать излучение в некотором диапазоне длин волн, и это зависит от материала и структуры полупроводникового кристалла лазера и его температуры. Обеспечение минимальных потерь при оптимальной длине волны для возможных полимерных материалов, может выходить за пределы стандарта длины волны, принятой в телекоммуникации (1310 и 1550 нм). В этой связи, стандартные лазеры, используемые для телекоммуникации, могут оказаться неоптимальными. Условия работы лазера и фотоприёмника в составе полимерной оптической шины передачи данных отличаются от традиционных для телекоммуникаций (плотность размещения, особенности ввода и вывода излучения в планарный волновод, параметры драйвера, управляющего лазером, температура близлежащих компонентов и др.), что потребует уточнения конструкции лазера и, как следствие, конструкции устройств сопряжения.

Несколько лет назад были предложены варианты конструкции устройств сопряжения излучателя и фотоприёмника с полимерным планарным оптическим волноводом, например, такие, как на рис. 2 [1].



а) б)

Рис. 2. Конструкция узлов сопряжения со сферическими (а) и плоскими (б) линзами

Расчёты показывают [1], что точность размеров оптических элементов устройств сопряжения должна составлять единицы микрометров, а точность позиционирования – порядка 5–10 мкм. Для таких устройств могут применяться светопрозрачные полимерные и стеклянные материалы, отражающие металлические покрытия, прецизионные несущие конструкции могут выполняться из керамики. Именно для таких устройств востребованы различные лучевые и струйные технологии, напыление и лазерная абляция, и многие, многие другие технологии из арсенала радиоэлектроники, оптики, фотоники. Наблюдается взаимопроникновение и взаимодополнение технологий – их конвергенция.

Базовая технология формирования устройств сопряжения должна обладать максимальной гибкостью, способностью обрабатывать широкий

спектр материалов, обеспечивать высокую точность и качество поверхности получаемых деталей и их покрытий. Сегодня комплекс таких технологий известен под широким названием «аддитивные технологии». В более узком смысле, рациональными технологиями для получения устройств сопряжения, по нашему мнению, могли бы стать технологии, известные под названием 3D-MID. Сегодня ряд производителей радиоэлектронного и оптоэлектронного оборудования за счёт использования технологии 3D-MID [6, 7] добиваются качественного улучшения своей продукции и нащупывают существенный потенциал для резкого нового прорыва в создании следующих поколений приборов и систем.

Заключение

Постоянный рост прецизионности радиоэлектронных технологий при одновременном расширении использования полимерных и керамических материалов при изготовлении микрооптики, внедрение струйных и лучевых методов обработки поверхности создали условия для конвергенции технологий фотоники и радиоэлектроники на современном этапе создания высокоскоростных оптических шин передачи данных.

Список используемых источников

1. Karppinen M. Embedded optical interconnect on printed wiring board // Proceedings of SPIE. 2004. Vol. 5453. PP. 150–164.

2. Ахманов А. С. Оптическая передача информации в супер-ЭВМ и микропроцессорных системах. Часть 1 // LIGHTWAVE. 2008. № 3. С. 46–53.

3. Immonen M., Wub J., Yanb H. J. etc. Electro-Optical Backplane Demonstrator with Multimode Polymer Waveguides for Board-to-Board Interconnects // Proceedings of the 5-th Electronics System-integration Technology Conference (ESTC), Helsinki, 16–18 Sept. 2014. Helsinki, Finland, 2014, PP. 1–6.

4. Соколов В. И., Ахманов А. С., Китай М. С. и др. Лазерные технологии формирования полимерных элементов микро и нанофотоники для высокоскоростных информационных систем [Электронный ресурс] // 30 лет Институту проблем лазерных и информационных технологий Российской академии наук (ИПЛИТ РАН). URL: http://shatura.laser.ru/laser.ru/30/Polymer_photonics.pdf (дата обращения: 26.03.2020).

5. Manvelova T A, Tarasov S A, Ivanov N N. Polymer Optoelectronic Bus for High-speed Data Transmission Systems // Journal of Physics: Conference Series. 2019. Vol. 1400. 066051. PP. 1–4.

6. Кондрашин А. А., Лямин А. Н., Слепцов В. В. Современные технологии изготовления трехмерных электронных устройств. М. : Техносфера, 2016. 150 с.

7. Киселёв С. А., Могильников И. А., Райков Д. В., Яковлев Д. М. Применение 3D MID-технологии для конструирования электронных устройств. URL: http://elar.urfu.ru/bitstream/10995/68381/1/fti_2018_08.pdf (дата обращения: 27.03.2020 г.).

УДК 621.3.095
ГРНТИ 49.29.01

ПРИМЕНЕНИЕ ПОЛЕВЫХ ОПТИЧЕСКИХ КАБЕЛЕЙ В РОБОТЕХНИЧЕСКИХ КОМПЛЕКСАХ

С. А. Иванов, Е. С. Сапченко, И. Ю. Смирнов

Военной академии связи им. Маршала Советского союза С. М. Буденного

Рассмотрены вопросы применения волоконно-оптических линий связи для управления робототехническими комплексами. Приведены недостатки применения оптического кабеля на основе кварцевых оптических волокон для управления робототехническими комплексами. Обосновано применение в полевых оптических кабелях полимерного оптического волокна. Приведен анализ полимерных оптических волокон отечественных и зарубежных производителей.

полевой оптический кабель, оптическое волокно, робототехнический комплекс, линии связи.

Робототехнические комплексы (РТК) – это, технологически сложные, устройства, нацеленные на выполнение поставленных задач в автоматическом режиме, когда заранее программируется алгоритм действий, или под управлением оператора. Дистанционное управление РТК осуществляется с пульта по радиоканалу или по кабельной линии управления. Управление по средствам радиоканала является преобладающим в РТК из-за своих возможностей, однако, существует ряд практических задач применения РТК, исключающих использование радиоуправления (например, выполнение задач в токопроводящих средах, в условиях электромагнитных воздействий и т. д.).

Управление РТК по проводным линиям связи возможно посредством использования электропроводного или оптического кабеля (ОК).

Прикладное значение волоконно-оптических линий связи (ВОЛС) для робототехнических комплексов специального назначения (РТКСН) обусловлено свойствами оптического волокна (ОВ):

– невосприимчивостью к электромагнитному излучению;

– помехозащищенностью;

– гальванической развязкой между передающей и приемной частью РКСН;

– возможностью работы в агрессивных и электропроводящих средах;

– высокой скоростью прохождения сигналов, низким уровнем собственных шумов и малым затуханием.

Не мене важным преимуществом ОВ для РТКСН является малый вес и объем применяемого ОК при достаточно высокой механической прочности. Кроме того, некоторые типы прозрачных оптических материалов невосприимчивы к воздействию гамма-излучения, что особенно актуально в очагах радиационного заражения [1].

Для управления РТКСН лучше применять полевые ОК, которые проектируются под работу в экстремальных эксплуатационных условиях во всех климатических зонах России. Полевые ОК проходят испытание на размотку-смотку, изгибы, кручение и раздавливание под воздействием внешних условий, таких как воздействие солнечного излучения, различных температурных перепадов в интервале от –60 до +70°С, повышенной влажности и т. д. Кабели обязательно проверяются на устойчивость к статическим растягивающим усилиям (в том числе в месте заделки в соединительную арматуру), а также на устойчивость к гамма-излучению и воздействию электромагнитного импульса. Они не должны распространять горение и иметь защиту от грызунов.

Тщательный подход к выбору конструкции и применяемых материалов полевых ОК обусловлен их малой массой и габаритными размерами. В полевых ОК обычно не применяются металлические элементы. Для придания им повышенной стойкости к воздействию отрицательных температур применяют стеклопластиковые элементы (рис. 1). Комбинация стеклопластиковых элементов с высокопрочными синтетическими нитями обеспечивает высокую устойчивость ОК к сжимающим и растягивающим нагрузкам [2].

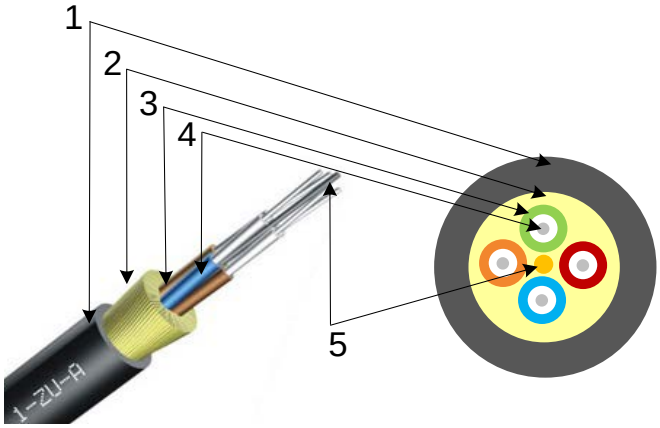


Рис. 1. Конструкция полевого оптического кабеля:
1 – полиэтиленовая оболочка; 2 – защитный слой из кевларовых нитей;
3 – трубки-модули с гидрофобным гелем; 4 – оптическое волокно;
5 – силовой элемент из стеклопластика

Недостатком ОК на основе кварцевых оптических волокон является его хрупкость, в особенности при изгибе на угол меньше 90°. Так как РТКСН

являются подвижными устройствами, то ОК практически не будет функционировать в статическом состоянии. В этом случае наработка до отказа ОК будет определяться стойкостью к критическим изгибам и равняться времени исправной работы его ОВ ($K_{и\ ок} = K_{и\ ов}$) [3].

Для реализации потенциальных возможностей применения ВОЛС в РТКСН необходима разработка специализированных ОВ и компонентов, устойчивых к механическим воздействиям, и достаточно дешевых для реализации массового выпуска в производстве.

Одним из решений задачи по повышению живучести линии связи с РТКСН является применение ОК на основе полимерных ОВ (ПОВ) (рис. 2). У полимерного волокна, по сравнению с кварцевым, имеются серьезные преимущества: большой диаметр сердцевины значительно облегчает соединение; гибкость и податливость облегчают быстрое развертывание; благодаря большой апертуре пластикового волокна ввод излучения в него значительно проще, поэтому вместо дорогостоящих узконаправленных лазеров или специальной фокусирующей оптики, в передатчиках для ПОВ возможно использовать дешевые светодиоды (LED) с широким углом расходимости, излучающие в видимом диапазоне [4].

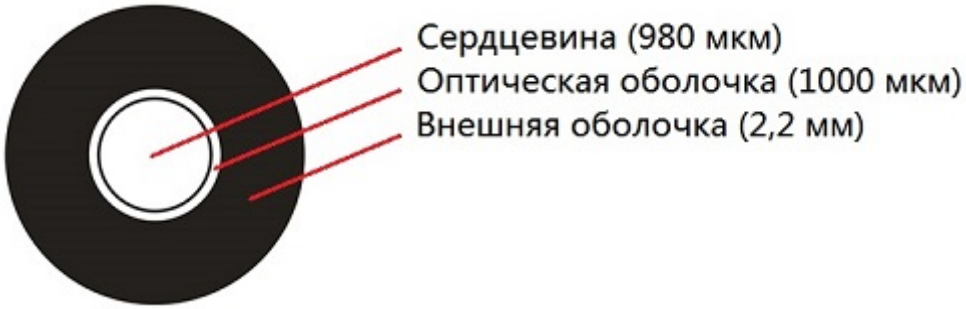


Рис. 2. Пример геометрических характеристик полимерного оптического волокна

Помимо особенностей, присущих самому ПОВ, этот тип волокна имеет все те же преимущества перед медными линиями, что и кварцевое волокно: невосприимчивость к электромагнитному излучению, изолирующие свойства, меньшие габариты и малый вес. ПОВ – это единственный тип ОВ, который может монтироваться повсюду без какого-либо специального оборудования, и поэтому потенциал использования ПОВ в робототехнике очень высок. А достижения последних лет в материаловедении, технологии производства ОВ, развитии новых типов оптических передатчиков, а также новых сетевых и промышленных приложений, сделали ПОВ привлекательным, несмотря на то, что характеристики его затухания и полосы пропускания существенно хуже, чем у кварцевого.

На сегодняшний день лидерами в производстве ПОВ являются японские компании Mitsubishi Chemical и Asahi Kasei, которые предлагают широкий ассортимент пластиковых волокон различных диаметров (от 125 мкм

до 3 мм) и в различных внешних оболочках, что позволяет использовать их, в частности, в экстремальных условиях. Затухание в их волокнах обычно составляет 0,15–0,19 дБ/м. Кроме стандартных ПОВ с одной сердцевиной, эти компании разрабатывают многосердцевинные волокна, имеющие малые потери на изгибе.

В России производство ПОВ осуществляет ООО «Технологический центр полимерного оптического волокна» (г. Тверь), производящий волокна диаметром 0,15–3 мм. Сравнительные характеристики отечественных и зарубежных ПОВ представлены в таблице.

ТАБЛИЦА 1. Характеристики отечественных и зарубежных ПОВ

№ п/п	Основные параметры	Производитель		
		ТЦ ПОВ Россия	Mitsubishi Chemical, Япония	Asahi Kasei, Япония
1	Тип ОВ	многомодовое	многомодовое	многомодовое
2	Номинальный диаметр ОВ, мм	0,2–0,3	0,2	0,2
3	Вносимые потери не более дБ на 1 км длины ОВ	200–500	160	150
4	Числовая апертура	0,45–0,5	0,5	0,4
5	Допустимое растягивающее усилие, Н (кг/мм^2)	(8,35)	140	245
6	Интервал рабочих температур	–50/+80	–55/+85	–55/+85

Как видно из таблицы потери в ПОВ, по сравнению с кварцевыми волокнами, достаточно высоки, это связано с собственным поглощением материала и обусловлено взаимодействием с гармониками колебаний углеводородных групп. Однако, существуют ПОВ, созданные с использованием фтора, в которых потери удалось снизить до 50 дБ/км (теоретически в данном типе ПОВ потери можно снизить до 10 дб/км) [5].

Обычно линии на основе ПОВ имеют длину порядка нескольких десятков метров, а максимальная скорость передачи ограничивается примерно 200 Мбит/с. В 2004 году была достигнута скорость передачи в 40 Гбит/с на расстоянии в 30 м.

Так же существуют термоустойчивые ПОВ, работающие в диапазоне от –55 до +105 °С (ПОВ на основе поликорбаната сохраняет свои оптические и механические свойства при температуре до 130–140 °С) [5].

Таким образом, ПОВ имеют ряд преимуществ, которые делают их конкурентно способными с кварцевыми ОВ при применении в РТКСН: высокая гибкость ПОВ (некоторые виды ПОВ выдерживают деформацию до 13 %), устойчивость к влиянию динамических механических нагрузок и вибрациям, увеличенный апертурный угол (достигает 60 градусов), радиационная

стойкость, малая плотность, позволяющая легко монтировать и обслуживать, а также быстро заменять поврежденные участки при необходимости. Решаемые задачи РТКСН разнообразны также, как и условия, в которых применяются эти комплексы. Использование для управления РТКСН полевых ОК на основе кварцевых ОВ не целесообразно из-за их хрупкости, что обуславливает необходимость создания новых специализированных типов полевых оптических кабелей на основе ПОВ.

Список используемых источников

1. Мендез А., Морзе Т. Ф. Справочник по специализированным оптическим волокнам. М. : Техносфера, 2012. 728 с.

2. Иванов Н. А., Иванов С. А., Стахеев И. Г. Современные специализированные оптические волокна // Актуальные проблемы инфотелекоммуникаций в науке и образовании: III Международная научно-техническая и научно-методическая конференция: сб. науч. ст. в 2-х т. СПб. : СПбГУТ, 2015. Т. 2. С. 1228–1232.

3. Иванов С. А., Иванов Н. А., Лапшин Б. А., Политыкин Р. В., Смирнов И. Ю. Способ моделирования линии связи с распределенными параметрами. Пат. 2583740 Российская Федерация; заявитель и патентообладатель Военная академия связи. – № 2015100724/08; заявл. 12.01.2015; опубл. 10.05.2015.

4. Иванов С. А. Смирнов И. Ю. Моделирование пассивных компонентов волоконно-оптических линий связи для робототехнических комплексов военного назначения // Сборник трудов 4 ЦНИИ МО РФ. 2017. Вып. 132. Т. 2. С. 49–52.

5. Семенов А. Перспективы полимерных световодов в СКС [Электронный ресурс] // Открытые системы: электрон. журн. 2004. URL: http://www.osp.ru/lan/2004/01/138519 (дата обращения 05.12.2019).

УДК 004.771
ГРНТИ 50.41.23

НАСТРОЙКА ФАЙЛОВОГО СЕРВЕРА SAMBA В ОПЕРАЦИОННОЙ СИСТЕМЕ ASTRA LINUX SPECIAL EDITION

В. И. Ивко, А. Н. Лапко

Академия Федеральной службы охраны Российской Федерации

Статья посвящена решению задачи сетевого взаимодействия в гетерогенных сетях на базе операционных систем семейств Windows и Linux. Представлен обоснованный выбор файлового сервера Samba для решения поставленной задачи, приведены варианты его конфигурирования в операционной системе Astra Linux SE. Описаны интерфейс и основной функционал приложения Samba, отмечена процедура настройки

доступа к сетевым ресурсам с использованием этого приложения. Выделены структура и параметры конфигурационного файла, приведен пример его заполнения.

сетевое взаимодействие, гетерогенная сеть, операционная система Astra Linux SE, файловый сервер Samba, конфигурационный файл smb.conf, параметры конфигурации.

Процесс перехода государственных учреждений на использование программного обеспечения с открытым исходным кодом приводит к появлению гетерогенных сетей. Так, наиболее распространенными являются сети, узлы которых функционируют под управлением операционных систем (ОС) семейств Windows и Linux. При этом возможно появление проблем сетевого взаимодействия, связанных с недоступностью сетевых ресурсов (директорий, файлов, принтеров), находящихся на узлах под управлением ОС другого семейства.

Для решения задачи сетевого взаимодействия используются различные технологии: Active Directory, Calculate Directory Server, Univention Corporate Server, Nextcloud, Astra Linux Directory, Samba [1, 2]. Помимо преимуществ, представленные технологии обладают ограничениями, которые затрудняют или вообще не позволяют их использовать для организации сетевого взаимодействия в гетерогенных сетях. Так, например:

– Active Directory и Astra Linux Directory не предназначены для организации сетевого взаимодействия в гетерогенных сетях, поскольку Active Directory применяется исключительно в ОС Windows, а Astra Linux Directory – в ОС Linux;

– Calculate Directory Server и Univention Corporate Server представляют собой полноценные ОС на базе Gentoo Linux и Debian GNU/Linux соответственно, установка которых может привести к дополнительным затратам, что не всегда целесообразно с экономической точки зрения;

– Nextcloud основана на облачном хранении данных, что в некоторых случаях не приемлемо с точки зрения обеспечения безопасности и безотказности доступа.

Таким образом, наиболее рациональным способом организации сетевого взаимодействия в гетерогенных сетях на базе ОС семейств Windows и Linux, является использование файлового сервера Samba. Samba работает по протоколу SMB/CIFS. Для его развертывания на узлах, функционирующих под управлением ОС Windows, используются штатные средства ОС, а на узлах, функционирующих под управлением ОС Linux, используется файловый сервер Samba.

Рассмотрим настройку файлового сервера Samba на примере ОС Astra Linux Special Edition. Существуют два варианта конфигурирования файлового сервера Samba: с использованием графической утилиты «Общие папки Samba» и путем редактирования файла конфигурации smb.conf [3].

Приложение Samba имеет интуитивно понятный графический интерфейс (рис. 1). Доступ к нему можно получить из панели управления или проводника: Сеть / Общие папки Samba.

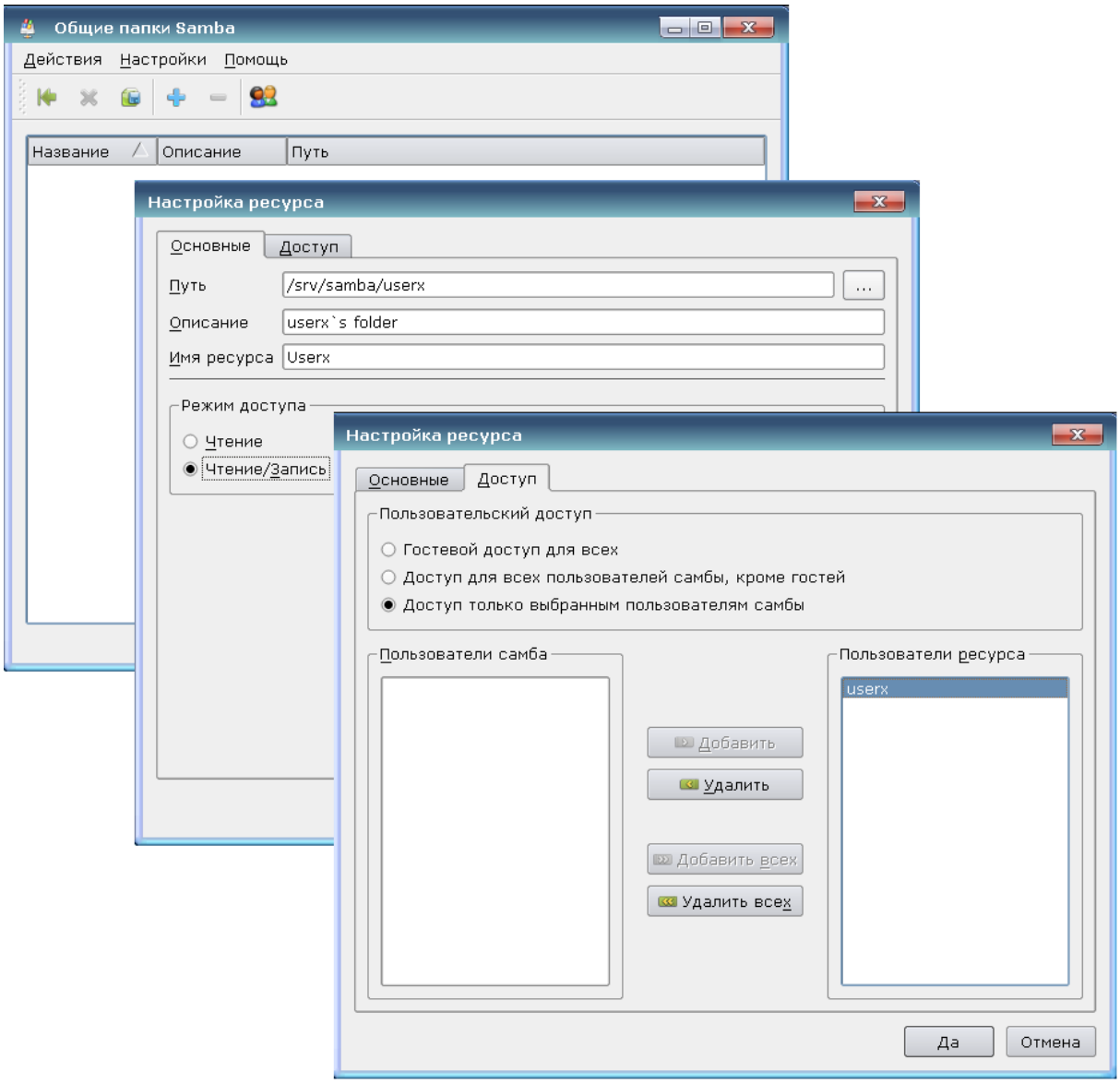


Рис. 1. Интерфейс приложения Samba

Приложение реализует функции:

– управления учетными записями пользователей;

– определения доступности сетевых ресурсов и установки режима доступа (чтение, чтение/запись) к сетевым ресурсам;

– настройки файлового сервера Samba: задание его названия в сетевом окружении, определение рабочей группы, разрешение доступа к печати;

– настройки параметров безопасности: выбор режима аутентификации и гостевой записи, включение шифрования паролей.

Так, при настройке доступа к общей директории, в главном окне программы требуется выбрать соответствующее действие. В окне «Настройка ресурса» следует указать полный путь к директории, ее описание и название сетевого ресурса, установить режим доступа. В настройках доступа выбрать вариант доступа к ресурсу и, при необходимости, указать список пользователей и групп (рис. 1).

Возможности приложения ограничены, по сравнению с файлом конфигурации smb.conf, который находится в каталоге etc/Samba/. Этот файл определяет, кому и к каким сетевым ресурсам предоставляется доступ, а также какие ограничения существуют на использование этих ресурсов. Файл является текстовым и содержит настраиваемые параметры в формате: параметр = значение. Перечисление нескольких значений для параметра осуществляется через пробел. Каждый параметр пишется с новой строки. Файл конфигурации не чувствителен к регистру, лишним пробелам и пустым строкам. Символ # является комментарием, % позволяет использовать значения подстановочных переменных (табл. 1).

ТАБЛИЦА 1. Подстановочные переменные

Переменная	Описание
%*a*	архитектура (ОС) клиента
%*g*	основная группа
%*h*	имя сервера
%*H*	домашняя директория пользователя
%*I*	IP-адрес клиента
%*L*	NetBIOS-имя сервера
%*m*	NetBIOS-имя клиента
%*M*	имя клиента
%*P*	корневая директория ресурса
%*S*	имя ресурса
%*T*	текущая дата и время
%*u*	имя пользователя
%*v*	версия Samba

Конфигурационный файл smb.conf разбит на разделы: global – определяет общие параметры, которые будут использоваться для определения доступа ко всем ресурсам; share definitions – определяет параметры доступа к каждому сетевому ресурсу (табл. 2, см. ниже). Каждый раздел должен начинаться с заголовка, который заключен в прямоугольные скобки.

Так, при настройке доступа к директории /srv/samba/user_x для пользователя user_x, администратора root и группы groop_x, а также доступа к директории /srv/samba/admin только для администратора root файл конфигурации smb.conf должен содержать:

ТАБЛИЦА 2. Основные конфигурационные параметры

Параметр	Описание
раздел global	
workgroup	рабочая группа сервера
netbios name	NetBIOS-имя сервера
server string	строка описания сервера (по умолчанию – номер версии Samba)
interfaces	интерфейс сетевой карты в формате: IP-адрес – маска подсети
security	уровень безопасности; допустимые значения: user – безопасность на уровне пользователей (по логину и паролю); share – на уровне ресурсов, server – на уровне сервера, domain – на уровне домена
map to guest	способ обработки запросов; допустимые значения: no – доступ пользователей, указавших неверный пароль, запрещен; bad user – пользователь получает права гостевой учетной записи
encrypt passwords	шифрование паролей при обмене с клиентом
guest account	имя пользователя, привилегии которого получают любые клиенты при доступе к общим ресурсам (по умолчанию – nobody)
invalid users	список пользователей, которым запрещен доступ к системе
read list	список пользователей с доступом только на чтение
write list	список пользователей с доступом на чтение и запись
hosts allow	список узлов, которым разрешен доступ к файловому серверу
hosts deny	список узлов, которым запрещен доступ к файловому серверу
log level	уровень отладки: 0 – ошибка, 1 – предупреждение, 2 – уведомление, 3 – сообщение
syslog	пороговое значение уровня отладки; отладочные сообщения с уровнем, меньшим порога, направляются в системный журнал
syslog only	отладочные сообщения помещаются только в системный журнал
log file	расположение и имя файла журнала
max log size	максимальный размер файла журнала
max open files	максимальное количество файлов, которое клиент может открыть на сервере
case sensitive	определяет чувствительность к регистру в именах файлов
unix charset	задает карту перекодировки для имен файлов
hide files	список файлов, которые являются невидимыми для клиентов
logon script	название файла, выполняемого на клиенте после входа на сервер
раздел share definitions	
path	полный путь к директории общего доступа
comment	описание ресурса
valid users	список пользователей, которым разрешен доступ к ресурсу
invalid users	список пользователей, которым запрещен доступ к ресурсу
read list	список пользователей с доступом к ресурсу только на чтение
write list	список пользователей с доступом к ресурсу на чтение и запись
guest ok	определяет, разрешен ли гостевой доступ
browseable	определяет видимость директории
writable	определяет можно ли записывать данные

```
[global]
workgroup = WORKGROUP
server string = Samba server %v
netbios name = Shared folders
security = user
map to guest = no

[User_x]
path = /srv/samba/user_x
comment = Userx’s folder
guest ok = no
browseable = yes
writable = yes
valid users = user_x root @group_x

[Admin]
path = /srv/samba/admin
comment = Admin’s folder
guest ok = no
browseable = yes
writable = yes
valid users = root
```

Здесь для каждой директории задается своя секция Share Definitions, в которой, помимо отключения гостевого доступа, задается список пользователей и групп, которым разрешен доступ к этому ресурсу. Перед группами нужно указывать символ @. Проверить корректность сконфигурированных параметров можно с помощью утилиты testparm из fly-терминала.

В целом, Samba DC позволяет решить задачу сетевого взаимодействия в гетерогенных сетях на базе ОС семейств Windows и Linux, в частности, создать сетевые ресурсы с общим доступом, разграничить доступ к сетевым ресурсам пользователей и групп, установить требуемый режим доступа (чтение, чтение/запись).

Список используемых источников

1. Руссинович М., Соломон Д. Внутреннее устройство Microsoft Windows. СПб. : Питер, 2013. 800 с.

2. Колисниченко Д. Н., Аллен Питер В. Linux: полное руководство. СПб. : Наука и техника, 2006. 784 с.

3. Операционная система специального назначения «Astra Linux Special Edition». Руководство администратора. Часть 1. 2018. 319 с. [Электронный ресурс]. URL: https://astralinux.ru/products/astra-linux-special-edition/documents-astra-se/rukovodstvo-administratora-chast-1-astra-se.pdf (дата обращения 18.12.2019).

УДК 004.056.55
ГРНТИ 81.93.29

ИССЛЕДОВАНИЕ СПОСОБА ПЕРЕДАЧИ КЛЮЧЕВОЙ ИНФОРМАЦИИ ПО ПОСТОЯННОМУ КАНАЛУ СВЯЗИ

М. М. Кабардов, У. М. Романова

Санкт-Петербургский государственный университет телекоммуникаций им. проф. М. А. Бонч-Бруевича

В одной из работ, представленных на заседании конференции АПИНО, описан протокол распределения ключей: «Protocol of key distribution over public noiseless channels executing without cryptographic assumptions». Сам протокол основан на вычислении легитимными участниками сеанса собственных значений случайно сгенерированных матриц. В данной работе приведены результаты исследования зависимости вероятности возникающих ошибок при уменьшении точности промежуточной записи собственных чисел. Важной частью при использовании протокола является расчет требуемого трафика для его выполнения. В этой работе также рассматривается расчет этого параметра.

схема EVSKey, протокол распределения ключей по постоянному каналу связи.

Протокол распределения ключей, основанный на схеме EVSKey (*Eigenvalue-based Secret Key* – секретный ключ на основе собственных значений), выполняет процедуры, указанные на рис. 1 [1].

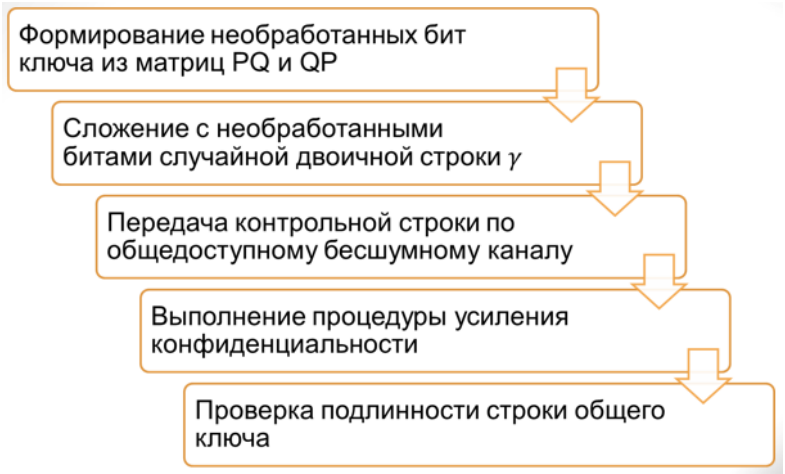


Рис. 1. Диаграмма протокола распределения ключей, основанном на схеме EVSKey

В ходе работы протокола распределения ключей на основе схемы EVSKey, представленном на рис. 2, генерируется двоичная необработанная

последовательность для дальнейшего создания общего ключа. Перед передачей Alice (A) и Bob (B) генерируют собственные матрицы $X_A, X_B \in \mathbb{C}^{n\times m}$ с независимыми элементами, распределенными согласно $CN(0,\sigma_X^2)$, а также случайные унитарные матрицы $G_A, G_B \in \mathbb{C}^{n\times n}$, где n – количество используемых антенн, m – длина сигнала.

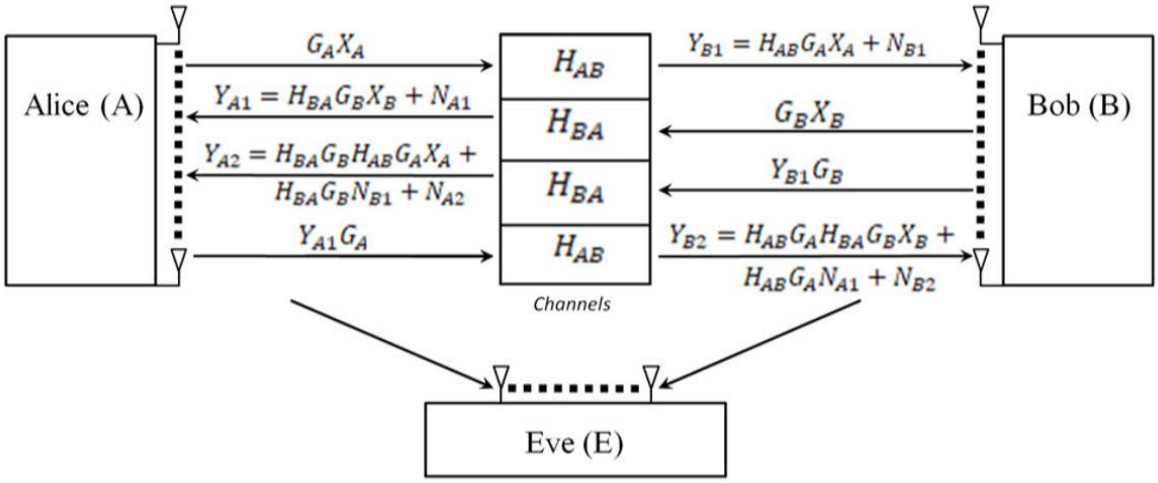


Рис. 2. Схема EVSKey

Поскольку A и B связаны постоянными бесшумными общедоступными каналами, исходные канальные матрицы H_{AB}, H_{BA} формируются участниками сеанса как случайные матрицы $(h_{ABij})_{ij}, (h_{BAij})_{ij} \sim CN(0,\sigma_W^2)$. N_{A1} и N_{B1} являются матрицами AWGN (*Additive white Gaussian noise* – аддитивный белый гауссовский шум) $(n_{A1ij})_{ij}, (n_{B1ij})_{ij} \sim CN(0,\sigma_W^2)$, соответственно сгенерированными A и B как матрицы искусственно созданных гауссовских шумов. Умножение исходных канальных матриц на соответствующие случайные унитарные матрицы дает следующие матрицы: $P = H_{BA}G_B$, $Q = H_{AB}G_A$. Тогда PQ и QP могут быть выражены участниками методом наименьших квадратов как:

$$PQ = Y_{A2}(X_A)^{-1},$$
$$QP = Y_{B2}(X_B)^{-1}.$$

Как видно по рис. 3 (см. ниже) после формирования необработанных бит из матриц PQ и QP пользователь B генерирует действительно случайную двоичную строку γ, которая суммируется по модулю два с необработанными битами K_B. Затем участник сеанса B передает строку $K_B \oplus \gamma$ по общедоступному бесшумному каналу участнику A, который добавляет эту строку к своим необработанным битам K_A, чтобы получить:

$$K_A{}' = K_B \oplus \gamma \oplus K_A = K_A \oplus \varepsilon_{AB} \oplus \gamma \oplus K_A = \gamma \oplus \varepsilon_{AB},$$

где ε_{AB} – строка дискретного шума между необработанными строками ключей K_A и K_B. Следовательно, пользователь B может повторять S раз каждый бит γ, что обеспечивает выполнение дополнительного протокола PIMC для исправления ошибок [2].

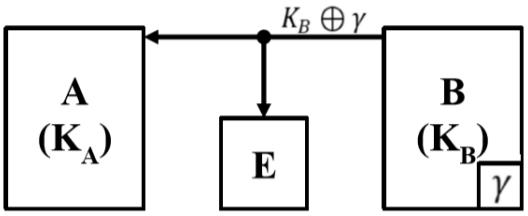


Рис. 3. Модифицированный протокол распределения ключей

Завершающим шагом протокола является аутентификация – процедура подтверждения легитимных участников сеанса. В [1] рекомендуется использование метода аутентификации, основанном на протоколе Нидхема-Шрёдера [4].

За одну итерацию генерируются матрицы размером 64×64. Вычисления проводятся в формате с плавающей запятой с двойной точностью, IEEE Standard 754. Вычисленные СЗ переводятся в формат с фиксированной запятой с заданной разрядностью в двоичной системе. Далее СЗ нумеруются, и номера переводятся в двоичный формат, что производит 384 бита. Делается 1000 итераций и битовые строки объединяются в большую 384000-битовую строку. Сравниваются строки у A и B и вычисляется относительная частота несовпадений.

От количества уровней квантования будет зависеть длина двоичной цепочки каждого передаваемого элемента матрицы и объем всего трафика, передаваемого по каналам от A к B и от B к A. Хотя собственные числа и не передаются по каналу, но они потом выделяются из матриц PQ и QP. На рис. 4 показана вероятность возникающих ошибок при уменьшении точности промежуточной записи СЗ.

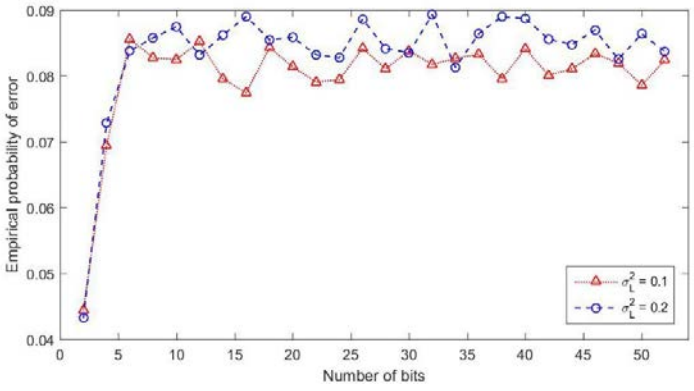


Рис. 4. График зависимости вероятности возникающих ошибок от количества бит в двоичной записи СЗ

Из рис. 4 следует, что при уменьшении точности промежуточной записи собственных чисел, вероятность возникающих ошибок почти не меня-

ется. Поэтому, далее следует проследить за изменением вероятности возникающих ошибок при уменьшении точности промежуточной записи самих элементов матриц, что показано на рис. 5.

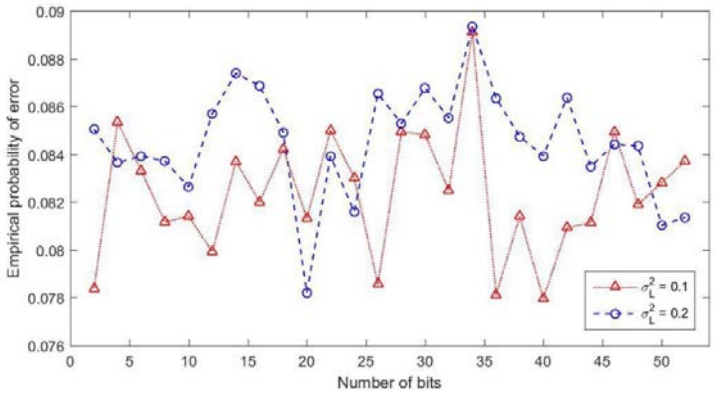


Рис. 5. График зависимости вероятности ошибок от разрядности (количества бит) элементов матриц

Из рис. 5 видно, что вероятность возникающих ошибок пренебрежимо слабо зависит от количества уровней квантования элементов матриц, но теоретически эта зависимость всегда есть.

Трафик, необходимый для описанного выше протокола, вычисляется по следующей формуле:

$$I \approx \left(8n^2 \beta S \frac{k_0}{6n(1-p)^s}\right) : 10^6 : 8 \text{ MB},$$

где S – количество итераций; k_0 – длина ключа; n – порядок матрицы, размер $n \times n$; p – вероятность возникающих ошибок у легитимных участников сеанса; β – количество бит в записи числа с фиксированной запятой. В таблице (см. ниже) приведен расчет передаваемого трафика в байтах при изменении разрядности элементов матриц, а на рис. 6 и 7 изображены графики зависимости передаваемого трафика от длины ключа, количества итераций, порядка матриц и количества уровней квантования элементов матриц.

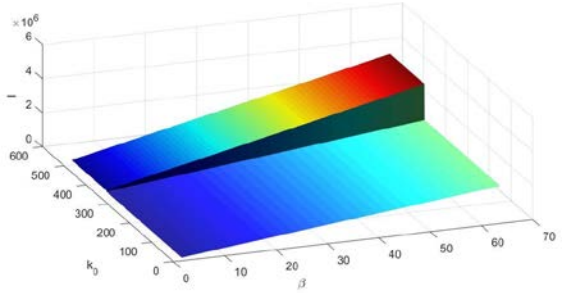


Рис. 6. График зависимости передаваемого трафика от длины ключа и количества уровней квантования элементов матриц

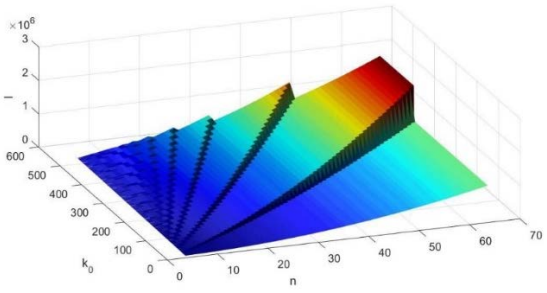


Рис. 7. График зависимости передаваемого трафика от длины ключа и порядка матриц при β = 32

ТАБЛИЦА. Передаваемый трафик при $n = 64$, $p = 0{,}08$

Кол-во бит в записи элементов матриц, β	Трафик S=3, байт			Трафик S=1, байт		
	128-битный ключ	256-битный ключ	512-битный ключ	128-битный ключ	256-битный ключ	512-битный ключ
2	24576	24576	49152	8192	8192	16384
4	49152	49152	98304	16384	16384	32768
8	98304	98304	196608	32768	32768	65536
12	147456	147456	294912	49152	49152	98304
16	196608	196608	393216	65536	65536	131072
20	245760	245760	491520	81920	81920	163840
24	294912	294912	589824	98304	98304	196608
28	344064	344064	688128	114688	114688	229376
32	393216	393216	786432	131072	131072	262144
36	442368	442368	884736	147456	147456	294912
40	491520	491520	983040	163840	163840	327680
44	540672	540672	1081344	180224	180224	360448
48	589824	589824	1179648	196608	196608	393216
52	638976	638976	1277952	212992	212992	425984

Анализ таблицы подтверждает, что трафик линейно зависит от порядка матрицы, количества бит в двоичной записи элементов матриц, количества производимых итераций и длины ключа, а также из рис. 6 видно, что трафик скачкообразно зависит от длины ключа. Это происходит потому, что биты ключа передаются «порциями». Соответственно, на рис. 7 тоже показана скачкообразная зависимость трафика от длины ключа, а также на этом рисунке видно, что размер трафика увеличивается с увеличением размера матриц.

В ходе исследования были проведены расчеты вероятности возникающих ошибок и трафика при различных условиях передачи ключевой информации по постоянному каналу связи. Результаты показали, что при уменьшении точности промежуточной записи собственных чисел, вероятность возникающих ошибок почти не меняется; вероятность возникающих ошибок пренебрежимо слабо зависит от количества уровней квантования элементов матриц; передаваемый трафик скачкообразно возрастает с увеличением длины ключа и линейно зависит от разрядности элементов матриц.

Список используемых источников

1. Коржик В. И., Яковлев В. А., Кабардов М. М., Герасимович А., Старостин В. С., Моралес-Луна Г. Информационно-теоретический безопасный протокол обмена ключами для бесшумных открытых каналов с постоянными параметрами без криптографических допущений // Материалы Федеральной конференции по компьютерным наукам и информационным системам (FedCSIS), Лейпциг (Германия), 1–4 сент. 2019. С. 361–366.

2. Коржик В. И., Моралес-Луна Г., Балакирский В. Теорема усиления конфиденциальности для основного канала с шумом // Конспект лекций в области компьютерных наук. 2001. Вып. 2200, 18–26 с.

3. Маурер У. Согласование секретного ключа путем публичного обсуждения на основе общей информации // IEEE Transactions on Information Theory. 1993. N. 39. PP. 733–742.

4. Нидхем П. М., Шрёдер М. Д. Использование шифрования для аутентификации в большой сети компьютеров». ACM. 1978. №. 21. С. 993–999.

УДК 004.421
ГРНТИ 50.41.25

КОНТРОЛЬ ПРИНИМАЕМЫХ СЕТЕВЫХ ПАКЕТОВ ЧАСТНОГО ПРОТОКОЛА С ИСПОЛЬЗОВАНИЕМ МОДУЛЯ NETFILTER УРОВНЯ ЯДРА ОС

Е. В. Каляшов, А. А. Савельева, А. В. Тарлыков

Санкт-Петербургский государственный университет телекоммуникаций им. проф. М. А. Бонч-Бруевича

В статье рассмотрен вопрос контроля сетевых пакетов при разработке частного транспортного протокола на основе ipv6. Приведены примеры решения задачи с использованием механизмов подсистемы netfilter – разработка, компиляция и установка модуля ядра. Даны примеры наиболее значимых узлов программного кода. Приведены результаты тестирования на реальном оборудовании и даны оценки для системных затрат.

протокол, фильтрация пакетов, netfilter, модуль ядра linux.

Частой задачей при разработке сетевых систем является разработка частного транспортного протокола. Достаточно распространённым вариантом является использование протокола UDP в качестве базового, но иногда требуется разработка частного транспортного протокола поверх протокола ip. В любом из этих сценариев может возникать задача контроля принимаемых по используемому протоколу сетевых пакетов, это может быть, как контроль целостности, так и фильтрация по определённому набору признаков.

В данной статье рассматривается вариант контроля принимаемых пакетов для частного протокола поверх протокола ipv6 [1]. Формат пакетов для используемого протокола приведён на рис. 1 (см. ниже). Пакеты используют стандартный фиксированный заголовок пакетов ipv6 размером 40 байт. В состав данного заголовка входит поле Next Header (NHDR

на рис. 1), которое определяет тип расширенного заголовка, расположенного следом за фиксированным заголовком ipv6. В случае используемого частного протокола присутствует единственный расширенный заголовок – заголовок, специфичный для частного протокола. Таким образом, поле Next Header содержит тип данного заголовка – в рамках статьи будет использован код 253 (диапазон 253–254 используется для экспериментов и тестирования [2]).

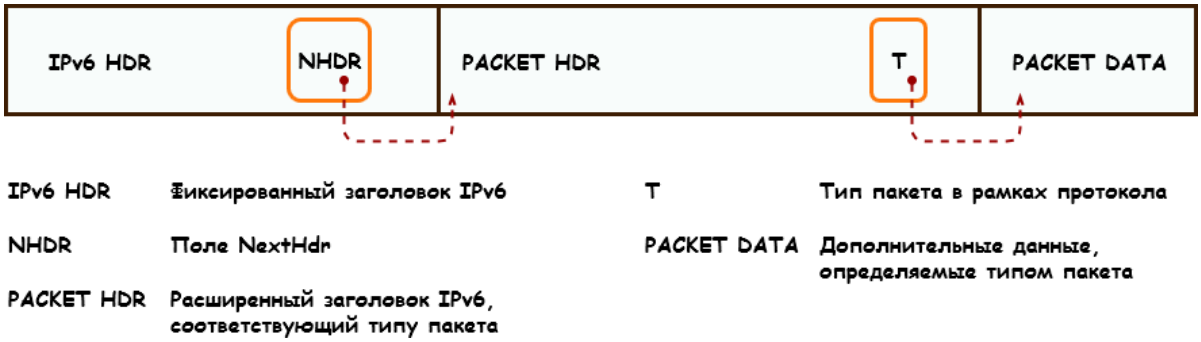


Рис. 1. Структура пакета в рамках протокола.

Детальная структура расширенного заголовка в рамках статьи является несущественной, зафиксируем размер заголовка величиной в 32 байта. Также в заголовке присутствует поле типа пакета в рамках протокола (поле T на рис. 1), пусть данное поле принимает значения от 1 до 3 для корректных пакетов. Собственно, данное поле и определяет структуру и размер хвостовой части пакета (поле PACKET DATA на рис. 1).

Разрабатываемый программный модуль netfilter [3] для контроля корректности пакетов будет выполнять следующие действия:

– контролировать пакеты разрабатываемого протокола,
– контролировать формат расширенного заголовка,
– контролировать тип пакета в рамках протокола,
– контролировать размер пакета (области данных).

В соответствие с архитектурой netfilter, прикладная система должна предоставить функцию определённого формата, получающую уведомления в процессе обработки ядром системы пакетов на разных стадиях. Подобная функция должна иметь следующую сигнатуру (рис. 2):

```
unsigned int hook_func_in(
    unsigned int hooknum,
    struct sk_buff *skb,
    const struct net_device *in,
    const struct net_device *out,
    int (*okfn)(struct sk_buff *))
{ ... }
```

Рис. 2. Сигнатура функции контроля

В рамках рассматриваемой задачи контроля пакетов, интересным является всего один параметр – *skb, указатель на буфер с данными принятого пакета [4]. Отложим пока реализацию данной функции и обеспечим её регистрацию в подсистеме netfilter, это можно выполнить следующим образом (рис. 3):

```
static struct nf_hook_ops nfho_in;
static int __init pf_module_init(void)
{
      nfho_in.hook     = (nf_hookfn*) hook_func_in;
  nfho_in.hooknum  = NF_INET_LOCAL_IN;
  nfho_in.pf       = NFPROTO_IPV6;
  nfho_in.priority = NF_IP6_PRI_FIRST;
  nf_register_net_hook(&init_net, &nfho_in);
      return 0;
}
static void __exit pf_module_exit(void)
{
    nf_unregister_net_hook(&init_net, &nfho_in);
}
module_init( pf_module_init);
module_exit( pf_module_exit);
```

Рис. 3. Инициализация модуля и регистрация функции контроля

В приведённом примере можно видеть общую структуру модуля ядра, она включает в себя функции, вызываемые при инициализации и выходе из модуля, в них и должна располагаться прикладная логика для интеграции с подсистемой netfilter. Интеграция производится с использованием специальной структуры типа nf_hook_ops [3], регистрируется функция-обработчик пакетов, настраивается её вызов для случая только принятых пакетов (NF_INET_LOCAL_IN), для пакетов типа IPV6 (NFPROTO_IPV6) и устанавливается максимальный приоритет (NF_IP6_PRI_FIRST) на случай существования нескольких обработчиков. Далее вызывается стандартная функция подсистемы netfilter для регистрации обработчика.

Реализация функции контроля пакетов также достаточно проста, не будем приводить её полностью, рассмотрим только основные моменты. Так как функция зарегистрирована для обработки пакетов ipv6, можно использовать следующий вариант для работы с фиксированным заголовком ipv6 (рис. 4):

```
struct ipv6hdr *ip6_hdr;
    ip6_hdr = (struct ipv6hdr*)(skb->data);
    if ((__u8)ip6_hdr->nexthdr != (__u8)253)
{
        return NF_ACCEPT;
    }
```

Рис. 4. Проверка типа пакета

В данном случае проводится проверка типа первого расширенного заголовка на соответствие разрабатываемому протоколу. Константа NF_ACCEPT сообщает подсистеме netfilter, что пакет является корректным и можно продолжить его дальнейшую обработку. Не будем останавливаться на структуре расширенного заголовка для рассматриваемого протокола, предположим, что его формат описан в структуре app_exthdr и содержит поле «type» с информацией о типе пакета в рамках разрабатываемого протокола. Получить и проверить тип можно следующим образом (рис. 5):

```
struct app_exthdr *ext_hdr = (struct app_ex-
thdr*)
      &(skb->data[sizeof(struct ipv6hdr)]);
  __u8 app_type = ext_hdr->type;
  if ((app_type < 1) || (3 < app_type)) {
      return NF_DROP;
  }
```

Рис. 5. Проверка типа пакета в рамках прикладного протокола

Константа NF_DROP, в данном случае, сообщает подсистеме netfilter, что пакет является некорректным и его необходимо исключить из дальнейшей обработки. Остальные проверки принятого пакета на корректность осуществляются аналогично и здесь не приводятся для экономии места.

Для компиляции сформированного таким образом модуля необходимо создать файл с названием «Makefile» следующего вида (рис. 6) [5]:

```
obj-m += appfilter.o
all:
      make -C /lib/modules/$(shell uname -r)/build
M=$(PWD) modules
clean:
      make -C /lib/modules/$(shell uname -r)/build
M=$(PWD) clean
```

Рис. 6. Пример управляющего файла для сборки модуля

Далее необходимо выполнить компиляцию модуля с использованием команды make. Результатом должен стать файл appfilter.ko, расположенный в том же каталоге. Включение и выключение модуля осуществляется командами «insmod appfilter.ko» и «rmmod appfilter».

Проверим работоспособность разработанного модуля фильтрации, будем использовать тестовый стенд с двумя серверами, оборудованными 1 GbE интерфейсами. Один сервер будет использоваться в качестве генератора, или источника, пакетов, второй – в качестве приёмника с подключённым модулем контроля. Передаваемые пакеты имеют небольшой размер и обеспечивают сетевой поток примерно 1,13 Mpps. Принимающая сторона

настроена таким образом, что обработка принимаемых пакетов осуществляется системой на одном ядре процессора, а обработка протокола – на другом. Рассмотрим два тестовых сценария:

– генерация и приём корректных пакетов,

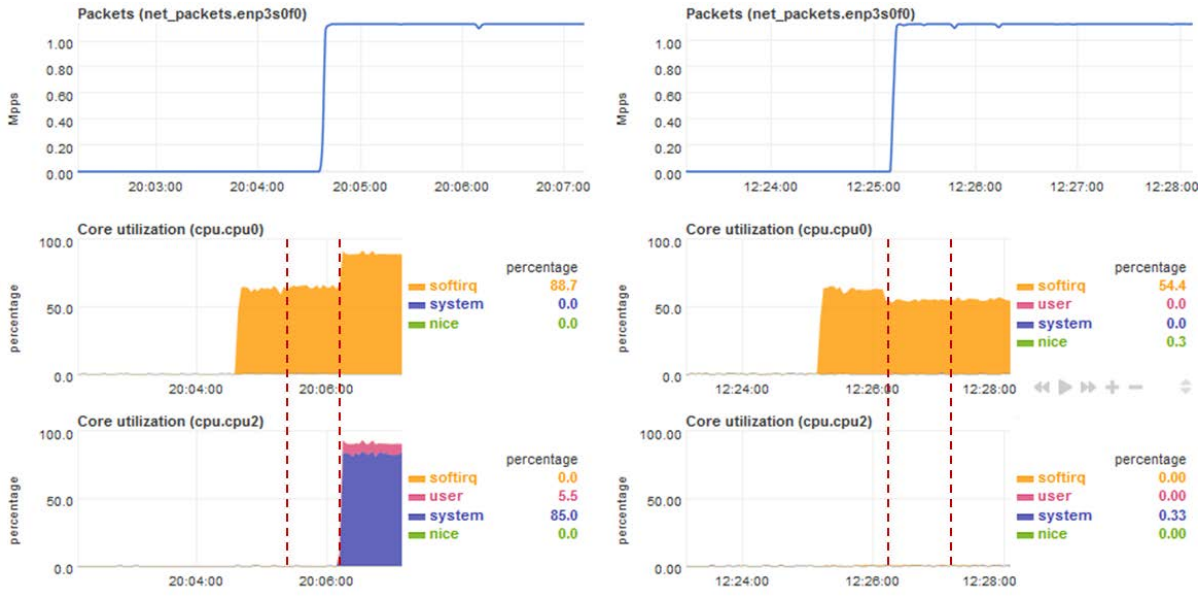
– генерация и фильтрация некорректных пакетов.

В ходе каждого сценария выделим три фазы на стороне, выделенной для приёма сетевых пакетов (рис. 7):

– приём и обработка сетевых пакетов операционной системой без разработанного модуля контроля и без приёмной части – обработчика протокола,

– подключение модуля контроля,

– подключения приёмника – обработчика протокола.



а) б)

Рис. 7. Поведение системы при использовании модуля фильтрации,
а) корректные пакеты, б) некорректные пакеты

Как видно на рис. 7а, в случае приёма корректных пакетов загрузка системы практически никак не меняется в первых двух фазах (оценка затрат на фильтрацию будет дана ниже) и вырастает при подключении приёмной части, что объясняется дальнейшей обработкой пакетов. В случае второго сценария (рис. 7б), нагрузка на систему снижается при подключении модуля фильтрации (вторая фаза), что объясняется отбрасыванием некорректных пакетов на более ранней стадии обработки. Также, во втором сценарии ничего не меняется при переходе к третьей фазе – пакеты отбрасываются модулем контроля и не попадают в обработчик протокола.

Что касается накладных расходов при использовании подобного модуля, они минимальны и не соизмеримы с затратами на приём и обработку сетевых пакетов ядром (как можно видеть на рис. 7а, загрузка системы

в процессе приёма пакетов без фильтрации достаточно высока). Максимальное время требуется для проверки корректных сетевых пакетов, в этом случае количество выполняемых проверок максимально – производится проверка всех условий до учёта пакета как корректного. В ходе исследования была проведена проверка работы модуля фильтрации с использованием тестового стенда, построенного на основе процессора Intel(R) Xeon(R) CPU L5630 4 cores @2,13GHz с использованием внешнего сетевого адаптера 1 GbE. В ходе измерений, проведённых на данном стенде, время выполнения одной итерации фильтрации составило ~4,95 нс, измерения проводились для корректных пакетов. Таким образом, для максимально возможного потока корректных пакетов в 1,13 Mpps суммарное время выполнения фильтрации можно оценить в $4{,}95 \times 1{,}13 \times 10^6$ нс или 5,6 мс в течение одной секунды, что составляет 0,56 % загрузки одного ядра процессора.

Таким образом, использование подсистемы netfilter для контроля принимаемых в рамках прикладного протокола пакетов является вполне оправданным и позволяет не только достаточно просто организовать контроль, но и обеспечить снижение системных затрат за счёт функционирования на ранней стадии обработки пакетов в сетевом стеке операционной системы.

Список используемых источников

1. IPv6 [Электронный ресурс]. Электрон. текстовые дан. 2020. Режим доступа: https://en.wikipedia.org/wiki/IPv6, свободный. Загл. с экрана. Яз. англ.

2. List of IP protocol numbers [Электронный ресурс]. Электрон. текстовые дан. 2020. Режим доступа: https://en.wikipedia.org/wiki/List_of_IP_protocol_numbers, свободный. Загл. с экрана. Яз. англ.

3. The netfilter.org project [Электронный ресурс]. Электрон. текстовые дан. 2020. Режим доступа: https://www.netfilter.org/, свободный. Загл. с экрана. Яз. англ.

4. socket buffer [Электронный ресурс]. Электрон. текстовые дан. 2020. Режим доступа: https://www.kernel.org/doc/html/latest/networking/kapi.html#c.sk_buff, свободный. Загл. с экрана. Яз. англ.

5. Building External Modules [Электронный ресурс]. Электрон. текстовые дан. 2020. Режим доступа: https://www.kernel.org/doc/Documentation/kbuild/modules.txt, свободный. Загл. с экрана. Яз. англ.

Статья представлена заведующим кафедрой ИКС СПбГУТ, кандидатом технических наук, доцентом А. А. Зарубиным.

УДК 004.421
ГРНТИ 50.41.25

ПРИЁМ IP-ПАКЕТОВ ПРОИЗВОЛЬНОГО ТИПА В JAVA С ИСПОЛЬЗОВАНИЕМ ИНСТРУМЕНТАРИЯ JNI ДЛЯ ДОСТУПА К СЕТЕВОМУ СТЕКУ ОС

Е. В. Каляшов, А. А. Савельева, А. В. Тарлыков

Санкт-Петербургский государственный университет телекоммуникаций им. проф. М. А. Бонч-Бруевича

В статье рассмотрены вопросы приёма сетевых ip-пакетов произвольного типа без использования стандартной библиотеки Java для работы с сетью. Рассмотрены вопросы работы с java native interface, интеграции с использованием технологии direct buffer и использования внешних библиотек на примере приёма ipv6 пакетов. Приведены примеры ключевых узлов программного кода.

транспортный уровень, custom ip, java, jni.

Достаточно часто в процессе реализации низкоуровневых сетевых приложений возникает задача приёма ip-пакетов различных типов, не ограничивающихся протоколами tcp и udp. Данная задача является достаточно простой для реализации при поддержке полноценного интерфейса сокетов на уровне стандартной библиотеки. В случае же использования для разработки приложения платформы Java [1], реализация подобной функциональности в стандартную библиотеку не включена.

Рассмотрим вариант реализации данной функциональности для работы в системе Linux (вариант с поддержкой нескольких систем также возможен, но требует более ёмкого описания и в рамках статьи не рассматривается). Для доступа к сетевым функциям ядра операционной системы необходимо воспользоваться возможностями специальной функциональности языка Java – java native interface [2]. Данный функционал позволяет спроектировать внешнюю библиотеку и обеспечивает прозрачный вызов функций такой библиотеки непосредственно из программы на языке Java. Таким образом, решение задачи приёма сетевых пакетов необходимо начинать с проектирования программного интерфейса библиотеки, являющейся связующим звеном между прикладной Java программной и сетевым стеком системы. В рамках рассматриваемой задачи простейшим вариантом интеграции является обеспечение доступа к стандартным функциям работы с сокетами – открытие, приём пакетов и закрытие.

Точкой интеграции со стороны Java должен выступать некий класс, в котором определяются методы, реализуемые внешней библиотекой. Объявить подобные методы в исходном коде необходимо специальным образом, с использованием модификатора native. Возможный вариант объявления приведён на рис. 1 ниже.

```
class RawSocket {
  native static int _socket(int protocol);
  native static int _close(int socket);
  native static int _receive(int socket, ByteBuffer
buffer,
                             int, int length);
  native static int _errno();
}
```

Рис. 1. Пример объявления внешних методов

В данном случае предполагается использование ipv6 сокетов типа SOCK_RAW [4] для заданного протокола, их создание и закрытие, возможность получения данные и анализа ошибок в случае возникновения.

Целевым объектом со стороны программы на Java для приёма данных будет использоваться класс ByteBuffer [5], доступный в составе стандартной библиотеки. Данный класс позволяет выделять необходимый объём памяти в так называемом режиме «direct», что выносит выделяемый буфер за пределы памяти, обслуживаемой системой сборки мусора. Буферы подобного типа являются неперемещаемыми в памяти, что упрощает и ускоряет работу с ними, в частности – с использованием внешней библиотеки. Таким образом, приём пакетов будет осуществляться в указываемую область буфера (параметр *offset*) и ограничиваться максимальным объёмом принимаемых данных (параметр *length*).

На основе определённого выше класса необходимо разработать внешнюю библиотеку с реализацией всех объявленных методов. Сделать это можно как полностью в ручном режиме, так и воспользовавшись инструментарием разработчика Java – утилитой javac [6], что сильно упрощает и ускоряет процесс разработки. Для генерации шаблона библиотеки необходимо выполнить команду следующего вида: “javac –h. RawSocket.java”. Утилита обеспечивает генерацию заголовочного файла с описанием native методов, объявленных в указываемом Java классе. Описание всех библиотечных методов включает два системных параметра и параметры, указанные при описании методов в классе Java. Например, метод приёма (для реализации в библиотеке) будет выглядеть следующим образом (рис. 2):

```
JNIEXPORT jint JNICALL Java_demo_RawSocket__1receive
  (JNIEnv *, jclass, jint, jobject, jint, jint);
```

Рис. 2 Описание метода на уровне библиотеки

Следующим шагом является реализация функций на основе сгенерированных описаний. В качестве примера рассмотрим создание сокета и приём данных через него (рис. 3):

```
JNIEXPORT jint JNICALL Java_demo__1socket
  (JNIEnv *env, jclass _class, jint protocol)
{  return socket(AF_INET6, SOCK_RAW, protocol); }

JNIEXPORT jint JNICALL Java_demo__1receive6
  (JNIEnv *env, jclass _class, jint sd, jobject buffer,
  jint offset, jint length) {
  struct sockaddr_in6 sin6;
  socklen_t socklen;

  memset(&sin6, 0, sizeof(struct sockaddr_in6));
  sin6.sin6_family = AF_INET6;
  socklen = sizeof(sin6);

  void address = (*env)->GetDirectBufferAddress(env, buffer);

  return recvfrom(sd, address + offset, length,
                  0, (struct sockaddr *)&sin6, &socklen);
}
```

Рис. 3. Пример реализации методов

Приведённый код упрощён с целью наглядности и не включает в себя обработку ошибок и поддержку дополнительных возможностей кроме прямого копирования принятого пакета в буфер приёма и возврата кода результата. Функция GetDirectBufferAddress [7], входящая в состав подсистемы java native interface [2], возвращает адрес расположения буфера в памяти для непосредственного доступа. Необходимо отметить, что данная возможность обеспечивается только для, так называемых, direct буферов. Реализация функций закрытия сокета и возврата кода ошибки не приводится в силу своей прозрачности. Скомпонованный таким образом код с реализацией всех функций необходимо скомпилировать в режиме shared библиотеки.

Для использования полученной библиотеки необходимо обеспечить её загрузку и инициализацию перед первым обращением к предоставляемым функциям. Выполнить данные действия можно путём включения блока статической инициализации в исходный Java класс (рис. 4):

```
Class RawSocket {
    static {
        System.loadLibrary("ipcimrs");
    }
```

Рис. 4. Пример загрузки библиотеки со стороны Java кода

После выполнения указанных шагов функции библиотеки становятся доступны для вызова через объявленные ранее методы исходного класса. Соответственно, в рамках рассмотренного примера, появляется возможность использования любого протокола транспортного уровня непосредственно из кода на языке Java. В приведённом примере сохранён достаточно низкоуровневый вариант работы, соответствующий вызовам сетевого стека операционной системы. В более общем случае библиотечная часть может включать в себя функции более высокого уровня, что упрощает прикладную часть кода.

Подводя итог, необходимо отметить, что использование подобного подхода позволяет достаточно быстро обеспечить приём пакетов различного типа. В тоже время, в отличие от использования сторонних библиотек, данный метод позволяет обеспечить прозрачность интеграции, что немаловажно в случае возможных неисправностей, а также – максимальную гибкость при реализации, что зачастую невозможно при использовании стороннего кода.

Список используемых источников

1. Java Language and Virtual Machine Specifications [Электронный ресурс]. Электрон. дан. 2020. Режим доступа: https://docs.oracle.com/javase/specs/index.html, свободный. Загл. с экрана. Яз. англ.

2. Java Native Interface Specification Contents [Электронный ресурс]. Электрон. дан. 2020. Режим доступа: https://docs.oracle.com/en/java/javase/13/docs/specs/jni/index.html, свободный. Загл. с экрана. Яз. англ.

3. socket - Linux socket interface [Электронный ресурс]. Электрон. дан. 2020. Режим доступа: http://man7.org/linux/man-pages/man7/socket.7.html, свободный. Загл. с экрана. Яз. англ.

4. socket - create an endpoint for communication [Электронный ресурс]. Электрон. дан. 2020. Режим доступа: http://man7.org/linux/man-pages/man2/socket.2.html, свободный. Загл. с экрана. Яз. англ.

5. Class ByteBuffer [Электронный ресурс]. Электрон. дан. 2020. Режим доступа: https://docs.oracle.com/en/java/javase/13/docs/api/java.base/java/nio/ByteBuffer.html, свободный. Загл. с экрана. Яз. англ.

6. The javac Command [Электронный ресурс]. Электрон. дан. 2020. Режим доступа: https://docs.oracle.com/en/java/javase/13/docs/specs/man/javac.html, свободный. Загл. с экрана. Яз. англ.

7. Chapter 4: JNI Functions # GetDirectBufferAddress [Электронный ресурс]. Электрон. дан. 2020. Режим доступа: https://docs.oracle.com/en/java/javase/13/docs/specs/jni/functions.html#getdirectbufferaddress, свободный. Загл. с экрана. Яз. англ.

Статья представлена заведующим кафедрой ИКС СПбГУТ, кандидатом технических наук, доцентом А. А. Зарубиным.

УДК 004.421
ГРНТИ 50.41.25

АНАЛИЗ ПРОИЗВОДИТЕЛЬНОСТИ РАЗЛИЧНЫХ РЕАЛИЗАЦИЙ QUEUE ПРИ ИСПОЛЬЗОВАНИИ ШАБЛОНА ПРОЕКТИРОВАНИЯ PRODUCER – CONSUMER

Е. В. Каляшов, А. В. Тарлыков

Санкт-Петербургский государственный университет телекоммуникаций им. проф. М. А. Бонч-Бруевича

В статье рассмотрены вопросы производительности различных вариантов реализации шаблона Producer-Consumer в задаче получения и обработки сетевых пакетов. Приведены данные производительности и загрузки системы. Представлены варианты использования различных типов очередей для разных задач обработки данных.

producer-consumer pattern, java, очереди, потоки.

Шаблон проектирования Producer – Consumer [1] представляет собой простой и эффективный способ асинхронной обработки данных. Producer (поставщик данных) генерирует данные и складывает их в очередь, Consumer (потребитель) забирает данные из очереди для последующей обработки. В общем случае поставщиков и потребителей может быть много. Схема данного шаблона приведена на рис. 1.

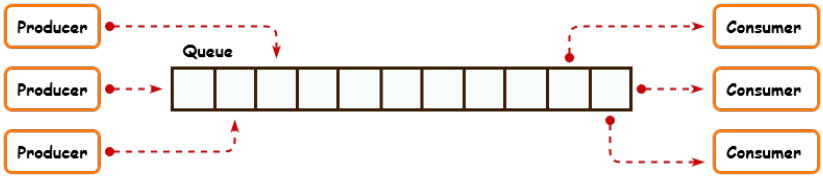


Рис. 1. Схема шаблона Producer/Consumer

В данной работе шаблон Producer – Consumer использовался в применении к задаче получения и обработки сетевых пакетов. Спецификой такой задачи является получение пакетов от одного поставщика и обработка несколькими потребителями. Для обеспечения максимально возможной производительности буферы данных выделяются в памяти один раз и затем используются многократно, ссылки на буферы с данными помещаются поставщиком в одну очередь (*used*), извлекаются из неё потребителями и, после обработки, заносятся в очередь свободных буферов, для последую-

щего использования поставщиком. В работе рассматриваются вопросы производительности такой схемы при использовании различных видов очередей.

Использовались следующие варианты реализации очередей в Java: ArrayBlockingQueue [2], SpscAtomicArrayQueue, MpscAtomicArrayQueue, SpmcAtomicArrayQueue [3]. Различалась также и организация очередей – в одних случаях на каждого потребителя создавалась пара очередей (*free* и *used*), в других эти очереди были общими для всех потребителей.

Были проведены тесты для схем 1 поставщик – 8 потребителей и 1 поставщик – 1 потребитель. В тестах использовались блокирующие вызовы take() и put(), неблокирующие вызовы poll() и offer(). Результаты тестов данной модели представлены в таблицах 1, 2. В тестах № 1, № 2, № 3 использованы ArrayBlockingQueue, в тесте № 4 – SpscAtomicArrayQueue, в тесте № 5 применена комбинация SpmcAtomicArrayQueue и MpscAtomicArrayQueue, реализующая функциональность «один ко многим» и «многие к одному».

ТАБЛИЦА 1. Производительность модели для случая 1 поставщик – 8 потребителей

№ теста	Кол-во очередей	Блокирующие вызовы	Производительность, млн итераций/сек	Загрузка CPU, %
1 (ABSCQ)	16	нет	3,1	240
2 (ABMCQ)	2	нет	2,3	170
3 (ABMCQB)	2	да	0,9	135
4 (SPSCQ)	16	нет	40,9	200
5 (SPMCQ)	2	нет	8,9	300

ТАБЛИЦА 2. Производительность модели для случая 1 поставщик – 1 потребитель

№ теста	Кол-во очередей	Блокирующие вызовы	Производительность, млн итераций/сек	Загрузка CPU, %
1 (ABSCQ)	2	нет	1,8	197
2 (ABMCQ)	2	нет	1,9	198
3 (ABMCQB)	2	да	1,9	200
4 (SPSCQ)	2	нет	28,8	200
5 (SPMCQ)	2	нет	7,1	200

В случае использования неблокирующих вызовов требуется выполнять постоянный опрос очереди до получения данных. Непрерывный опрос полностью загружает соответствующее ядро процессора, использование задержки между опросами в виде Thread.sleep() также потребляет некоторые ресурсы вследствие переключения контекста потока. В работе был использован усложненный цикл опроса, позволяющий минимизировать дополнительную загрузку процессора. В начале внутри основного цикла вводится

цикл опроса с использованием Thread.onSpinWait(), ограниченный счётчиком counter. Если в течение первичного цикла данные не появились, вводится второй внутренний цикл с использованием ожидания вида Thread.sleep(). Такой подход позволяет минимизировать накладные расходы при получении данных от очереди, пример кода представлен на рис. 2.

```
while (true) {
  Object buffer = queueUsedBuffers.poll();
  if (buffer == null) {
    int counter = 100;
    while (((buffer = queueUsedBuffers.poll()) == null) &&
           (0 < --counter)) {
      Thread.onSpinWait();
    }
    if (buffer == null) {
      while ((buffer = queueUsedBuffers.poll()) == null) {
        try { Thread.sleep(1); }
        catch (InterruptedException e) {}
      }
    }
  }

  while (!queueFreeBuffers.offer(buffer)) {
    Thread.onSpinWait();
  }
}
```

Рис. 2. Фрагмент кода, осуществляющий опрос очереди.

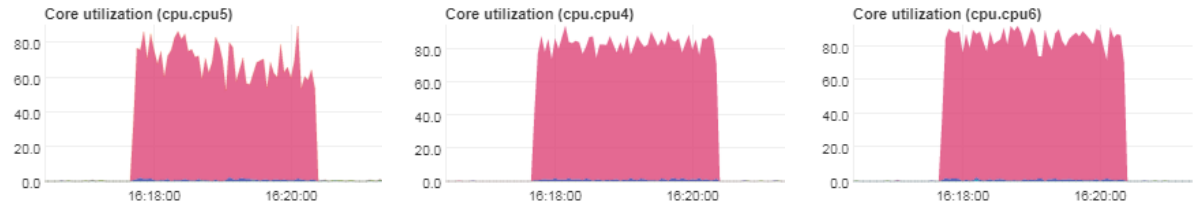
В ходе тестов был отмечен высокий разброс показаний от выборки к выборке в пределах одного теста. Разброс объясняется постоянным переключением исполняемых потоков на разные ядра процессора, что подтверждается неравномерной загрузкой ядер. Такое переключение должно в общем случае также снижать производительность модели. Для устранения подобного поведения использовалось контролируемое распределение потоков выполнения по ядрам процессора [4]. Оптимальной оказалась привязка потока поставщика к одному ядру, а потоков потребителей – к двум другим ядрам одного процессора. Разброс значений производительности в таком случае существенно снижается, отмечено также общее повышение производительности. Кроме того, в ряде тестов отмечено снижение загрузки процессора. Так, для теста № 5 загрузка процессора снизилась с 900 до 300 %. Тесты проводились на компьютере со следующими характеристиками: процессор Intel(R) Xeon(R) CPU L5630 2.13GHz, 24Gb, система Ubuntu 18.04, openjdk version "12.0.1".

Результаты, приведенные в таблице 1, демонстрируют значительный разброс как производительности, так и загрузки процессора для разных тестов. Минимальную производительность показывает тест с использованием блокирующих вызовов. Тест № 5, использующий очереди SPMC и MPSC,

показывает хорошую производительность, но и самую высокую загрузку процессора, 9 потоков полностью используют 3 выделенных ядра процессора. Наилучшее соотношение производительность / загрузка показал тест № 4, где 8 потребителей обслуживаются каждый собственной очередью.

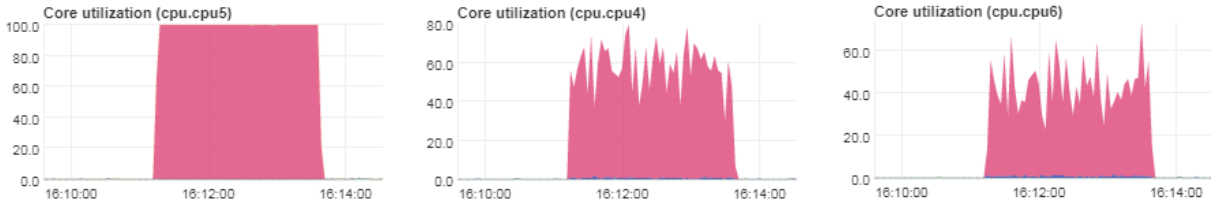
В случае схемы 1 поставщик – 1 потребитель во всех случаях загрузка процессора близка к 200 %. Выполнение происходит в 2-х потоках, которые полностью занимают 2 ядра процессора, накладные расходы на переключение потоков отсутствуют. Производительность для всех тестов, за исключением 3-го падает. Очевидно, затраты времени на блокировку в тесте № 3 при обработке 9 потоков оказываются значительными.

Загрузка процессора определялась с помощью утилиты top, также были сняты графики загрузки ядер процессора. Примеры загрузки отдельных ядер для схемы 1 поставщик – 8 потребителей представлены на рис. 3 и 4. При сравнимых загрузках производительность в тестах № 1 и № 4 различается на порядок.



a) b) c)

Рис. 3. Пример загрузки ядер процессора для теста № 1:
a) загрузка ядра поставщиком данных, b) и c) – загрузка ядер потребителями



a) b) c)

Рис. 4. Пример загрузки ядер процессора для теста № 4:
a) загрузка ядра поставщиком данных, b) и c) - загрузка ядер потребителями

Оценка влияния многократного использования буферов производилась на примере теста № 4 – наиболее производительного варианта, использующего максимальное количество буферов передачи данных. Использовалась только одна очередь передачи, каждый раз создавались новые буферы – байтовые массивы размером 256 байт. Производительность такого варианта составила 14,5 млн итераций в секунду, что почти втрое меньше производительности в случае многократного использования буферов.

По результатам приведенных тестов можно сделать следующие выводы. Наилучшим из протестированных вариантов оказался класс

SpscAtomicArrayQueue, используемый в качестве очереди. Привязка потоков выполнения к конкретным ядрам выравнивает нагрузку на процессор и повышает производительность передачи данных. При необходимости задействовать несколько потребителей обеспечение каждого потребителя своим набором очередей дает существенный выигрыш в производительности. Следует отметить, что многократное использование заранее выделенных буферов данных позволяет уменьшить накладные расходы на систему.

Список используемых источников

1. Mark Grand. Patterns in Java: A Catalog of Reusable Design Patterns Illustrated with UML, 2nd Edition, volume 1. Wiley, 2002. 544 p. ISBN-10: 9780471227298, ISBN-13: 978-0471227298. Яз. англ.

2. Class ArrayBlockingQueue<E> [Электронный ресурс]. Электрон. дан. 2020. Режим доступа: https://docs.oracle.com/javase/7/docs/api/java/util/concurrent/ArrayBlockingQueue.html, свободный. Загл. с экрана. Яз. англ.

3. JCTools [Электронный ресурс]. Электрон. дан. 2020. Режим доступа: https://github.com/JCTools/JCTools, свободный. Загл. с экрана. Яз. англ.

4. Limiting execution to certain CPUs [Электронный ресурс]. Электрон. дан. 2020. Режим доступа: https://www.gnu.org/software/libc/manual/html_node/CPU-Affinity.html, свободный. Загл. с экрана. Яз. англ.

Статья представлена заведующим кафедрой ИКС СПбГУТ, кандидатом технических наук, доцентом А. А. Зарубиным.

УДК 004.421
ГРНТИ 50.41.25

РАСПРЕДЕЛЕНИЕ ПРИКЛАДНЫХ ПОТОКОВ ВЫПОЛНЕНИЯ ПРОГРАММЫ НА ЯЗЫКЕ JAVA ПО ЯДРАМ ПРОЦЕССОРА ДЛЯ ОПТИМИЗАЦИИ ВЫПОЛНЕНИЯ В СИСТЕМЕ LINUX

Е. В. Каляшов, А. В. Тарлыков

Санкт-Петербургский государственный университет телекоммуникаций им. проф. М. А. Бонч-Бруевича

В статье рассмотрен вопрос привязки потоков выполнения программы, написанной на языке Java, к фиксированным вычислительным ядрам процессора. Приведены примеры реализации ключевых фрагментов кода с использованием инструментария java native interface. Показаны результаты, демонстрирующие эффект применения в задаче обработки сетевых пакетов.

распределение потоков, affinity, java, потоки.

Периодически, для ряда программных систем, может возникать задача контролируемого распределения потоков выполнения программы по фиксированным ядрам процессора или, в случае NUMA архитектуры, по разным процессорам. Подобная задача не представляет особой проблемы в случае доступности системных функций, но в ряде программных систем, например, таких как платформа Java [1], такой доступ отсутствует, и подобная функциональность не присутствует в стандартной библиотеке.

Иногда задача может быть решена путём использования возможностей операционной системы по ограничению процессорных ядер, доступных для выполняемой программы как единого целого, например, команда teskset [2] в операционной системе Linux. Но подобного механизма недостаточно в случае использования программой нескольких потоков выполнения с требованием чёткого распределения по отдельным или, что ещё более важно, конкретным ядрам процессора. В качестве примера подобной задачи можно привести обработку сетевых пакетов. Производительные сетевые адаптеры обычно поддерживают возможность распределения обработки входящих сетевых пакетов по нескольким аппаратным очередям. Обработчики таких очередей могут быть привязаны к конкретным фиксированным ядрам процессора для снижения накладных расходов. В данном случае оптимальным вариантом для прикладной программы является приём пакетов на том же ядре процессора, где располагается и обработчик аппаратной очереди. Также может быть полезной возможность разгрузки ядра процессора, выделенного на первичную обработку входящих пакетов, от других задач.

Для решения указанной задачи будем использовать инструментарий java native interface [3] и набор следующих системных вызовов системы Linux: sched_setaffinity, sched_getaffinity [4].

Со стороны программного кода на языке Java создадим класс Affinity и определим в нем два метода (рис. 1).

```
native static byte[] __getAffinity();
native static void   __setAffinity(byte[] affinity);
```

Рис. 1. Фрагмент кода

Методы будут оперировать битовыми масками в виде массива байт, где каждый бит определяет факт привязки текущего потока выполнения к соответствующему ядру процессора (в соответствии с системной нумерацией). Например, в случае наличия в машине 24 вычислительных ядер соответствие битов номерам ядер может аналогичным представленному в таблице 1.

ТАБЛИЦА 1. Пример битовой маски для 24 вычислительных ядер

[7 6 5 4 3 2 1 0]	[15 14 13 12 11 10 9 8]	[23 22 21 20 19 18 17 16]
байт #0	байт #1	байт #2

Удобными для использования представляются методы привязки потока выполнения не по маске, а к одному конкретному вычислительному ядру, что сильно упрощает программный код для большинства случаев. Удобным является и указание набора вычислительных ядер с использованием класса BitSet [5] из набора стандартной библиотеки Java, его использование также существенно нагляднее вариант на основе массива байт (рис. 2).

```
void setAffinity(int cpu) {
        int idxSlot = cpu >> 3;
        byte idxBit = (byte)(0x01 << (cpu & 0x7));
        byte[] mask = new byte[1 + idxSlot];
        mask[idxSlot] = idxBit;
        __setAffinity(mask);
    }
    void setAffinity(BitSet mask) {
        __setAffinity(mask.toByteArray());
    }
    BitSet getAffinity() {
        byte[] bytes = __getAffinity();
        return BitSet.valueOf(bytes);
    }
```

Рис. 2. Примеры реализации подобных методов

Реализация исходных методов на уровне jni библиотеки также достаточно прозрачна, требуется передать данные из памяти Java программы в локальную структуру и воспользоваться стандартным набором системных функций для работы с привязкой потоков. Пример реализации привязки текущего потока приведён на рис. 3.

```
JNIEXPORT void JNICALL Java_demo_Affinity__1_1setAffinity
  (JNIEnv *env, jclass _class, jbyteArray affinity)
{
    cpu_set_t mask;
    const size_t mask_size = sizeof(mask);
    CPU_ZERO(&mask);
    jbyte* elements = env->GetByteArrayElements(affinity, 0);
    uint64_t length = (uint64_t)env->GetArrayLength(affin-
ity);
    if (mask_size < length) {
        length = mask_size;
    }
    memcpy(&mask, elements, length);
    sched_setaffinity(0, mask_size, &mask);
    env->ReleaseByteArrayElements(affinity, elements, 0);
                                }
```

Рис. 3. Привязка текущего потока к набору вычислительных ядер

Отметим, что при работе с функциями привязки рекомендуется использовать не массивы байт, а соответствующие структуры (*cpu_set_t* [6]) и набор макросов CPU_* [6] из стандартной библиотеки.

```
JNIEXPORT jbyteArray JNICALL Java_demo_Affinity__1_1get-
Affinity
  (JNIEnv *env, jclass _class)
{
    cpu_set_t mask;
    const size_t mask_size = sizeof(mask);
    int res = sched_getaffinity(0, mask_size, &mask);
    if (res < 0) {
        return NULL;
    }
    jbyteArray obj = env->NewByteArray(mask_size);
    jbyte* elements = env->GetByteArrayElements(obj, 0);
    memcpy(elements, &mask, mask_size);
    env->ReleaseByteArrayElements(obj, elements, 0);
    return obj;
}
```

Рис. 4. Запрос привязанных вычислительных ядер для текущего потока выполнения

Вариант реализации библиотечной функции для определения состояния привязки текущего потока к вычислительным ядрам приведён на рис. 4. В данном случае библиотечный код с использованием функций библиотеки jni создаёт в памяти Java программы новый массив, куда и копирует результат привязки, полученный от операционной системы.

Подключение созданной таким образом библиотеки к программе на языке Java даёт возможность привязки любого потока к конкретному ядру процессора. Как упоминалось выше, данный подход позволяет повысить производительность в ряде случаев. Например, результат подобной привязки можно видеть на рис. 5 (см. ниже), где потоки-обработчики сетевой нагрузки со стороны Java программы были зафиксированы на 0м и 1м ядрах процессора, что позволило значительно повысить максимальное количество обрабатываемых пакетов в единицу времени.

Подводя итог, необходимо заметить, что задача привязки потоков выполнения программы на языке Java реализуется относительно несложно, хотя и требует разработки внешней библиотеки. Но необходимо помнить, что подобное распределение потоков выполнения программы по вычислительным ядрам снижает гибкость системы, возможно возникновение ситуаций с перегрузкой одних частей системы и неполным использованием других. Автоматическая балансировка нагрузки в подобных сценариях работать не будет, единственным решением является постоянный мониторинг системы. Тем не менее, данный подход может существенно повысить производительность системы в ряде задач и пренебрегать им не стоит.

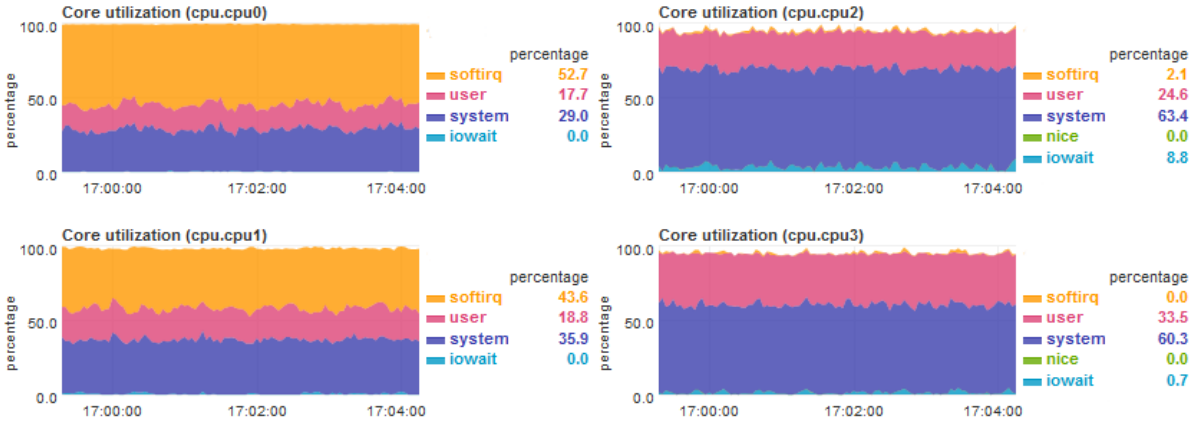


Рис. 5. Пример фиксации потоков Java программы на вычислительных ядрах, выделенных для обработки сетевых потоков

Список используемых источников

1. Java Language and Virtual Machine Specifications [Электронный ресурс]. Электрон. дан. 2020. Режим доступа: https://docs.oracle.com/javase/specs/index.html, свободный. Загл. с экрана. Яз. англ.

2. taskset – set or retrieve a process's CPU affinity [Электронный ресурс]. Электрон. дан. 2020. Режим доступа: http://man7.org/linux/man-pages/man1/taskset.1.html, свободный. Загл. с экрана. Яз. англ.

3. Java Native Interface Specification Contents [Электронный ресурс]. Электрон. дан. 2020. Режим доступа: https://docs.oracle.com/en/java/javase/13/docs/specs/jni/index.html, свободный. Загл. с экрана. Яз. англ.

4. Limiting execution to certain CPUs [Электронный ресурс]. Электрон. дан. 2020. Режим доступа: https://www.gnu.org/software/libc/manual/html_node/CPU-Affinity.html, свободный. Загл. с экрана. Яз. англ.

5. Class BitSet [Электронный ресурс]. Электрон. дан. 2020. Режим доступа: https://docs.oracle.com/en/java/javase/13/docs/api/java.base/java/util/BitSet.html, свободный. Загл. с экрана. Яз. англ.

6. CPU_SET, CPU_CLR, CPU_ISSET, CPU_ZERO, CPU_COUNT, CPU_AND, CPU_OR, CPU_XOR, CPU_EQUAL, CPU_ALLOC, CPU_ALLOC_SIZE, CPU_FREE, CPU_SET_S, CPU_CLR_S, CPU_ISSET_S, CPU_ZERO_S, CPU_COUNT_S, CPU_AND_S, CPU_OR_S, CPU_XOR_S, CPU_EQUAL_S – macros for manipulating CPU sets [Электронный ресурс]. Электрон. дан. 2020. Режим доступа: http://man7.org/linux/man-pages/man3/CPU_SET.3.html, свободный. Загл. с экрана. Яз. англ.

Статья представлена заведующим кафедрой ИКС СПбГУТ, кандидатом технических наук, доцентом А. А. Зарубиным.

УДК 004.421
ГРНТИ 50.41.25

СНИЖЕНИЕ НАКЛАДНЫХ РАСХОДОВ НА ПРИЁМ СЕТЕВЫХ ПАКЕТОВ В JAVA С ИСПОЛЬЗОВАНИЕМ ГРУППОВОГО ПРИЁМА И ИСКЛЮЧЕНИЕМ ДОПОЛНИТЕЛЬНОГО КОПИРОВАНИЯ

Е. В. Каляшов, А. В. Тарлыков, А. А. Швидкий

Санкт-Петербургский государственный университет телекоммуникаций им. проф. М. А. Бонч-Бруевича

В статье рассмотрен вопрос оптимизации приёма сетевых пакетов без использования стандартной библиотеки Java для работы с сетью. Рассмотрены способы повышения быстродействия путём использования интерфейса для получения нескольких пакетов с использованием одного системного вызова, исключения промежуточного копирования принимаемых пакетов. Приведены примеры ключевых частей программного кода.

приём пакетов транспортного уровня, java, jni.

При реализации сетевых приложений на языке Java [1] могут встать проблемы приёма большого объёма пакетов транспортного уровня. Стандартная библиотека языка предоставляет возможность получения пакетов типа UDP, что обычно является достаточным для большинства приложений. Тем не менее, может возникнуть необходимость приёма пакетов других типа, например – специфичных для разрабатываемого приложения. Также, вследствие структуры интерфейса стандартной библиотеки, приём UDP пакетов сопровождается промежуточным копированием принимаемых данных – с использованием системного вызова производится приём пакета в промежуточный буфер, затем данные копируются в пространство памяти виртуальной машины, где они становятся доступными прикладной программе. В случае приёма большого объёма пакетов данное копирование привносит заметные накладные расходы. Третьим моментом является использование стандартной библиотекой отдельного системного вызова для получения каждого пакета, что также сильно сказывается на загрузке системы. Решение перечисленных проблем может заключаться в использовании внешних библиотек, но подобную задачу можно решить и без их использования, что позволяет минимизировать количество потенциальных проблем при использовании внешнего кода.

Рассмотрим один из вариантов решения перечисленных выше проблем без использования сторонних решений и библиотек. Для реализации будем использовать доступ к стандартным функциям сетевого стека операционной системы с использованием инструментария java native interface [2].

Система предоставляет системный вызов recvmmsg [3], предназначенный для получения набора сетевых пакетов за одно обращение к сетевому стеку. Вызов принимает в качестве параметров описание приёмного буфера для пакетов и ограничение на количество возвращаемых пакетов. Рассмотрим этот вопрос более подробно. Будем использовать протокол ipv6 в качестве основы и предположим, что принимаемые в рамках разрабатываемого протокола пакеты ограничены размером 128 байт без учёта заголовка ipv6. Максимальное количество принимаемых за один вызов пакетов ограничим значением 16. Приёмный буфер будет иметь следующую структуру:

```
[СЛОТ0 | СЛОТ1 | . . . | СЛОТ16]
```

где каждый элемент «СЛОТ» предназначен для размещения одного принятого пакета и содержит две последовательные области данных:

```
[ОПИСАТЕЛЬ | ПРИНЯТЫЕ ДАННЫЕ]
```

Размер области «ПРИНЯТЫЕ ДАННЫЕ» соответствует указанному выше размеру в 128 байт, а размер области «ОПИСАТЕЛЬ» составит 32 байта и будет включать информацию о соответствующем пакете, включая его размер в байтах. Таким образом, совокупный размер буфера для одновременного приёма до 16 пакетов составит $(32 + 128) \times 16 = 2560$ байт.

Со стороны приёмной части на языке Java в качестве буфера будет выступать экземпляр стандартного класса ByteBuffer [4], создаваемый в режиме direct с использованием следующей операции: ByteBuffer.allocateDirect(2560). Подобный режим гарантирует, что буфер будет создан вне области памяти, контролируемой системой сборки мусора, и его положение в памяти будет фиксированным, что упрощает и ускоряет работу с ним. В частности, данный режим позволяет получить адрес буфера для обращения из внешней библиотеки, разработанной с использованием java native interface. Для этого может быть использована стандартная функция GetDirectBufferAddress [5].

Рассмотрим более подробно реализацию функции получения пакетов. Со стороны прикладной программы на языке Java функция может быть объявлена следующим образом (рис. 1, см. ниже).

Функция принимает в качестве параметров целевой буфер для размещения принимаемых пакетов и размер слота, как описано выше.

```
native static int _recvmmsg(
    int socket,
    ByteBuffer buffer,
    int slotSize);
```

Рис. 1. Пример объявления внешних методов

Со стороны библиотечной части потребуется описать указанный выше формат буфера в соответствие с требованиями функции recvmmsg [3, 6]. Это потребует создания двух массивов со следующими структурами, описывающими местоположение и ограничения для каждого принимаемого пакета (рис. 2):

```
struct mmsghdr headers[16];
struct iovec   messages[16];
memset(headers, 0, sizeof(struct mmsghdr) * 16);
memset(messages, 0, sizeof(struct iovec) * 16);
```

Рис. 2. Системные структуры для задания конфигурации приёма

Структуры-описатели должны быть настроены следующим образом (рис. 3):

```
void *address  = (*env)->GetDirectBufferAddress(env,
buffer);
for (int i = 0; i < 16; i++) {
    uint64_t slot_base = i*_slotSize;
    messages[i].iov_base = address + slot_base + 32;
    messages[i].iov_len = slotSize - 32;
    headers[i].msg_hdr.msg_iov = &messages[i];
    headers[i].msg_hdr.msg_iovlen = 1;
    headers[i].msg_hdr.msg_name = address + slot_base;
    headers[i].msg_hdr.msg_namelen = 32;
}
```

Рис. 3. Конфигурация для приёма пакетов

В данном случае указывается адрес памяти для размещения принимаемых данных (*iov_base*) и ограничение на размер (*iov_len*), далее формируется описатель размещения служебной информации (*msg_hdr.msg_name*) – области, выделенной в начале каждого слота буфера. Описатель соответствует структуре sockaddr_in6 [7] и имеет размер 28 байт.

Далее необходимо произвести вызов функции приёма пакетов, передав её подготовленные описатели для размещения принимаемых данных (рис. 4, см. ниже).

Параметр MSG_WAITFORONE [3] определяет режим работы – в случае отсутствия принятых пакетов выполнение функции будет заблокиро-

вано до появления следующего пакета, но, если на момент вызова присутствуют принятые пакеты, они будет возвращены сразу же. Далее необходимо проанализировать возвращаемое значение (количество принятых пакетов) и перенести в служебную часть каждого слота буфера информацию о размере пакета в слоте (рис. 5).

```
int recv_number = recvmmsg(
    sd, headers, maxPackets, MSG_WAITFORONE, NULL);
```

Рис. 4. Настройка параметров приёма

```
for (int i = 0; i < recv_number; i++) {
  uint64_t slot_base = i*slotSize;
  *(int32_t*)(address + slot_base + 28) = head-
ers[i].msg_len;
}
```

Рис. 5. Сохранение размера для всех принятых пакетов

Таким образом, мы получили достаточно простую реализацию функции приёма сетевых пакетов, лишённую многих недостатков исходного решения на уровне стандартной библиотеки языка. Необходимо отметить, приведённый пример сознательно упрощён с целью наглядности и минимизации размера. Рабочий вариант решения должен поддерживать буферы различного размера и слоты различной структуры. Тем не менее, представленный вариант является вполне работоспособным и обеспечивает решение основной озвученной в начале статьи задачи – уменьшение накладных расходов на приём каждого пакета.

Список используемых источников

1. Java Language and Virtual Machine Specifications [Электронный ресурс] // Электрон. дан. 2020. Режим доступа: https://docs.oracle.com/javase/specs/index.html, свободный. Загл. с экрана. Яз. англ.

2. Java Native Interface Specification Contents [Электронный ресурс] // Электрон. дан. 2020. Режим доступа: https://docs.oracle.com/en/java/javase/13/docs/specs/jni/index.html, свободный. Загл. с экрана. Яз. англ.

3. recvmmsg - receive multiple messages on a socket [Электронный ресурс] // Электрон. дан. 2020. Режим доступа: http://man7.org/linux/man-pages/man2/recvmmsg.2.html, свободный. Загл. с экрана. Яз. англ.

4. Class ByteBuffer [Электронный ресурс] // Электрон. дан. 2020. Режим доступа: https://docs.oracle.com/en/java/javase/13/docs/api/java.base/java/nio/ByteBuffer.html, свободный. Загл. с экрана. Яз. англ.

5. Chapter 4: JNI Functions # GetDirectBufferAddress [Электронный ресурс] // Электрон. дан. 2020. Режим доступа: https://docs.oracle.com/en/java/javase/13/docs/specs/jni/functions.html#getdirectbufferaddress, свободный. Загл. с экрана. Яз. англ.

6. recv, recvfrom, recvmsg – receive a message from a socket [Электронный ресурс] // Электрон. дан. 2020. Режим доступа: http://man7.org/linux/man-pages/man2/recvmsg.2.html, свободный. Загл. с экрана. Яз. англ.

7. ipv6 – Linux IPv6 protocol implementation [Электронный ресурс] // Электрон. дан. 2020. Режим доступа: http://man7.org/linux/man-pages/man7/ipv6.7.html, свободный. Загл. с экрана. Яз. англ.

Статья представлена заведующим кафедрой ИКС СПбГУТ, кандидатом технических наук, доцентом А. А. Зарубиным.

УДК 004.421
ГРНТИ 50.41.25

ФИКСАЦИЯ ТРЕКОВ С ИСПОЛЬЗОВАНИЕМ LOCATION API И SENSOR FRAMEWORK СИСТЕМЫ ANDROID

Е. В. Каляшов, А. В. Тарлыков, А. А. Швидкий

Санкт-Петербургский государственный университет телекоммуникаций им. проф. М. А. Бонч-Бруевича

В статье рассмотрены возможности использования комплекта датчиков современных смартфонов для записи треков движения объекта. Приведены оценки достижимой точности данных. Представлены примеры использования Android Location API и sensor framework для работы с датчиками. Предложены варианты комплексного использования данных с различных датчиков для повышения качества фиксации треков.

трек, Android, Location API, sensor framework.

Информация о перемещениях объекта может иметь ценность в приложении к определению качества автомобильных дорог, разработке логистических рекомендаций, оздоровительных и рекламных целях и т. п. Определение траектории движения требует данных о координатах и скорости объекта в трёх измерениях. Для оценки качества дорог дополнительно требуются данные об ускорениях и поворотах объекта. Для логистических исследований необходимы временные метки в каждой точке траектории. Запись всех вышеупомянутых наборов данных позволяет получить трек движения объекта, последующая обработка которого дает возможность выделять интересующую информацию.

Уровень развития современных мобильных устройств (смартфонов, планшетов) позволяет использовать их в качестве приборов фиксации тре-

ков для определённого круга задач. Современные смартфоны оснащены значительным количеством разнообразных датчиков. В массовых моделях присутствуют акселерометр, гироскоп, датчик GPS-координат. Многие модели оснащены также магнитометром и барометром. Точность данных, получаемых от этих датчиков, вполне достаточна для решения многих прикладных задач. Оценка диапазонов измерений и чувствительности разных типов датчиков приведена на примере смартфона Nexus 5 (табл. 1).

ТАБЛИЦА 1. Датчики смартфона Nexus 5

Тип измерения	Чип	Диапазон	Чувствительность	Примечание
GPS	Qualcomm WTR1605L	–	8 м	Может быть улучшена на новой элементной базе
Акселерометр	MPU-6515	±16 g	0,59 мм/с^2	
Гироскоп	MPU-6515	± 2000 град/сек	0,007 град/сек	
Магнитометр	AK8963	± 4800 μT	0,6 μT	Напряжённость магнитного поля Земли: 25–65 μT
Барометр	BMP280	30–1100 hPa	0,12 hPa	Приведена относительная чувствительность, абсолютная: ~ ±1 hPa

Можно отметить, например, что акселерометр смартфона может быть использован для регистрации сейсмической активности. Так, пиковое ускорение грунта при землетрясении интенсивностью 1 балл составляет 0,44 см/с^2 [1]. Чувствительность барометра 0,12 hPa эквивалентна изменению высоты ±1метр [2]. При этом барометр не подвержен вибрациям, имеет малый температурный дрейф, а дрейф вследствие погодных условий имеет низкую частоту, и эквивалентен нескольким метрам в час [3]. Данные же изменения высоты движущегося объекта находятся во временном диапазоне нескольких минут. Таким образом, использование фильтра верхних частот позволяет достаточно просто выделить их значения из показаний барометра.

Для взаимодействия со встроенными датчиками в системе Android используются Location API [4] и sensor framework [5]. Данные позиционирования предоставляются датчиком глобальных навигационных спутниковых систем – GPS, ГЛОНАСС, BeiDou и т. п., доступ к которому обеспечивает Location API. Для регистрации датчика GPS сначала необходимо создать объект класса GoogleApiClient, затем с его использованием зарегистрировать объект-слушатель, который будет получать изменения данных позиционирования (рис. 1).

```
GoogleApiClient api =
  new GoogleApiClient.Builder(context).
  addApi(LocationServices.API).
  addConnectionCallbacks(connectionCallback).
  build();
LocationServices.FusedLocationApi.
    requestLocationUpdates(
      api, locationRequest, locListener);
```

Рис. 1. Пример регистрации датчика GPS.

В данном случае connectionCallback – объект класса GoogleApiClient.ConnectionCallbacks, обеспечивающий необходимую логику при подключении к датчику GPS, locationRequest – объект, содержащий набор параметров для получения данных, locListener – объект-слушатель, реализующий метод-обработчик событий позиционирования (рис. 2).

```
void onLocationChanged(Location loc) {...}
```

Рис. 2. Фрагмент кода

Доступ к датчикам других типов производится с использованием объекта класса SensorManager, предоставляемого системой Android. Получение данных от других датчиков обеспечивается регистрацией в системе специального объекта для требуемого датчика (рис. 3).

```
sensorManager.registerListener(
    listener,
    sensorManager.
        getDefaultSensor(Sensor.TYPE_ACCELEROMETER),
    samplingPeriodUs,
    maxReportLatencyUs);
```

Рис. 3. Фрагмент кода регистрации акселерометра

Где listener – это и есть объект-слушатель, в котором, при возникновении событий, будет вызываться метод onSensorChanged с указанием нового значения. Параметр samplingPeriodUs определяет время между последовательными опросами датчика в микросекундах, может также задаваться предопределёнными константами вида SENSOR_DELAY_* класса SensorManager. Параметр samplingPeriodUs определяет максимальную задержку события системой до передачи приложению и, в общем случае, выставляется в нуль. Для фиксации треков, кроме акселерометра, рекомендуется зарегистрировать гироскоп, магнитометр и датчик давления.

В Sensor API существуют также виртуальные датчики типов TYPE_GRAVITY и TYPE_LINEAR_ACCELERATION, позволяющие получать раздельно составляющую, соответствующую проекции вектора ускорения свободного падения и линейное ускорение смартфона по трём осям. Но в ряде случаев такие датчики выдают некорректные данные, например,

величина полученного вектора ускорения свободного падения оказывается не равна 9,81 м/с^2. Вместо использования этих типов датчиков, вектор гравитации и линейное ускорение могут быть вычислены по исходным данным акселерометра с использованием фильтрации (рис. 4).

```
gravity = A×gravity + (1 – A)×values;
linear_acceleration = values – gravity;
```

Рис. 4. Пример вычисления

Здесь gravity – вектор ускорения свободного падения, linear_acceleration – вектор ускорения объекта за вычетом gravity, A – константа, определяемая частотой среза фильтра низких частот, может быть вычислена по формуле:

$$A = \text{timeConstant} / (\text{timeConstant} + dt),$$

где *dt* – время между соседними событиями, приходящими с датчика. При timeConstant = 0,2 (частота среза 5 Гц) и *dt* = 0,02 вычисленное значение A равняется 0,91.

Следует отметить, что повышенная частота опроса датчиков приводит к повышенному расходу батареи смартфона, поэтому разумно выставлять частоту опроса в соответствии с задачей. Для фиксации трека идущего человека достаточно значение SENSOR_DELAY_NORMAL, в то время как трек автомобиля при проезде участков с нарушением дорожного покрытия может содержать повышенные частоты в спектре ускорений. На примере смартфона Nexus 5, частота опроса акселерометра имеет следующие значения, представленные в таблице 2.

ТАБЛИЦА 2. Частота событий от акселерометра

Тип опроса	Частота, событий/сек.
SENSOR_DELAY_NORMAL	14
SENSOR_DELAY_UI	16
SENSOR_DELAY_GAME	50
SENSOR_DELAY_FASTEST	200

Частота событий от GPS датчика существенно меньше, рекомендации для разработчиков предлагают устанавливать период опроса в несколько секунд для сценариев реального времени и несколько минут для фоновых сценариев. Для фиксации треков оказывается приемлемым период в одну секунду. Таким образом, встаёт задача совмещения данных трека от различных датчиков. Эта задача решается аппроксимацией данных от датчиков на временной сетке, соответствующей максимальной частоте опроса (или на более высокой частоте, кратной максимальной частоте).

При фиксации трека базовые величины положения и скорости определяются при помощи GPS датчика. Данные акселерометра могут уточнять показания скорости на малых промежутках времени. Положение смартфона определяется по вектору гравитации, дополнительные координаты определяются с помощью данных магнитометра. Изменения углов поворота смартфона могут корректироваться показаниями гироскопа на малых промежутках времени. При интегрировании показания гироскопа и акселерометра дают ошибку, возрастающую с течением времени, и не могут быть напрямую использованы для определения углов поворота, скорости и пройденного расстояния. Но с коррекцией этих данных по показаниям GPS и магнитометра учёт показаний гироскопа и акселерометра могут повысить точность фиксации трека. Учёт показаний барометра с фильтрацией погодных изменений позволяет учитывать изменения высоты трека – детектирование смены этажа, проезд по эстакадам, резкие подъёмы и спуски.

Подводя итог, можно сделать вывод, что современный уровень развития смартфонов позволяет использовать их в качестве приборов для записи треков перемещения объектов. Результирующая точность фиксации треков оказывается вполне удовлетворительной, позволяя в ряде применений избежать использования специализированных технических комплексов.

Список используемых источников

1. ГОСТ Р 57546-2017 Землетрясения. Шкала сейсмической интенсивности [Электронный ресурс]. Режим доступа: http://docs.cntd.ru/document/1200146265, свободный. Загл. с экрана. Яз. рус.

2. Hypsometric equation [Электронный ресурс]. Электрон. текстовые дан. 2019. Режим доступа: https://en.wikipedia.org/wiki/Hypsometric_equation, свободный. Загл. с экрана. Яз. англ.

3. Using Mobile Phone Barometer for Low-Power Transportation Context Detection [Электронный ресурс]. Электрон. текстовые дан. 2014. Режим доступа: http://sensys.acm.org/2014/papers/p191-sankaran.pdf, свободный. Загл. с экрана. Яз. англ.

4. Location and context overview [Электронный ресурс]. Электрон. текстовые дан. 2020. Режим доступа: https://developer.android.com/training/location, свободный. Загл. С экрана. Яз. англ.

5. Sensors Overview [Электронный ресурс]. Электрон. текстовые дан. 2020. Режим доступа: https://developer.android.com/guide/topics/sensors/sensors_overview, свободный. Загл. с экрана. Яз. англ.

Статья представлена заведующим кафедрой ИКС СПбГУТ, кандидатом технических наук, доцентом А. А. Зарубиным.

УДК 654.152
ГРНТИ 49.33.29

МЕТОД РАСЧЁТА ПРЕДЕЛЬНОЙ ПРОТЯЖЁННОСТИ КАБЕЛЬНОГО ТРАКТА «ДЛИННОГО» ETHERNET

Е. В. Кандзюба

Московский технический университет связи и информатики

Рассмотрен метод расчёта предельной протяжённости кабельного тракта «длинного» Ethernet на основании нормативных параметров, действующих стандартов. Показана возможность расчёта характеристик кабеля, предназначенного для широкополосной передачи цифрового сигнала, на основании вычислений для одной частоты. Определяющая частота для трапециевидного сигнала, описанного в стандарте ANSI X3.263-1995, равна 31,25 МГц.

кабельный тракт, Long Ethernet, переходная помеха, уровень сигнала, сетевой интерфейс.

Внедрение современных цифровых решений невозможно без информационно-телекоммуникационных систем (ИТС), физический уровень которых построен на базе структурированной кабельной системы (СКС) [1].

Задачи, возникающие при передаче данных посредством IP-телефонии и IP-видеонаблюдения [2] успешно решаются сетями на основе Fast Ethernet. Однако появление множества новых разновидностей устройств, подключаемых посредством Fast Ethernet, не привело к изменению стандартов 1995 года в части 100BASE-TX [3], архитектурным фундаментом которых являлась кампусная модель организации СКС.

Самым простым и экономически целесообразным способом увеличения радиуса покрытия ИТС, одновременно повышающая эффективность его использования, является наращивание длины симметричного кабеля [4].

Однако отсутствие инженерных методов расчёта предельной протяжённости L кабельного тракта затрудняет внедрение кабельных трактов «длинного» Ethernet. Решение этой задачи на основании теории Шеннона [2], не может считаться полным из-за отсутствия, рекомендованного IEEE или хотя бы общепризнанного коэффициента запаса, учитывающего не 100-процентную утилизацию предельной пропускной способности в реальных условиях.

Метод, предложенный в данной работе, свободен от указанного недостатка и сформулирован, исходя из следующих положений:

– учитывая стационарный характер большинства терминальных устройств различных систем, кабельный тракт «длинного» Ethernet построен по схеме direct connection (рис. 1). Для связи сетевых устройств применён типовой сетевой интерфейс IEEE 802.3u [3] или Fast Ethernet;

– для структур direct connection характерны малые длины коммутационных шнуров, что при L > 100 метров позволяет отказаться от отдельного учёта отличия электрической и физической длин тракта;

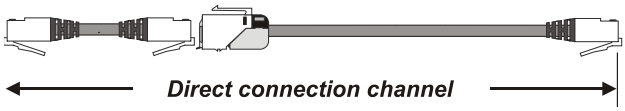


Рис. 1. Структура тракта direct connection

– сетевые интерфейсы Fast Ethernet работают в базовой полосе, верхняя граничная частота которой не превышает 100 МГц, что даёт возможность не учитывать отличие рабочего затухания от характеристического.

Суть метода заключается в нахождении простой зависимости мощности широкополосного сигнала на входе приёмника сетевого интерфейса от мощности одночастотного сигнала.

Длина тракта L задаётся отношением сигнал-шум. Качественная передача информации в сети Fast Ethernet обеспечивается при отношении, равном 21,6 дБ. Мощность шума для тракта категории 5e определяется переходной помехой на ближний конец и рассчитывается по известной модели IEEE единожды. Предельное значение L находится решением уравнения:

$$p_r(L) - p_{NEXT} = 21{,}6, \text{ дБ}, \quad (1)$$

где p_r – уровень сигнала на входе приемника сетевого интерфейса; p_{NEXT} – уровень мощности переходного шума на ближний конец.

При передаче последовательности 10101010 спецификация ANSI X3.263-1995 [5] нормирует сигнал интерфейса на входе в линию как комбинацию трапециевидных импульсов амплитудой 1 В и длительностью T = 1/125 МГц = 8 нс, измеренной на уровне ±0,5 В. Фронт сигнала равен 3 нс.

Дальнейший анализ выполняется целью выяснения работы приёмника в наиболее жёстких условиях работы. При этом на вход приёмника поступает последовательность 0101, что соответствует режиму ожидания Idle в кодировке 4B5B.

Эпюра такого сигнала приведена на рис. 2 (см. ниже), а в таблице (см. ниже) указаны ее узловые точки, что позволяет определить сигнал как кусочно-линейную функцию $F(t)$ с периодом T = 32 нс.

Мощность входного сигнала при 100-омной нагрузке находится как:

$$G_T = \frac{1}{100*T}\int_0^T F(t)^2 dt = 4{,}38, \text{ мВт}. \quad (2)$$

ТАБЛИЦА. Временные соотношения входного сигнала

Номер точки	1	2	3	4	5	6	7
Время, нс	0	2,5	5,5	10,5	13,5	18,5	32
Амплитуда, В	0	0	1	1	0	0	0

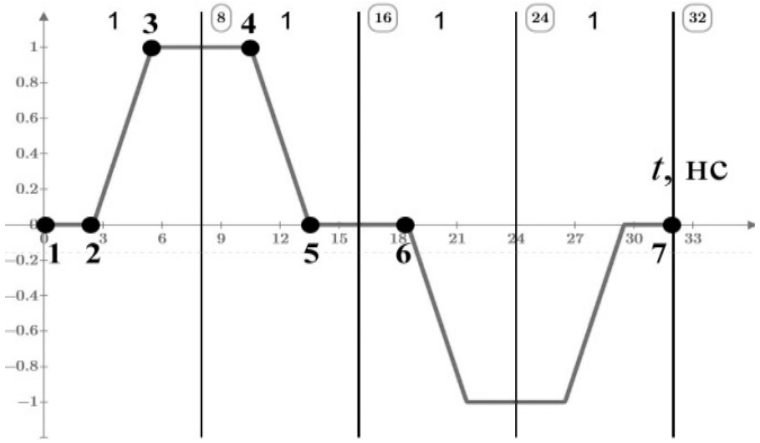


Рис. 2.Эпюра входного сигнала

Считая $F(t)$ нечётной функцией времени, определим её спектр с учётом рис. 1 как [6]:

$$\mathcal{F}(\omega) = \int_0^T F(t) * \sin(\omega * t)\, dt.$$

$\mathcal{F}(\omega)$ (рис. 3), имеет максимум на частоте 31,25 МГц при бесконечной последовательности сигналов (рис. 2). Эта частота принимается как определяющая широкополосный сигнал в дальнейшем анализе.

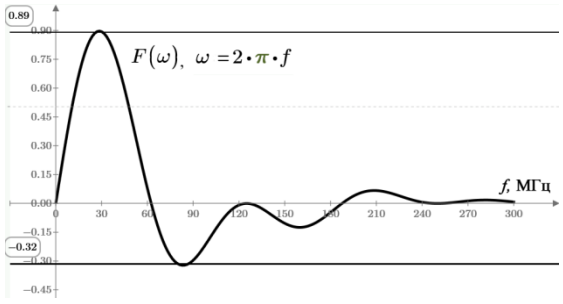


Рис. 3. Спектральная плотность $F(t)$

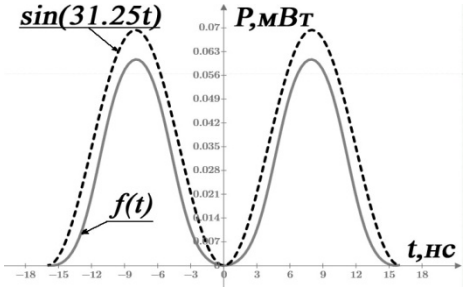


Рис. 4. Мгновенная мощность сигнала и синусоиды на выходе кабельного тракта

Возможность такого перехода определяется наличием однозначной связи между импульсным и синусоидальным сигналами на выходе тракта, рис. 4.

Коэффициент передачи тракта (рис. 1), равен:

$$K = 10^{-\alpha(f)\frac{L}{100}}, \text{ где} \qquad \alpha(f) = a\sqrt{f} + bf + d\sqrt{f},$$

а коэффициенты *a*, *b*, *d* определены стандартом ISO/IEC 11801 [7].

Введём функцию:

$$G(L) = \frac{G_{\sin}(L)}{G_{rec}(L)}, \quad (3)$$

где

$$G_{rec}(L) = \frac{2}{100 \cdot T \cdot \pi} \int_0^{\infty} \left(\mathcal{F}(\omega) 10^{-0{,}05 \cdot \alpha\left(\frac{\omega}{2\pi}\right) \cdot L} \right)^2 d\omega,$$

– мощность сигнала на выходе тракта, а

$$G_{\sin}(L) = \frac{1}{2 \cdot 100} \left(\mathrm{e}^{-(0{,}23 \cdot \mathrm{Att}(31{,}25) \cdot L)} \right),$$

– мощность одночастотного сигнала с амплитудой 1 В.

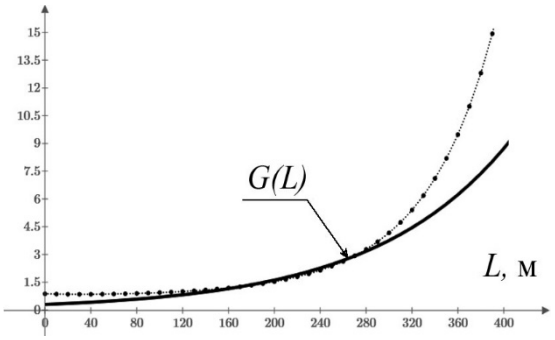


Рис. 5. Зависимость *G*(*L*)

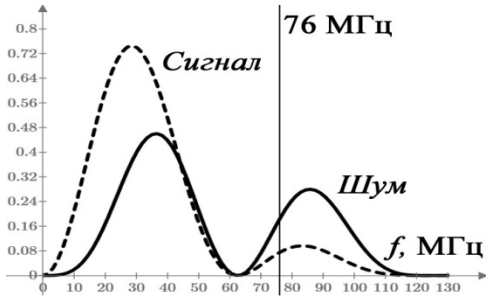


Рис. 6. Нормированные спектральные плотности мощности сигнала и переходной помехи на выходе передатчика

$G(L)$ (3) при длинах кабеля «длинного» Ethernet от 120 до 300 м хорошо описывается экспоненциальной зависимостью (рис. 5):

$$G(L) = \mathrm{e}^{-1{,}21+0{,}0085L}.$$

Мощность широкополосного сигнала на входе в приёмник составляет:

$$G_{rec}(L) = 0{,}005 \cdot \mathrm{e}^{-0{,}027*L} \cdot G(L). \quad (4)$$

Уровень сигнала на входе приёмника согласно (2) и (4) составит:

$$p_r(L) = 10 \log \cdot \left(\frac{G_{rec}(L)}{G_T} \right). \quad (5)$$

Мощность шума определяется переходной помехой на ближний конец:

$$G_{\text{пп}} = \frac{2}{100 \cdot T \cdot \pi} \int_0^{\infty} \left(\mathcal{F}(\omega) 10^{-0{,}05 \cdot NEXT\left(\frac{\omega}{2\pi}\right)} \right)^2 d\omega, \quad (6)$$

где $NEXT$ (ω) – переходное затухание, равное:

$$NEXT(f) = -20 * \log \left(10^{-\frac{NEXT_0 - 15\, lg(f)}{20}} \right), \quad (7)$$

где $f = \omega/2\pi$; $NEXT_0$ – переходное затухание кабеля на ближний конец при f = 1 МГц; $NEXT_0$ определена стандартом ISO/IEC 11801.

Расчёт мощности переходной помехи по (6) и (7) даёт $G_{\text{пп}} = 6{,}65 * 10^{-4}$, мВт, что эквивалентно уровню шума: $p_{NEXT} = 0{,}94NEXT(31{,}25) = -38{,}18$ дБ.

Подстановка (5), (7) в (1) в результате даёт:

$$L = \frac{26{,}25+0{,}94\cdot NEXT(31{,}25)}{0{,}037-\alpha(31{,}25)} = 151, \text{ м.}$$

Заметим, что спектр линейного сигнала и создаваемой им переходной помехи – различны (рис. 6). Это позволяет улучшить отношение сигнала к шуму на входе приёмника применением ФНЧ. Следуя рекомендациям стандарта IEEE 802.3, в качестве входного используем фильтр Баттерворта пятого порядка [8] с передаточной функцией:

$$K = \frac{1}{1+\left(\frac{f}{f_c}\right)^{2n}},$$

где n – порядок фильтра, f_c – частота среза.

Для определения частоты среза ФНЧ введём функцию:

$$G1(x) = \frac{2}{100\cdot T\cdot \pi}\int_0^x \mathcal{F}^2(\omega)\, d\omega,$$

для которой справедливо $G1(\infty) = P_{\text{вх}}$.

За $f_{\text{в}}$ примем решение уравнения:

$$\frac{G1(x)}{P_{\text{вх}}} = 0{,}9, \qquad (8)$$

Численное решение (8) даёт $f_{\text{в}}$ = 76 МГц (рис. 6).

Применение фильтра при $f_{\text{с}} = f_{\text{в}}$ приводит к снижению уровня переходных помех на 2,86 дБ и сигнала на 0,7 дБ. Это позволяет увеличить протяжённость кабельного тракта до 196 м при его реализации на стандартной элементной базе кат. 5е.

При переходе на технику категории 6 предельная протяжённость увеличивается до 293 метра.

Заключение

1. Предельная протяженность тракта «длинного» Ethernet в случае его реализации на стандартной для СКС элементной базе полностью определяется её параметрами на частоте 31,25 МГц.

2. Предлагаемый метод применим при расчёте кабельных трактов с длинами более 150 метров – «длинный» Ethernet.

3. Предельная протяженность трактов «длинного» Ethernet может превышать 200 м даже без использования специализированных кабелей.

Список используемых источников

1. Челышков П. Д., Семенов А. Б. Влияние «Умного города» на телекоммуникации // Вестник связи. 2019. № 2. С. 4–7.
2. Семенов А. Б., Кандзюба Е. В. Перспективы увеличения протяженности симметричного тракта систем цифрового видеонаблюдения // Перспективные технологии в средствах передачи информации – ПТСПИ-2017. Материалы 12-й международной научно-технической конференции, в 2-х т. 2017. С. 215–218.
3. IEEE Std 802.3™–2018 IEEE Computer Society – IEEE Standard for Ethernet. 2018. 5600 p.
4. Семенов А. Б., Кандзюба Е. В., Руденко В. И. «Длинный» Ethernet – дальше, дальше, дальше // Первая миля. 2017. № 7 (68). С. 32–36.
5. ANSI X3.263-1995 Information Technology Industry Council – Fibre Distributed Data Interface (FDDI) – Token Ring Twisted Pair Physical. Layer Medium Dependent (TP-PMD). American National Standard. 1995. 68 p.
6. Жуков А. И. Метод Фурье в вычислительной математике. М. : Наука, 1992. 176 с.
7. ISO/IEC 11801:2011 Information technology – Generic cabling for customer premises. International standard. 2011. 194 p.
8. Рабинер Л., Гоулд Б. Теория и применение цифровой обработки сигналов : пер. с англ. М. : Мир, 1978. 848 с.

Статья представлена научным руководителем, доктором технических наук А. Б. Семёновым.

УДК 004.451.86
ГРНТИ 50.41.15

АНАЛИЗ МЕХАНИЗМОВ РАЗГРАНИЧЕНИЯ ДОСТУПА В СИСТЕМАХ СПЕЦИАЛЬНОГО НАЗНАЧЕНИЯ

А. И. Катасонов, А. Ю. Цветков

Санкт-Петербургский государственный университет телекоммуникаций им. проф. М. А. Бонч-Бруевича

В наши дни вопрос обеспечения информационной безопасности является одним из наиболее острых. Он важен не только для каждого отдельного пользователя, но и касается вопросов государственной важности. В данной статье рассматривается проблема обеспечения безопасности данных в операционных системах специального назначения. Проводится анализ модуля безопасности PARSEC, использующегося в системе специального назначения Astra Linux.

операционные сети, безопасность, Astra Linux, PARSEC, администрирование.

В наши дни, тема безопасности, управления и контроля за секретными данными в компьютерных системах (КС), является одной из наиболее значимых для многих людей. Особенно это касается специальных служб, секретность данных которых является задачей государственной важности. Для решения проблем безопасности необходимо уметь решать задачи анализа безопасности управления доступом, а именно знать, как реализуется безопасность данных при помощи средств, используемых в системах специального назначения. Одним из таких средств является модуль безопасности PARSEC, использующийся в операционной системе (ОС) специального назначения семейства GNU/Linux – Astra Linux. В данной статье рассматривается принципы работы мандатной сущностно-ролевой модели, реализованной при помощи модуля безопасности PARSEC в операционной системе специального назначения Astra Linux [1].

В качестве базовой модели в Astra Linux взята DAC модель, дискреционная модель доступа. Такая модель реализована на основе произвольного управления доступом (субъект-субъектная модель) и доступа на основе ACL (*Access Control Lists* – списки доступа).

Так как Astra Linux это операционная система, прошедшая сертификацию, то она должна соответствовать их требованиям, а одно из самых важных требований – это реализация принудительного контроля доступа, реализованного в качестве MAC модели (*Mandatory access control* – мандатное управление доступом). Однако разработчики не стали включать эту модель в состав ядра Linux, они реализовали её при помощи специальных модулей LSM, которые в нужный момент перехватывают потоки данных и производят проверку на соответствие доступа.

Идея LSM проста. В моменты кода ядра, когда субъекту требуется доступ к какому-либо объекту, LSM модуль перехватывает управление и производит свой контроль доступа. Удобство такого подхода заключается в том, что внутри LSM модуля можно реализовать любую модель управления доступом.

Модуль LSM не заменяет основную модель DAC. Он вступает в работу только после прохождения проверки доступа системы DAC. Такой способ позволяет не перегружать функциями безопасности те системы, в которых это не требуется.

Поскольку Astra Linux уже находится в эксплуатации у многих людей и различных специальных служб, то разработчики имеют огромное количество статистики, исследуя которую можно судить о корректности работы данной модели, а также можно судить об огромном количестве проблем, связанных с обеспечением безопасности [2].

Для того чтобы решить эти проблемы разработчики задействовали дополнительный модуль LSM, который реализован в системе

PARSEC (рис. 1). Таким образом, и была создана мандатная сущностно-ролевая ДП модель.

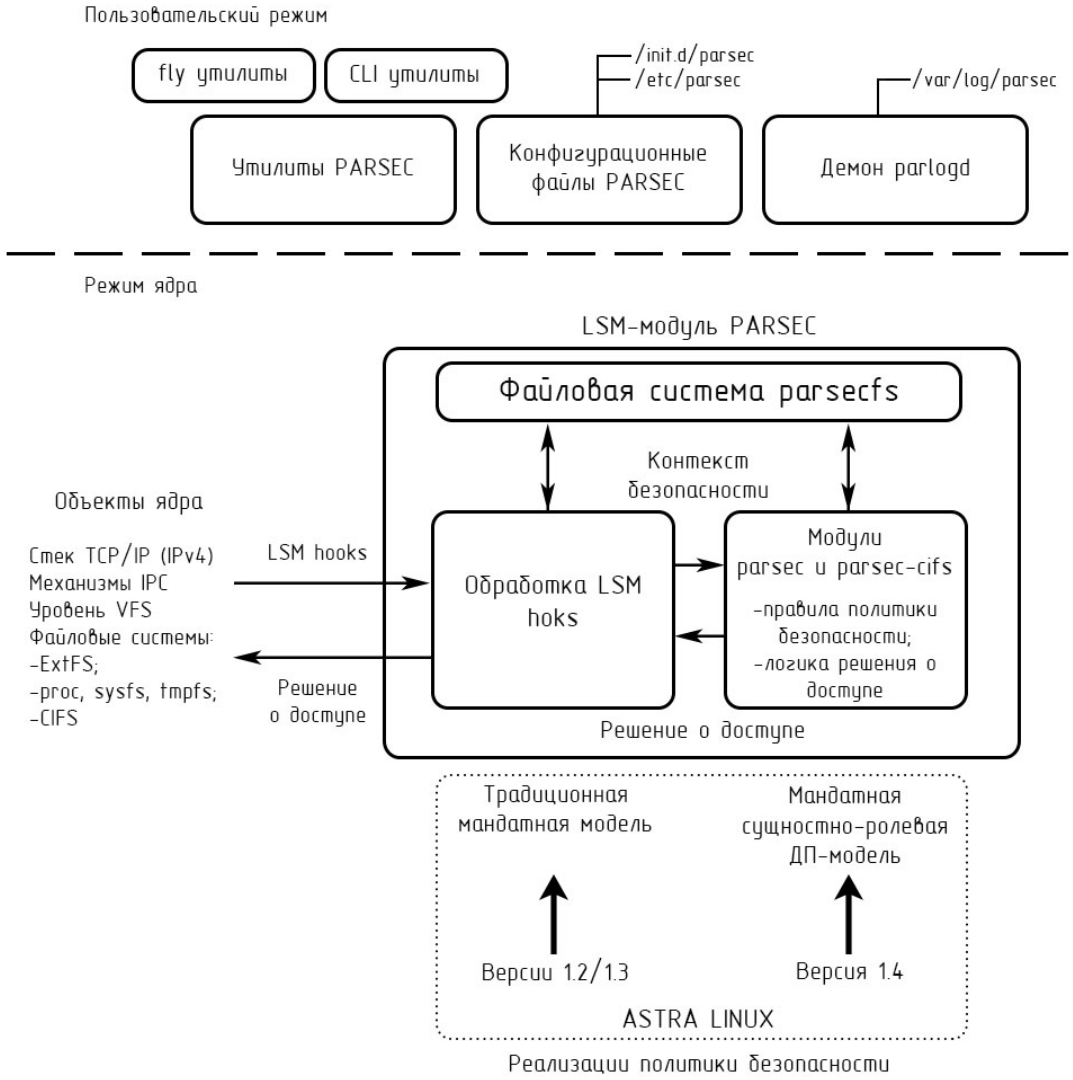


Рис. 1. Принципиальная схема LSM модуля PARSEC

Подсистема безопасности модуля PARSEC состоит не только из модулей LSM, которых в ней очень большое количество. В ней находится также и собственная файловая система parsecfs, конфигурационные файлы, демоны и утилиты. Эта модель относится к классу ДП-моделей, т. к. она занимается управлением доступа (Д) и информационными потоками (П). Такие модели могут учитывать, куда распространяется поток информации, который был запущен определенными приложениями для выполнения какой-либо операции над данными, а не только единичный акт доступа к этим данным [3].

Мандатная сущностно-ролевая модель безопасности отличается от стандартной МАС тем, что она представляет собой симбиоз мандатного

и ролевого управления доступом. Таким образом, управление доступом происходит не только за счет мандатной модели управления доступом, но и за счет мандатного контроля целостности (MIC – *Mandatory Integrity Control*) [4]. Схему взаимодействия трех ДП-моделей вы можете видеть на рис. 2.

Управление целостностью правильнее будет назвать уровнем доверия, который позволяет следить за тем, чтобы субъект, имеющий низкий уровень доверия (IL – *integrity level*) не смог внести изменения в объект, имеющий высокий уровень доверия, что позволяет обеспечить целостность данных

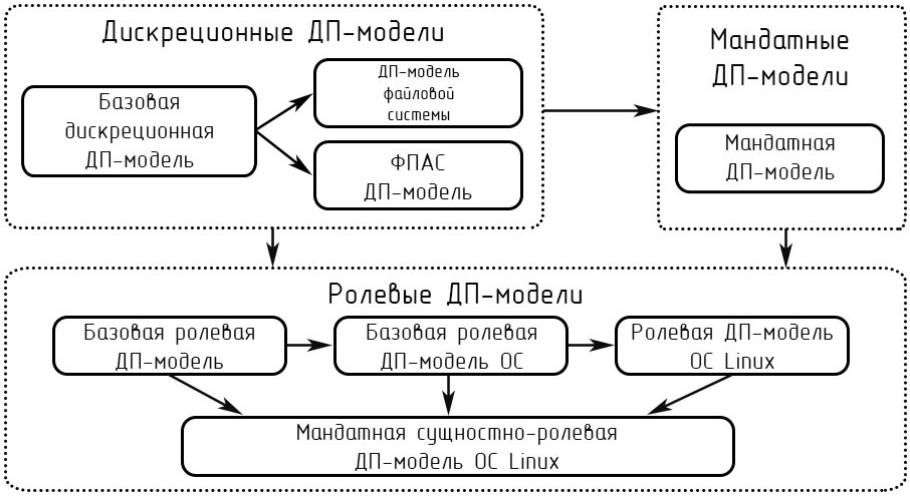


Рис. 2. Схема взаимодействия трех ДП моделей

Еще одной важной особенностью мандатной сущностно-ролевой модели является учет иерархичности организации как ряда объектов доступа, так и функций (ролей), выполняемых субъектами. При помощи такого учета можно считать подобные объекты, а также роли субъектов доступа как категорию «сущность». Благодаря такому подходу и осуществляется контроль за тем, чтобы внутрь контейнера, имеющего низкий уровень целостности, не мог попасть объект, имеющий высокий уровень [5].

Схему взаимодействия системы с дополнительными модулями можно видеть на рис. 3 (см. ниже).

Также в модели PARSEC существуют специальные атрибуты сущностей-контейнеров, например, установка атрибута ehole, благодаря которому можно игнорировать мандатные метки целостности, когда выполняешь запись в них. Это может быть необходимо для работы с объектами общего пользования, вроде директории tmp. Также существует атрибут ccnr, который реализует возможности, при которых метка конфиденциальности не применяется при просмотре объектов внутри сущности контейнера. На рис. 4 можно видеть скрипт инициализации правил разграничения доступа для ключевых директорий корневой файловой системы Astra Linux.

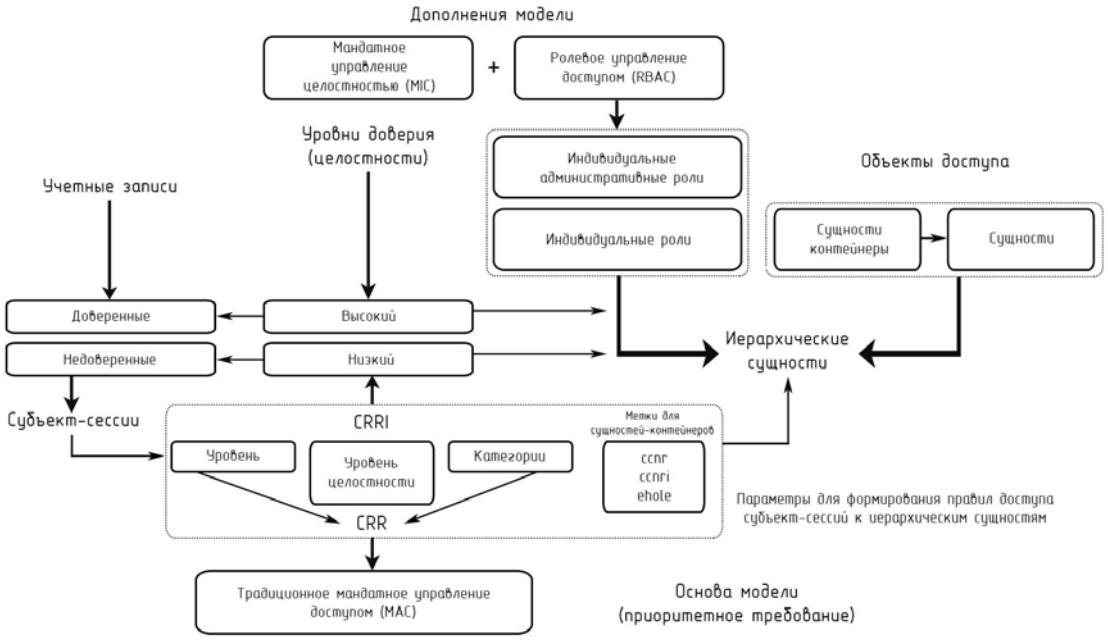


Рис. 3. Схема взаимодействия с дополнительными модулями

```
pdp-init-fs       [----]  0 L:[  1+27  28/ 28] *(593 / 593b) <EOF>
#!/bin/bash

sysmaxlev=3
sysmaxilev=0
sysmaxcat=0xffffffffffffffff

sysmaxlbl="$sysmaxlev:0:$sysmaxcat"

pdp-flbl "$sysmaxlev:$sysmaxilev:$sysmaxcat:CCNRALL" /
pdp-flbl "$sysmaxlbl:ccnr" /dev

pdp-flbl "$sysmaxlbl:ccnr,ehole" /tmp

pdp-flbl "$sysmaxlbl:ccnr" /var/
pdp-flbl "$sysmaxlbl:ccnr" /var/private/
pdp-flbl "$sysmaxlbl:ccnr" /var/private/*
pdp-flbl "$sysmaxlbl:ccnr" /var/run/
pdp-flbl "$sysmaxlbl:ccnr" /var/spool/
pdp-flbl "$sysmaxlbl:ccnr,ehole" /var/run/shm/
pdp-flbl "$sysmaxlbl:ccnr,ehole" /var/mail/

pdp-flbl "$sysmaxlbl:ccnr" /home/
pdp-flbl "$sysmaxlbl:ccnr" /home/.pdp/
```

Рис. 4. Скрипт инициализации правил разграничения доступа для ключевых директорий корневой файловой системы Astra Linux SE

Реализовав модули LSM, разработчики не забыли создать и большое количество утилит для удобного администрирования данной системы, ведь стандартный набор утилит был создан для администрирования стандартной MAC модели и не учитывал рассмотренные выше новшества [6].

Также, начиная с версии 1.4 в Astra Linux, появилась совокупность утилит pdp-, которые необходимы для просмотра и модификации как стандарт-

ных MAC атрибутов, но и MIC атрибутов, а также дополнительных атрибутов (*ccnr, ccnri, ehole*). Однако утилиты предыдущих версий также остались и в новой версии для удобства администраторам процесса миграции уже функционирующих информационных систем на новую модель [7].

Таким образом, в данной статье рассматриваются основные особенности работы модуля безопасности PARSEC, который используется в операционной системе специального назначения семейства GNU/Linux – Astra Linux. Исследуемая операционная система обеспечивает высокий уровень безопасности хранимых на ней данных, имеет большие возможности в разграничении доступа, а также обеспечивает высокую целостность данных. Astra Linux отвечает всем требованиям центров сертификации, однако требует высокого уровня освоения принципов её работы для качественного её администрирования.

Список используемых источников

1. Штеренберг С. И., Щеголева Д. И., Виноградова О. М. Синхронизированное использование систем защиты информации для контроля учёта рабочего времени //Вестник Санкт-Петербургского государственного университета технологии и дизайна. Серия 1: Естественные и технические науки. 2019. № 4. С. 3–8.

2. Штеренберг С. И., Полтавцева М. А. Распределенная система обнаружения вторжений с защитой от внутреннего нарушителя // Проблемы информационной безопасности. Компьютерные системы. 2018. № 2. С. 59–68.

3. Волкогонов В. Н., Гельфанд А. М., Деревянко В. С. Актуальность автоматизированных систем управления // Актуальные проблемы инфотелекоммуникаций в науке и образовании (АПИНО 2019). VIII Международная научно-техническая и научно-методическая конференция : сб. науч. ст. в 4 т. 2019. С. 262–266.

4. Волкогонов В. Н., Гельфанд А. М., Карамова М. Р. Обеспечение безопасности персональных данных при их обработке в информационных системах персональных данных // Актуальные проблемы инфотелекоммуникаций в науке и образовании (АПИНО 2019). VIII Международная научно-техническая и научно-методическая конференция : сб. науч. ст. в 4 т. 2019. С. 266–270.

5. Ушаков И. А. Обнаружение инсайдеров в корпоративной компьютерной сети на основе технологий анализа больших данных // Вестник Санкт-Петербургского государственного университета технологии и дизайна. Серия 1: Естественные и технические науки. 2019. № 4. С. 38–43.

6. Исаков А. С., Ковцур М. М. Развертывание удостоверяющего центра на ОС Astra Linux для обеспечения поддержки pki // Актуальные проблемы инфотелекоммуникаций в науке и образовании (АПИНО 2017). VI Международная научно-техническая и научно-методическая конференция : сб. науч. ст. в 4-х т. 2017. С. 371–375.

7. «Хакер» – Русский бронированный Debian. Как устроена новая модель управления доступом в Astra Linux SE [Электронный ресурс] // yztm.ru [сайт]. URL: http://yztm.ru/2017/10/07/haker/ (дата обращения 10.01.2020).

Статья представлена заведующим кафедрой ЗСС СПбГУТ, кандидатом технических наук, доцентом А. В. Красовым.

УДК 004.056.53
ГРНТИ 81.93.29

АЛГОРИТМ ОБНАРУЖЕНИЯ АТАК НА ИНТЕРФЕЙСЕ N2 5G СЕТЕЙ

Т. В. Катина, М. М. Ковцур

Санкт-Петербургский государственный университет телекоммуникаций им. проф. М. А. Бонч-Бруевича

Статья посвящена проблемам безопасности 5G-сетей и Интернета вещей. Актуальность статьи обусловлена тем, что информационная безопасность таких сетей является недостаточно изученной проблемой. Авторы анализируют безопасность протокола сигнализации NGAP. Проводят обзор работ аномального трафика в 5G-сетях в протоколе NGAP. Для DDoS-атак на идентификатор абонента в работе предлагается обобщенный алгоритм обнаружения.

5G-сети, NG-RAN, DDoS-атака, протокол NGAP, Интернет вещей.

По мере того, как страны по всему миру начинают внедрять технологию 5G звучат обещания более высоких скоростей и лучшего обслуживания. Однако такие инновации иногда скрывают множество проблем информационной безопасности (ИБ), влияющих на мобильную связь. Эти проблемы ИБ существуют, несмотря на улучшения в области шифрования данных, аутентификации и конфиденциальности, описанных в последних выпусках документации 3GPP (организация по техническим стандартам сотовой связи).

Технология NG-RAN обеспечивает и NR и LTE радиодоступ в сети. Узлом NG-RAN (т. е. базовой станцией) может быть: либо gNB, обеспечивающая услуги и сервисы и для плоскости управления, и для плоскости пользователя; либо ng-eNB, обеспечивающая связь услуг и сервисов LTE/E-UTRAN к UE. Станции gNB и ng-eNB соединяются друг с другом с помощью Xn-интерфейсов. К сети 5G они подключаются с помощью NG-интерфейсов [1]. NG интерфейсы также называют N2 интерфейсами.

AMF – Access and Mobility Management Function – означает узел в сети 5G, отвечающий за функцию управления доступом и мобильностью, а UPF – User Plane Function – это узел сети, реализующий функцию управления в плоскости пользователя. AMF отвечает за выполнение таких функций как управление регистрацией, соединением, мобильностью, аутентификация доступа и т.д. UPF осуществляет инспекцию пакетов, маршрутизацию и пересылку пакетов, обработку QoS для плоскости пользователя и т. д.

Для обмена сообщениями между gNB и AMF/UPF был разработан протокол NGAP. Этот протокол реализует все необходимые механизмы для поддержания процедур между AMF и RAN. Все возможные службы

и сервисы реализованы путем выполнения так называемых элементарных процедур (единицами взаимодействия между NG-RAN и AMF [2]).

Хотя технологии NG-RAN и 5GC являются новым шагом на пути к высокотехнологичному будущему, решения по обеспечению их информационной безопасности вызывают много вопросов даже среди экспертов [3]. К сожалению, основные проблемы, с которыми сталкиваются предыдущие поколения мобильных технологий – GSM, 4G и LTE – не были рассмотрены в стандартах 5G. И одна из них – это возможность перехватывать так называемые сообщения предварительной аутентификации между базовой станцией пользователя и вышкой сотовой связи. В связи с тем, что UE принимает широковещательные сообщения с вышки сети, эта вышка может быть, как 3G, так и 4G. Она сообщает пользователю, что она является вышкой оператора UE. И нет никакого криптографического способа проверить так ли это. Злоупотребляя этими незащищенными сообщениями, злоумышленники могут реализовывать различные атаки.

Стандарты LTE, и стандарты 5G разработаны для предотвращения несанкционированного раскрытия международного идентификатора абонента (IMSI – *International Mobile Subscriber Identity*), или, в терминологии технологии 5G, атаки на постоянный идентификатор подписки (SUPI – *Subscription Permanent Identifier*), но эти стандарты являются необязательными [4]. Разберем один из возможных сценариев атаки на 5G. Атака заключается в том, что вредоносное UE инициирует хэндовер через N2/Xn интерфейсы, что приводит к огромному количеству передач сообщений сигнализации. Термин хэндовер означает процесс передачи входящего вызова или сессии из одного канала, подключенного к основной сети, в другой [5]. Процесс осуществления атаки представлен на рис. (см. ниже).

Для осуществления атаки требуется выполнить следующие шаги:

1) UE жертвы подключается к вредоносной базовой станции gNB, так как эта станция обладает наиболее высоким уровнем сигнала. Атака может быть проведена в общественном месте, чтобы число жертв было больше [6].

2) Нарушитель передает сообщение (запрос от легитимного UE к базовой станции на регистрацию) с помощью вредоносной базовой станции gNB и одного из вредоносных UE в легитимную базовую станцию gNB, где:

а) вредоносное UE может появится в различных посещенных местах, которые могут находиться на довольно большом расстоянии;

б) нарушитель может достичь своей цели сконструировав аппарат вредоносного UE с использованием USRP с применением стека протоколов 5G.

3) Нарушитель размещает вредоносное UE в различных географических точках и подключает их к локальной PLMN.

4) Нарушитель перенаправляет запрос жертвы на регистрацию в вредоносное UE используя сеть, чтобы вредоносное UE «появилось» в другом посещенном месте.

5) Вредоносное UE отправляет этот запрос на регистрацию локальной сотовой сети, где:

а) нарушителю нужно только постоянно переключать «обслуживаемое» UE чтобы сделать так что UE жертвы «появилось» в разных местах;

б) интервал переключения не больше 5 минут, чтобы настоящий запрос на регистрацию от UE жертвы в итоге был оценен домашней сетью как фальшивый.

6) Домашняя сеть блокирует UE жертвы.

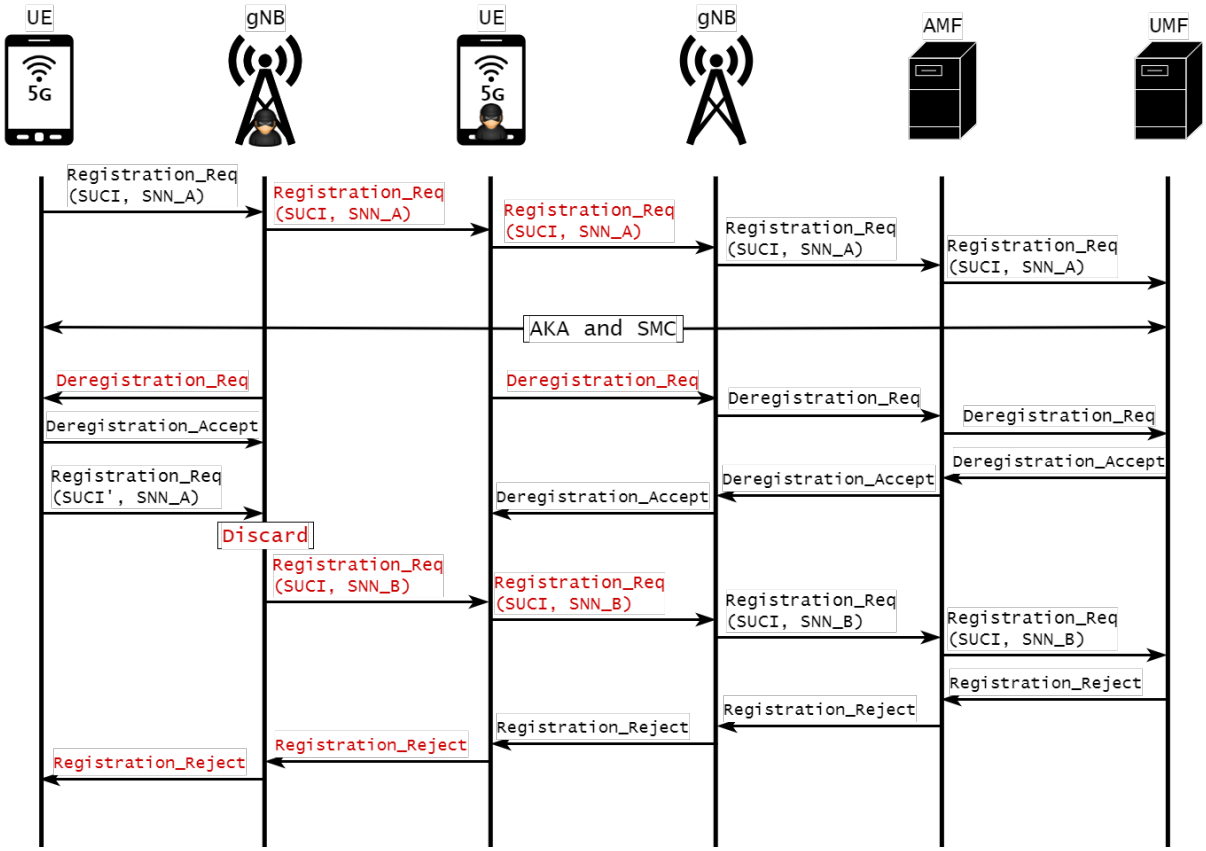


Рис. Структура транзакции сообщений при реализации атаки

Таким образом, домашняя сеть запрещает доступ UE-жертвы к сети по причине того, что UE жертвы был атакован DoS-атакой, а атака не была обнаружена. Продолжительность DoS-атаки зависит от настроек оператора. Поэтому она может варьироваться от нескольких часов до нескольких дней.

Чтобы улучшить безопасность 5G-сети, 3GPP усилили контроль за домашней сетью путем использования протоколов AKA (*Authentication and Key Agreement*). Однако нарушитель может использовать эти алгоритмы защиты, чтобы обманным путем обойти протокол безопасности и закрыть доступ к сети для UE жертвы.

Также нарушитель может атаковать сразу несколько UE для реализации большого количества вредоносных UE. Поэтому симптомами атаки является большое количество заблокированных UE в одной сети. Симптомы атаки перечислены ниже:

1) большое количество сообщений реализации хэндовера на интерфейсе N2;

2) большое количество UE с одними и теми же параметрами (SUCI, SUPI, SNN);

3) UE с конкретным SUCI перемещаются на большие расстояния за очень короткое время;

4) большое количество заблокированных UE в одной сети.

Для защиты от описанной атаки можно использовать цифровые сертификаты, чтобы предоставить UE способ криптографической проверки того, что они действительно подключены к базовой станции [7]. Однако и у этого решения есть свои сложности. Во-первых, это потребует глобальных изменений стандартов, потому что стандарты 5G в настоящее время не предусматривают такого рода сертификаты шифрования. Во-вторых, UE не могут заранее блокировать сертификаты, которые когда-то были надежными, но теперь были отозваны, потому что до тех пор, пока пользователи не установят соединение с оператором, они не смогут получить доступ к Интернету [8].

Поэтому первоначально следует разработать алгоритм обнаружения атаки, который в будущем можно будет использовать для нейтрализации атаки. При разработке алгоритма следует учитывать следующее:

1) обычное поведение UE;

2) обычное местоположение для этого UE;

3) обычное время, которое UE проводит в его привычных местах;

4) обычное количество сообщений хэндовера от UE.

Основными входными данными для алгоритма обнаружения являются данные входящего трафика AMF о сообщениях хэндовера.

Тогда в качестве выходных данных получим следующее:

1) поведение нарушителя;

2) количество атак;

3) количество сообщений хэндовера;

4) различие временных меток;

5) различие в местоположениях;

6) стандартное отклонение для сообщений хэндовера;

7) стандартное отклонение для разности временных меток;

8) стандартное отклонение между местоположениями;

9) идентификатор gNB, доступной вредоносному UE;

10) идентификатор AMF, доступного вредоносному UE;

11) SUCI/SUPI;

12) количество заблокированных UE.

Описанный алгоритм обнаружения аномального поведения может быть реализован с использованием средств машинного обучения таких как обучение без учителя, а именно – алгоритм BIRCH или алгоритм робастой ковариации (*Robust Covariance*). Эти алгоритмы уже были успешно использованы при обнаружении аномального поведения в других исследованиях [9].

Таким образом, в статье был дан краткий обзор протокола NGAP относительно общей структуры NG-RAN, рассмотрен сценарий реализации DoS-атаки на скрытый идентификатор подписки (SUCI) с использованием вредоносной базовой станции gNB и вредоносного UE, также был предложен обобщенный алгоритм обнаружения атаки подобного типа с описанием входных и выходных данных для его реализации.

Список используемых источников

1. 3GPP TS 38.401 V16.0.0 (2019-12) “Technical Specification Group Radio Access Network; NG-RAN; Architecture description”.

2. 3GPP TS 38.413 V16.0.0 (2019-12) “Technical Specification Group Radio Access Network; NG-RAN; NG Application Protocol (NGAP)”.

3. Виткова Л. А., Дудникова М. Н., Петрова А. Н. Вопросы управления информационной безопасностью // Актуальные проблемы инфотелекоммуникаций в науке и образовании (АПИНО 2018). VII Международная научно-техническая и научно-методическая конференция : сб. науч. ст. в 4-х т. 2018. С. 143–146.

4. 3GPP TS 33.501 V15.1.0 (2018-07) “Technical Specification Security architecture and procedures for 5G System”.

5. Сахаров Д. В., Левин М. В., Фостач Е. С., Виткова Л. А. Исследование механизмов обеспечения защищенного доступа к данным, размещенным в облачной инфраструктуре // Наукоемкие технологии в космических исследованиях Земли. 2017. Т. 9. № 2. С. 40–46.

6. Донской Д. М., Рябова О. Н., Сахаров Д. В., Виткова Л. А. Некоторые аспекты модели нарушителя информационной безопасности в интернете вещей // Интернет вещей и 5G. 2016. С. 47–50.

7. Jover R. P., Marojevic V. Security and protocol exploit analysis of the 5G specifications // IEEE Access. 2019. V. 7. PP. 24956–24963.

8. Виткова Л. А., Герлинг Е. Ю., Головлёва Ю. А., Ковцур М. М. Конвергенция информационных технологий для повышения эффективности управления информационным пространством Санкт-Петербурга // Актуальные проблемы инфотелекоммуникаций в науке и образовании (АПИНО 2018). VII Международная научно-техническая и научно-методическая конференция : сб. науч. ст. в 4-х т. 2018. С. 140–142.

9. Santos J. et al. Anomaly detection for smart city applications over 5g low power wide area networks // NOMS 2018-2018 IEEE/IFIP Network Operations and Management Symposium. IEEE, 2018. PP. 1–9.

УДК 004.7
ГРНТИ 49.33.29

РАЗРАБОТКА МОДЕЛЕЙ И МЕТОДОВ ТЕСТИРОВАНИЯ СЕТЕЙ СВЯЗИ 2030

Р. В. Киричек, М. Н. Сторожук

Санкт-Петербургский государственный университет телекоммуникаций им. проф. М. А. Бонч-Бруевича

С развитием технологии Интернет Вещей на современные сети ложится большая нагрузка. Для многих областей очень важно качество каналов, по которым передается информация. Невыдерживание параметров этих каналов может привести к негативным последствиям. Такие сети нуждаются в непрерывном мониторинге и контроле. Для обеспечения выполнения заданных параметров нужны новые методы оценки параметров сетей и оборудование, способное их выполнять.

сети 2030, интернет вещей, технологии пакетной коммутации, измерение параметров.

Стремительное развитие науки и технологий ставит перед современными сетями связи все более сложные задачи. Появление новых разработок в областях автоматизации, робототехники, интернета вещей, тактильного интернета, автономного транспорта и многих других увеличивает количество передаваемого трафика в сотни раз и предъявляет более высокие требования к его качеству. Это справедливо и для таких областей, как медицина и критическая инфраструктура, где также важен не только объем передаваемых данных, но и своевременность их доставки без сбоев и ошибок. Эти аспекты накладывают на современные сети строгие требования к параметрам каналов, несоответствие которым может привести к негативным последствиям. Для обеспечения выполнения заданных параметров нужны новые методики оценки качества сетей и соответствующие средства измерений.

Для технологии пакетной коммутации характерно совместное использование большого количества маршрутизаторов и коммутаторов разных уровней, произведенных разными предприятиями, принадлежащих различным операторам и использующих неодинаковые алгоритмы маршрутизации. Тем не менее, на их основе строится общая среда передачи, оптимизированная для распространения цифровой информации, уже в этой среде создаются виртуальные сети IP телефонии, передаются сигналы телевещания или видеоконференцсвязи и многое другое. Неоднородность самих сетей и использование множества протоколов и технологий передачи в их разных сегментах тоже можно отнести к факторам, усугубляющим ситуацию,

как и отсутствие сквозной управляемости. Однако все это не приводит к неработоспособности различных сетевых устройств или сервисов, а лишь осложняет задачу доставки пакетов, которые, хоть и с задержками, но чаще всего все-таки добираются до своего адресата. Именно этот факт и приводит подчас к ошибочному мнению, что сети передачи пакетной информации являются полностью автономной средой и, как следствие, отсутствует необходимость их обслуживания, тестирования и измерения качественных параметров передачи информации в каналах.

С приходом каждой новой телекоммуникационной технологии возникает иллюзия ее идеальности и универсальности. При этом часто поднимался вопрос об отсутствии необходимости контроля и измерения параметров качества каналов, делались попытки сократить «лишний» обслуживающий персонал и сэкономить на закупке контрольно-измерительного оборудования. Но по прошествии некоторого времени все становилось на свои места, новое оборудование не избавляло от отсутствия перерывов связи и деградации ее качества, а операторам все так же приходилось нести эксплуатационные расходы на содержание специалистов и на приобретение измерительных приборов.

Иллюзии о высочайшей надежности работы IP-среды на сегодняшний день уже ушли в прошлое, но четких представлений о том, что и с какой точностью нужно измерять в процессе эксплуатации и какие значения параметров считать приемлемыми, до сих пор не выработано. Ситуация осложняется тем, что необходимые величины конкретных параметров сети для разных услуг или сервисов отличаются.

В отличие от предшествующих телекоммуникационных технологий коммутация пакетов длительное время развивалась в нашей стране в правовом вакууме, долго не было законодательных актов, регламентирующих параметры каналов с коммутацией пакетов и средств измерений этих параметров, что приводило к злоупотреблениям со стороны операторов связи, которые в договорах с потребителями часто фиксировали лишь максимальную скорость передачи и не оговаривали остальные качественные параметры. Со временем пакетные технологии все шире стали применяться для передачи информации, обеспечивающей работоспособность предприятий и поддержание технологических процессов, а ситуация с неконтролируемостью их качественных параметров становилась неприемлемой, она стала постепенно меняться.

Состояние отечественной нормативно-правовой базы

С 1 сентября 2003 г. был введен в действие ГОСТ 8.417-2002. «Единицы величин» [1], в котором наряду с другими были определены и единицы количества информации: бит и байт. 23 января 2006 г. вышло постановление правительства РФ № 32 «Об утверждении правил оказания услуг

связи по передаче данных» [2]. 10 сентября 2007 г. вышло постановление правительства РФ № 575 «Об утверждении правил оказания телематических услуг связи» [3]. Министерство информационных технологий и связи Российской Федерации в 2007 году издало Приказ № 113 «Об утверждении требований к организационно-техническому обеспечению устойчивого функционирования сетей связи общего пользования» [4], в нем были прописаны нормы на показатели функционирования сетей с коммутацией пакетов по следующим показателям: средняя задержка передачи пакетов; отклонение от средней задержки передачи пакетов информации; коэффициент потери пакетов информации; коэффициент ошибок в пакетах информации.

23 июля 2015 г. вышел приказ Министерства связи и массовых коммуникаций Российской Федерации от № 277 «Об утверждении Обязательных метрологических требований к измерениям, относящимся к сфере государственного регулирования обеспечения единства измерений, в части компетенции Министерства связи и массовых коммуникаций Российской Федерации» [5]. В нем установлены диапазон и пределы допускаемой погрешности при измерениях разности шкал времени в сетях операторов связи относительно национальной шкалы времени РФ, продолжительность телефонных соединений и сеансов передачи данных, количества переданной (принятой) информации (данных); 20 декабря 2016 г. вышел приказ Министерства связи и массовых коммуникаций Российской Федерации № 673 «Об утверждении требований к организационно-техническому обеспечению устойчивого функционирования сети связи общего пользования в части установления требований к допустимой величине разности (расхождению) шкал времени в сетях операторов связи» [6]. В нем установлены нормы на разность (расхождение) шкал времени в сетях операторов связи относительно национальной шкалы времени Российской Федерации. Таким образом, на сегодняшний день в нашей стране законодательно определены параметры сетей с пакетной коммутацией, которые нужно мерить, но методика измерений в вышеперечисленных документах не оговаривается.

Единственное, чем могли воспользоваться службы эксплуатации операторов связи, это международный опыт в данной области. Во многих странах, а в последние годы и в России, стандартом для измерения параметров пакетных сетей де-факто стали международные рекомендации, разработанные Инженерным советом Интернет IETF (*Internet Engineering Task Force*) и Сектором по стандартизации телекоммуникаций в составе Международного союза электросвязи ITU-T (*International Telecommunication Union – Telecommunication sector*). Поэтому большинство отечественных и импортных контрольно-измерительных приборов, эксплуатируемых операторами связи, производят измерения, используя методики этих рекомендации. Эпизодические эксплуатационные измерения, производимые техническим пер-

соналом при помощи этих приборов, не могут обеспечить постоянный контроль, который необходим для бесперебойного функционирования объектов интернета вещей. Такой контроль можно осуществить только при помощи мониторинга качества услуг связи, основными целями которого являются [7]:

– поддержка конкурентоспособности на телекоммуникационном рынке;

– определение необходимости расширения, модернизации сети связи для обеспечения поддержки контролируемых значений показателей качества услуг связи при возрастающем объеме пропускаемого трафика;

– привлечение новых абонентов и сохранение лояльности существующих абонентов путем опубликования результатов измерений качества услуг связи, поддерживаемых сетью связи.

Системы мониторинга должны решать следующие задачи:

– контроль доступности каналов связи – является очень важным параметром для интернета вещей;

– измерение качества каналов связи пакетной сети. От качественных параметров канала зависит своевременность и достоверность доставки информации, что необходимо для интернета вещей;

– подтверждение качества каналов передачи данных, предоставляемых сетевым оператором связи или сторонним провайдером. Иначе будет не ясно, добросовестно ли оператор связи выполняет взятые на него обязательства по предоставлению канала связи;

– измерение односторонних задержек. Является одной из ключевых характеристик, изменение которой может указывать не только на изменения качества канала, но и на попытку криптографической атаки «человек посередине»;

– обеспечение устойчивого функционирования объектов информационной инфраструктуры при проведении в отношении них компьютерных атак, попыток несанкционированного доступа и копирования или искажения информации.

Также 19 декабря 2019 года вышел приказ № 870 «Об утверждении Перечня измерений, относящихся к сфере государственного регулирования обеспечения единства измерений и выполняемых при обеспечении целостности и устойчивости функционирования сети связи общего пользования, и обязательных метрологических требований к ним, в том числе показателей точности измерений» [8]. В нем определен следующий перечень измерений: измерения параметров сетей передачи данных; измерения параметров сетей тактовой сетевой синхронизации; измерения параметров временной синхронизации; измерения параметров цифровых стыков и синхронной цифровой иерархии (СЦИ).

Данный приказ вступит в силу через год, потому что нет аттестованных и утвержденных методик измерения этих параметров. Планируется, что их разработают в течение этого года и они будут аттестованы и утверждены ко времени вступления приказа в силу.

Заключение

Мониторинг – это единственное средство непрерывного отслеживания функционирования сетей связи, которое обеспечивает объективный контроль параметров каналов передачи данных, а также степень соблюдения оператором закрепленных в соглашении о качестве показателей, обслуживания. Благодаря этому возможно оперативно реагировать на ухудшение связи и контролировать работу телекоммуникационного оператора и доступность сервисов для пользователей.

Такое решение наилучшим образом подходит для обеспечения функционирования интернета вещей.

Список используемых источников

1. ГОСТ 8.417-2002. «Единицы величин». М. : Изд-во стандартов, 2002.

2. Постановление Правительства РФ от 23.01.2006 № 32 (ред. от 25.10.2017) «Об утверждении Правил оказания услуг связи по передаче данных».

3. Постановление Правительство Российской Федерации от 10 сентября 2007 г. № 575 «ОБ утверждении правил оказания телематических услуг связи».

4. Приказ Министерства информационных технологий и связи РФ от 27 сентября 2007 г. № 113 «Об утверждении Требований к организационно-техническому обеспечению устойчивого функционирования сети связи общего пользования».

5. Приказ Министерства связи и массовых коммуникаций Российской Федерации № 277 от 23.07.2015 «Об утверждении Обязательных метрологических требований к измерениям, относящимся к сфере государственного регулирования обеспечения единства измерений, в части компетенции Министерства связи и массовых коммуникаций Российской Федерации».

6. Приказ Министерства связи и массовых коммуникаций Российской Федерации № 673 от 20.12.2016 «Об утверждении требований к организационно-техническому обеспечению устойчивого функционирования сети связи общего пользования в части установления требований к допустимой величине разности (расхождению) шкал времени в сетях операторов связи».

7. Сторожук Н. Л. Некоторые аспекты обеспечения качественных параметров каналов связи // Информация и космос. 2018. № 1. С. 33 –36.

8. Приказ Министерства цифрового развития, связи и массовых коммуникаций РФ от 19 декабря 2019 г. N 870 «Об утверждении Перечня измерений, относящихся к сфере государственного регулирования обеспечения единства измерений и выполняемых при обеспечении целостности и устойчивости функционирования сети связи общего пользования, и обязательных метрологических требований к ним, в том числе показателей точности измерений» (документ не вступил в силу).

УДК 65.011.56
ГРНТИ 49.33.29

ВОЗМОЖНЫЕ НАПРАВЛЕНИЯ ПРИМЕНЕНИЯ МЕТОДОВ ИНТЕЛЛЕКТУАЛЬНОГО АНАЛИЗА ДАННЫХ ДЛЯ ДИНАМИЧЕСКОГО УПРАВЛЕНИЯ АВТОНОМНЫМИ СЕТЯМИ СВЯЗИ

П. В. Киселева[1], С. В. Кисляков[1,2]

[1]Санкт-Петербургский государственный университет телекоммуникаций им. проф. М. А. Бонч-Бруевича
[2]ООО «НТЦ Аргус»

Поставщики услуг по всему миру в настоящее время находятся в процессе цифрового преобразования в сторону сетей 5G. Технологии 5G/M2M позволяют пересмотреть подходы в сторону идеи «Plug&Play», то есть развивая концепцию Автономных сетей связи (Autonomous Networks). Целью настоящей статьи является отражения результатов исследований по выявлению возможных направлений применения методов интеллектуального анализа данных применительно к автономным сетям связи.

автономные сети, 5G/M2M, TM Forum, Artificial Intelligence (AI).

Введение

По данным Huawei's Global Industry Vision к 2025 году во всем мире будет насчитываться в общей сложности 100 миллиардов соединительных подключений [1]. Значительный рост спроса на подключение объектов может вызвать трудности у производителей и интеграторов оборудования из-за сложности развертывания сети, а именно: большой территориальной разрозненности сетевой архитектуры, проблематичной интеграции с предшествующими технологиями, неэффективности своих операций и отсутствия знаний, методологий и опыта инсталляции. Кроме того, технология 5G требует заниматься грамотным проектированием и последующим развертыванием сети до начала ее эксплуатации [2].

Автономные сети имеют значительный потенциал, и данные Всемирного экономического форума свидетельствуют о том, что автоматизация сети может принести 9 млрд долл. США вследствие менее частых и более коротких перебоев в работе сети, что позволяет стремиться к показателю устойчивости сети равному 0,99999 (40 мс простоя сети в год) [3].

Автономные сети должны использовать преимущества методов искусственного интеллекта (AI), больших данных, облачных вычислений и обеспечивать возможность полной (сквозной) автоматизации, самовосстановления и самооптимизации на всех уровнях и для всех задач – от управления

ресурсами до эксплуатации и обслуживания клиентов и обеспечения сервисного обслуживания.

Автономные сети: рамки и уровни

Высокий уровень автоматизации предполагает использование алгоритмов, позволяющих контролировать быстро протекающие процессы.

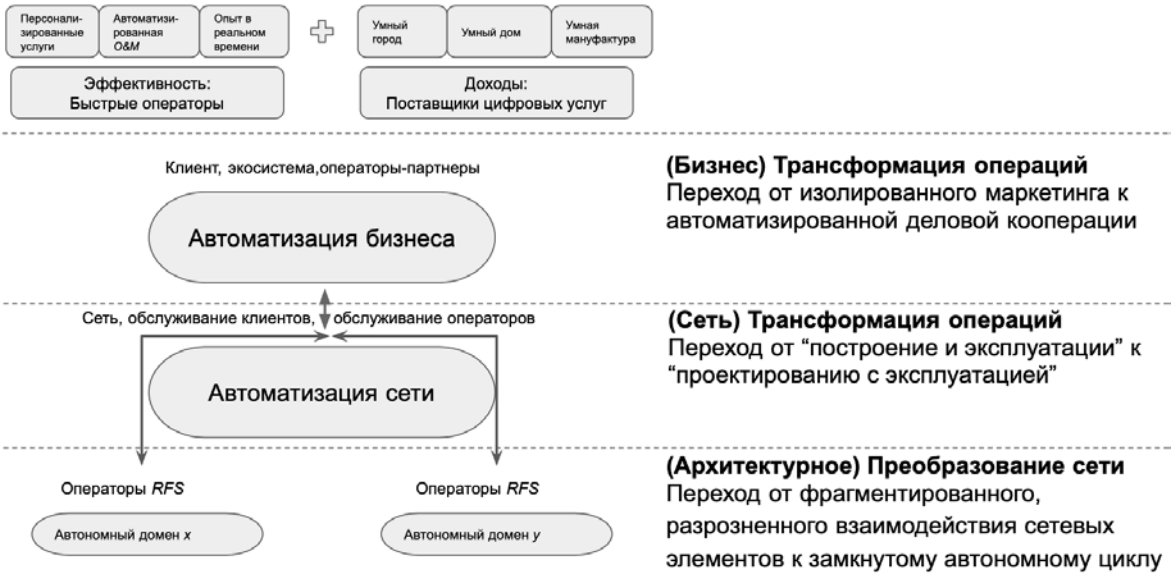


Рис. 1. Уровни автоматизации автономных сетей

Для измерения степени развитости автономии сети организацией TM Forum предложены уровни развитости автоматизации рис. 1. [4]:

Нулевой уровень – ручное управление: система обеспечивает возможности вспомогательного мониторинга, что означает, что все динамические задачи должны выполняться вручную.

Первый уровень – вспомогательное управление: автоматизация повторных действий или удаление избыточной информации на основе правил.

Второй уровень – частично автономная сеть: система позволяет осуществлять эксплуатацию и техническое обслуживание с замкнутым контуром для определенных блоков на основе моделей интеллектуального анализа данных.

Третий уровень – условно автономная сеть: опираясь на возможности 2 уровня, система «с интеллектом» может «чувствовать» изменения окружающей среды в реальном времени, а в некоторых сетевых доменах оптимизировать и настроить себя на внешнюю среду, чтобы обеспечить управление замкнутым циклом, основанное на AI.

Четвертый уровень – высоко автономная сеть: опираясь на возможности 3 уровня, система позволяет в более сложной междоменной среде ана-

лизировать и принимать решения, основанные на прогнозируемом или активном замкнутом управлении сетями, ориентированными на обслуживание и клиентский опыт.

Пятый уровень – полностью автономная сеть: высший уровень автоматизации на основе сквозного взаимодействия всех уровней и доменов, а также кросс-доменного взаимодействия [5].

Применение AI в работе автономных сетей связи

Пятый уровень является конечной целью эволюции телекоммуникационных сетей. Ожидается наличие системы с возможностями замкнутого цикла автоматизации по нескольким услугам, функции которой:

- Программно и постоянно проверять сеть.
- Автоматическое исправление проблем.
- Проверка сети после внесения изменений.

Машинное обучение (ML – *Machine Learning*) [6], вероятно, будет играть ключевую роль в создании автоматизированных и самоуправляемых сетей. Рассмотрим несколько направлений применения методов интеллектуального анализа, в том числе и AI, для автономных сетей связи.

1. AI поддерживает сквозную автоматизацию, само-оптимизацию сети и TCO (*Total Cost of Ownership*) [7].

Достижения AI и ML делают возможной сквозную автоматизацию замкнутого контура с помощью NFV (*Network Function Virtualization*) [8], что будет иметь важное значение для удаленного мониторинга и управления тысячами периферийных местоположений сети и миллиардами подключенных устройств. Будучи интегрированными с системами операционной поддержки и бизнеса (OSS/BSS), возможности сетевого мониторинга и прогнозирующей сетевой аналитики на основе AI будут обнаруживать сетевые аномалии и сбои, анализировать основные причины и запускать восстановление после сбоев до того, как сбои действительно произойдут в сети. Самоконтроль, самоуправление и самовосстановление сетей позволяют динамически регулировать распределение ресурсов и энергопотребление, что приведет к сокращению затрат на развертывание дорогостоящего технического персонала.

2. Аналитика зашифрованного трафика.

По оценкам Google, более 90 процентов всего веб-трафика Google зашифровано, а по оценкам Gartner, в 2019 году зашифровано 80 процентов корпоративного веб-трафика. Хотя это большой прогресс, злоумышленники могут использовать методы шифрования, чтобы избежать обнаружения и замаскировать вредоносные атаки. Сегодня большинство предприятий не могут просматривать зашифрованный трафик и проводить глубокую проверку пакетов на наличие вредоносного контента, но AI обещает новые

меры защиты от этих атак. Заполняя модели AI данными телеметрии, такими как последовательность пакетов, границы пакетов, характер вычислительных операций и шаблоны доступа к памяти, можно эффективно и действенно выполнять обнаружение вторжений в реальном времени, изоляцию сети и превентивные действия с зашифрованным трафиком.

3. Оптимизация радиопокрытия и энергозатрат.

Применение AI поможет оптимизировать беспроводное покрытие и пропускную способность, реализовать улучшенное управление трафиком, динамическое распределение пользователей по частотам для улучшения взаимодействия с пользователем, динамическое управление радиоресурсами, управление трафиком с множественным радиодоступом, управление ресурсами с учетом обслуживания для сетевых сегментов.

Одним из крупнейших нововведений в беспроводных сетях является технология MIMO (*Multiple Input Multiple Output*) [9], которая расширяет пропускную способность радиолинии с использованием нескольких передающих и приемных антенн. Модель глубокого обучения, обученная с использованием исторических данных временных рядов, может непрерывно оптимизировать диаграммы направленности на основе типа устройства, местоположения пользователя, поведения трафика, помех и других параметров. Потребление энергии – это одна из областей, в которой поставщики услуг связи могут применять эту инновацию для значительной экономии средств. По аналогии с автоматизацией с обратной связью сетевые операторы могут применять модели машинного обучения, основанные на моделях трафика, для прогнозирования объемов трафика и оптимизации энергопотребления (перевода в состояние низкой мощности) радиооблаков.

Список используемых источников

1. Huawei's Global Industry Vision 2025: Unfolding the Industry Blueprint of an Intelligent World // huawei.com URL: https://www.huawei.com/en/press-events/news/2018/4/Huawei-Global-Industry-Vision-2025 (дата обращения 10.01.2020).

2. 5G Network Planning and Optimization // ieeexplore.ieee.org URL: https://ieeexplore.ieee.org/abstract/document/8788401 (дата обращения 5.10.2019).

3. Digital Transformation Initiative. Telecommunications Industry // reports.weforum.org URL: http://reports.weforum.org/digital-transformation/wp-content/blogs.dir/94/mp/files/pages/files/dti-telecommunications-industry-white-paper.pdf (дата обращения 22.12.2019).

4. Autonomous Networks: Empowering Digital Transformation for the Telecoms Industry // tmforum.org URL: https://www.tmforum.org/wp-content/uploads/ 2019/05/22553-Autonomous-Networks-whitepaper.pdf (дата обращения 20.10.2019).

5. Intelligent Network O&M in the Era of Cloud Computing // e.huawei.com URL: https://e.huawei.com/in/publications/global/ict_insights/201710091554/special-report/201710101105 (дата обращения 13.02.2020).

6. Machine Learning. What it is and why it matters // sas.com URL: https://www.sas.com/en_us/insights/analytics/machine-learning.html (дата обращения 21.01.2020).

7. Total cost of ownership (TCO) – 3 Key Components of TCO // purchasing-procurement-center.com URL: https://www.purchasing-procurement- center.com/total-cost-of-ownership.html (дата обращения 12.12.2019).

8. Как проблемы операторов связи решит Network Function Virtualization (NFV)? // networkguru.ru URL: https://networkguru.ru/network-function-virtualization-nfv/ (дата обращения 12.03.2019).

9. What is MIMO Wireless Technology // electronics-notes.com URL: https://www.electronics-notes.com/articles/antennas-propagation/mimo/what-is-mimo-multiple-input-multiple-output-wireless-technology.php (дата обращения 18.11.2019).

УДК 004.056
ГРНТИ 49.33.35

АДАПТАЦИЯ БИОИНСПИРИРОВАННЫХ АЛГОРИТМОВ ОБНАРУЖЕНИЯ КИБЕРАТАК ДЛЯ АНАЛИЗА БОЛЬШИХ ОБЪЕМОВ СЕТЕВОГО ТРАФИКА

Д. А Клеверов, И. В. Котенко

Санкт-Петербургский институт информатики и автоматизации Российской академии наук

С появлением технологий больших данных и ростом сложности атак, существующие алгоритмы анализа сетевого трафика требуют серьезной доработки. В статье представлено современное состояние в области обнаружения вторжений на основе биоинспирированных алгоритмов, а также предложены различные подходы к адаптации таких алгоритмов для анализа трафика сверхвысоких объемов.

биоинспирированные алгоритмы, обнаружение вторжений, большие данные, генетический алгоритм, искусственная иммунная система.

Современные системы используют модельный подход к обнаружению атак, в котором нормальное или анормальное поведение обобщается в адаптирующейся модели [1]. Перспективным направлением с точки зрения такого моделирования являются биоинспирированные алгоритмы [2]. Однако в условиях больших данных, данные алгоритмы нуждаются в переработке и адаптации к сверхбольшим объемам трафика.

Трафик сверхвысоких объемов

Рассмотрим анализ трафика сверхвысоких объемов в виде процесса, реализуемого системой обработки больших данных. Этот анализ является многоступенчатым, как показано на схеме, представленной на рис. 1.

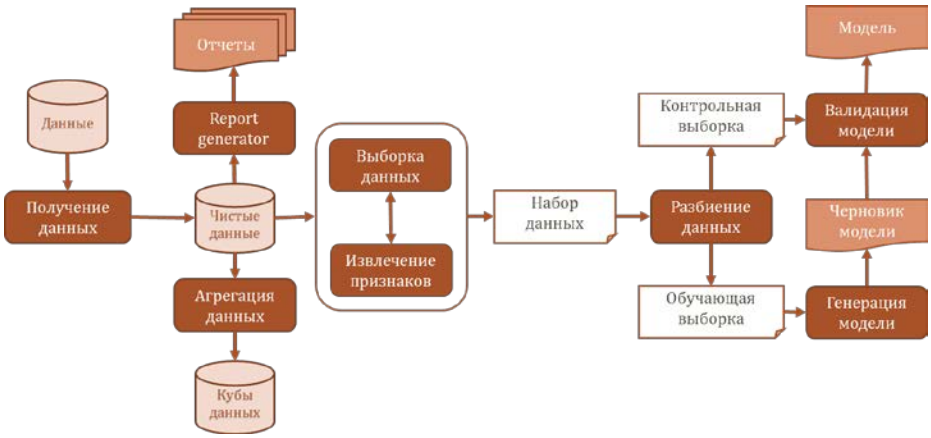


Рис. 1. Схема анализа больших данных

Такой анализ производится с учетом параметров (характеристик) обрабатываемых данных и процесса обработки, таких как объем, разнородность, скорость обработки, достоверность и изменчивость. На вход такой системе поступают сырые данные (сетевой трафик). Далее происходит очистка этих данных, которая может включать в себя предобработку, например, предварительную кластеризацию. Далее осуществляется реорганизация данных (для упрощения их интерпретации и хранения в памяти), а также вычленение важных атрибутов данных. Финальные этапы представлены моделями машинного обучения.

Биоинспирированные алгоритмы обнаружения вторжений

Под этими алгоритмами понимается целый класс алгоритмов, представляющих собой алгоритмы оптимизации, основанные на сходстве с природными сущностями и явлениями. Выделим биоинспирированные алгоритмы, основанные на эволюционных вычислениях, роевом интеллекте, иммунных системах и экологических алгоритмах.

Эволюционные алгоритмы. Эволюционные алгоритмы – это алгоритмы поиска для решения задач оптимизации и моделирования путём подбора и комбинирования искомых параметров с использованием механизмов, напоминающих биологическую эволюцию. Суть алгоритма состоит в генерации некоторой популяции генов в хромосомах с последующей оценкой их функции приспособленности и отборе наиболее удачных экземпляров. В обнаружении вторжений такие алгоритмы применяются для классификации [3], генерации правил [4], подбора параметров для других алгоритмов [5], а также извлечения важных атрибутов данных [6]. В качестве одной

из значимых областей применения этих алгоритмов является администрирование сетей [7, 8].

Роевой интеллект. В алгоритмах этой группы все индивиды системы взаимодействуют для достижения общей цели, следуя ряду простых правил, что приводит к выработке глобального роевого поведения в отличие от индивидуального. Алгоритмы на основе роя могут быть применены для задач обнаружения вторжений. Так муравьиный алгоритм [9] использовался для детектирования DoS-атак [10], выявления DDoS-атак [11], в том числе с использованием набора данных KDD-99 [12]. Пчелиный алгоритм нашел своё применение в работе [13], касающейся беспроводных сетей. Алгоритмы роя используются и в комбинации с другими алгоритмами [14].

Иммунные системы. В алгоритмах искусственной иммунной системы (ИИС) различные индивиды в группе выполняют разные задачи. Подход вдохновлен иммунными клетками человека, среди которых можно несколько видов клеток, такие как антитела, антигены и клетки памяти. Данная модель предложена в работе [15] и дополнялась в работах [16, 17]. ИИС в обнаружении вторжений использовались для классификации трафика [18], генерации правил в комбинации с алгоритмами эволюции [19] и машинного обучения [20].

Экологические алгоритмы. Эти алгоритмы основаны на взаимодействии видов внутри экосистемы. В экосистеме такое взаимодействие может быть внутривидовым и внешним, помогающим и соревновательным. Примечательными здесь являются алгоритмы P2SO [21], IWO [22], биогеографический алгоритм [23].

Биоинспирированные алгоритмы для анализа больших данных

Ряд работ, посвящен адаптации генетических алгоритмов к технологиям больших данных, а именно улучшению результатов кластеризации данных [24], планированию ресурсов [25] и отбору признаков [26]. Однако эти работы не касаются темы безопасности напрямую.

Роевые алгоритмы являются новой областью науки. При этом существует несколько модификаций исходных алгоритмов для задач кластеризации [27], балансировки нагрузки [28] и отбора признаков [29]. В работе [30] роевой алгоритм бактериального кормления использован для задач анализа сетевого трафика.

В качестве значимой модификации ИИС можно выделить многокритериальную клональную селекцию [31], показавшую хорошие результаты оптимизации функций в условиях изменчивости исходных данных и алгоритм [32] уменьшающий размерность данных.

Предлагаемый подход и дальнейшие исследования

Проблема адаптации алгоритмов в исследованиях авторов статьи рассматривается с двух сторон. С одной стороны, выявлены различные этапы обработки больших данных и предложены алгоритмы, которые могут быть использованы на каждом этапе. С другой стороны, предложен подход по адаптации алгоритмов с учетом характеристик данных.

Позадачный подход. Для исходной схемы анализа на шаге предварительной обработки данных могут использоваться наработки, посвященные кластеризации данных с использованием генетических алгоритмов. На шаге представления данных таких алгоритмов пока не используется. Генетические алгоритмы и алгоритмы роя могут быть использованы для извлечения атрибутов и подбора параметров модели. Однако данные подходы требуют адаптации под конкретную область компьютерной безопасности. Основываясь на этих результатах, можно сделать предположение, что дальнейшие исследования будут посвящены изучению применимости иммунной системы и экологических алгоритмов на различных этапах анализа. Кроме того, в области отбора атрибутов еще не проверена применимость генетических, роевых и экологических алгоритмов к задаче обнаружения вторжений.

Подход, основанный на данных. Разрабатывая систему обнаружения вторжений, нужно учитывать все перечисленные характеристики больших данных. Для этих целей предлагается использовать многокритериальный алгоритм клональной селекции в такой системе, так как он хорошо себя показал в средах с изменчивыми и разнородными данными.

Для адаптации к объемам данных следует использовать распределенные версии биоинспирированных алгоритмов, однако лишь малое число работ посвящено вычислительной сложности и оптимизации данных алгоритмов под конкретные задачи.

Для поддержки достоверности данных возможно использование эволюционных стратегий и экологических алгоритмов с целью контроля допустимых уровней изменения атрибутов и избавления от шума в данных.

Данное исследование проводится при поддержке Минобрнауки России в рамках Соглашения № 05.607.21.0322 (идентификатор RFMEFI60719X0322).

Список используемых источников

1. Branitskiy A., Kotenko I. Hybridization of computational intelligence methods for attack detection in computer networks // J. Comput. Sci. Elsevier, 2017. Vol. 23. PP. 145–156.

2. Dressler F., Akan O. Bio-inspired networking: From theory to practice // IEEE Commun. Mag. 2010. Vol. 48, No 11. PP. 176–183.

3. Chittur A. Model generation for an intrusion detection system using genetic algorithms // High School Honors Thesis, Ossining High School. In. 2001.

4. Li W. Using genetic algorithm for network intrusion detection // Proc. United States Dep. Energy Cyber Secur. Gr. 2004 Train. Conf. Kansas City, Kansas. 2004. PP. 24–27.

5. Kim D. S., Nguyen H. N., Park J. S. Genetic algorithm to improve SVM based network intrusion detection system // Proceedings – International Conference on Advanced Information Networking and Applications, AINA. IEEE, 2005. Vol. 2. PP. 155–158.

6. Xia T. et al. An efficient network intrusion detection method based on information theory and genetic algorithm // Conference Proceedings of the IEEE International Performance, Computing, and Communications Conference. IEEE, 2005. PP. 11–17.

7. Mueller-Bady R. et al. Using Genetic Algorithms for Deadline-Constrained Monitor Selection in Dynamic Computer Networks // Proceedings of the Companion Publication of the 2015 on Genetic and Evolutionary Computation Conference - GECCO Companion ’15. New York, New York, USA: ACM Press, 2015. PP. 867–874.

8. Saenko I., Kotenko I. Administrating role-based access control by genetic algorithms // Proceedings of the Genetic and Evolutionary Computation Conference Companion on – GECCO ’17. New York, New York, USA: ACM Press, 2017. PP. 1463–1470.

9. Colorni A., Dorigo M., Maniezzo V. Distributed Optimization by ant colonies // Proceedings of the First European Conference on Artificial Life. 1991. PP. 134–142.

10. Gupta A. et al. Intelligent perpetual echo attack detection on user datagram protocol port 7 using ant colony optimization // Proceedings – International Conference on Electronic Systems, Signal Processing, and Computing Technologies, ICESC 2014. IEEE, 2014. PP. 419–424.

11. Chen H. H., Huang S. K. LDDoS attack detection by using ant colony optimization algorithms // J. Inf. Sci. Eng. 2016. Vol. 32, No 4. PP. 995–1020.

12. Cai C., Yuan L. Intrusion detection system based on ant colony system // J. Networks. Academy Publisher, 2013. Vol. 8, No 4. PP. 888–894.

13. Barani F., Barani A. Dynamic intrusion detection in AODV-based MANETs using memetic artificial bee colony algorithm // 22nd Iranian Conference on Electrical Engineering, ICEE 2014. IEEE, 2014. PP. 1040–1046.

14. Qian Q., Cai J., Zhang R. Intrusion detection based on neural networks and Artificial Bee Colony algorithm // 2014 IEEE/ACIS 13th International Conference on Computer and Information Science, ICIS 2014 - Proceedings. IEEE, 2014. PP. 257–262.

15. Dasgupta D., Forrest S. Artificial immune systems in industrial applications // Proceedings of the 2nd International Conference on Intelligent Processing and Manufacturing of Materials, IPMM 1999. IEEE, 1999. Vol. 1. PP. 257–267.

16. Wang D. et al. Exploiting Artificial Immune systems to detect unknown DoS attacks in real-time // 2012 IEEE 2nd International Conference on Cloud Computing and Intelligence Systems. IEEE, 2012. PP. 646–650.

17. Garrett S.M. Parameter-free, adaptive clonal selection // Proceedings of the 2004 Congress on Evolutionary Computation, CEC2004. IEEE, 2004. Vol. 1. PP. 1052–1058.

18. Hofmeyr S.A., Forrest S. Architecture for an Artificial Immune System // Evol. Comput. MIT Press 238 Main St., Suite 500, Cambridge, MA 02142-1046 USA journals-info@mit.edu, 2000. Vol. 8, No 4. PP. 443–473.

19. Shen J., Wang J. Network intrusion detection by artificial immune system // IECON Proceedings (Industrial Electronics Conference). IEEE, 2011. PP. 4716–4720.

20. Branitskiy A.A. Hierarchical hybridization of binary classifiers for detecting anomalous network connections // SPIIRAS Proc. 2017. Vol. 3, No 52. PP. 204–233.

21. Fong S., Wong R., Vasilakos A. V. Accelerated PSO Swarm Search Feature Selection for Data Stream Mining Big Data // IEEE Trans. Serv. Comput. Institute of Electrical and Electronics Engineers, 2016. Vol. 9, No 1. PP. 33–45.

22. Rezaei Pouya A., Solimanpur M., Jahangoshai Rezaee M. Solving multi-objective portfolio optimization problem using invasive weed optimization // Swarm Evol. Comput. Elsevier B.V., 2016. Vol. 28. PP. 42–57.

23. Pu X. et al. Developing a Novel Hybrid Biogeography-Based Optimization Algorithm for Multilayer Perceptron Training under Big Data Challenge // Sci. Program. 2018. Vol. 2018.

24. Saida I.B., Nadjet K., Omar B. A new algorithm for data clustering based on cuckoo search optimization // Advances in Intelligent Systems and Computing. Springer, Cham, 2014. Vol. 238. PP. 55–64.

25. Kune R. et al. Genetic Algorithm Based Data-Aware Group Scheduling for Big Data Clouds // Proceedings - 2014 International Symposium on Big Data Computing, BDC 2014. IEEE, 2015. PP. 96–104.

26. Mafarja M. M., Mirjalili S. Hybrid Whale Optimization Algorithm with simulated annealing for feature selection // Neurocomputing. Elsevier, 2017. Vol. 260. PP. 302–312.

27. Ilango S. S. et al. Optimization using Artificial Bee Colony based clustering approach for big data // Cluster Comput. Springer, 2018. Vol. 22, No S5. PP. 1–9.

28. Hossain M. S. et al. Big Data-Driven Service Composition Using Parallel Clustered Particle Swarm Optimization in Mobile Environment // IEEE Trans. Serv. Comput. 2016. Vol. 9, No 5. PP. 806–817.

29. Banerjee S., Badr Y. Evaluating Decision Analytics from Mobile Big Data using Rough Set Based Ant Colony. Springer, Cham, 2018. PP. 217–231.

30. Neeba E.A., Koteeswaran S. Bacterial foraging information swarm optimizer for detecting affective and informative content in medical blogs // Cluster Comput. Springer, 2017. Vol. 22, No S5. PP. 1–14.

31. Luo W. et al. A clonal selection algorithm for dynamic multimodal function optimization // Swarm Evol. Comput. Elsevier, 2019. Vol. 50. PP. 100459.

32. Brown J., Anwar M., Dozier G. An artificial immunity approach to malware detection in a mobile platform // Eurasip J. Inf. Secur. SpringerOpen, 2017. Vol. 2017, No 1. PP. 7.

УДК 004.056
ГРНТИ 49.33.35

ОТБОР ПРИЗНАКОВ БОЛЬШИХ ДАННЫХ С ПОМОЩЬЮ АЛГОРИТМОВ БИКЛАСТЕРИЗАЦИИ В ЗАДАЧЕ ОБНАРУЖЕНИЯ КИБЕРАТАК

М. А. Клеверов, И. В. Котенко

Санкт-Петербургский институт информатики и автоматизации Российской академии наук

В настоящее время необходимость работы с большими данными является одной из ключевых проблем области обнаружения атак. Для решения этой проблемы многие авторы используют различные методики отбора важных признаков. В работе продемонстрирован подход, использующий методы бикластериации и позволяющий выбрать наиболее важные для детектирования атаки атрибуты данных, основываясь на ана-

лизе результатов других алгоритмов. Алгоритмы бикластеризации известны своей способностью предоставлять интерпретируемый результат, что делает предложенный подход перспективным для поиска путей комбинирования различных алгоритмов.

отбор признаков, машинное обучение, ансамблевая классификация, бикластеризация.

Современные тенденции обнаружения кибератак

Сложность обеспечения безопасности в киберпространстве обуславливается множеством особенностей:

– во-первых, объем потоков данных велик, что делает его непрактичным для ручного анализа;

– во-вторых, постоянно появляются новые уязвимости, что заставляет использовать недолговечные модели и различные адаптивные алгоритмы.

Подобные ограничения естественным образом подводят к активному применению методик машинного обучения, предпочитая их классическим алгоритмам [1]. Обратившись к современным обзорам использования методов машинного обучения для обнаружения атак [2, 3, 4] несложно выяснить, что основной интерес для специалистов в этой области представляют различные алгоритмы классификации и методы их улучшения.

Можно выделить два основных направления подобных улучшений.

Одно из них – объединение классификаторов и других методик машинного обучения для разной вспомогательной работы. Различные методики могут использоваться для уменьшения размерности данных, как, например, в работе Салама и др. [5] объединяют ограниченную машину Больцмана (RBM) для уменьшения размерности данных и известный классификатор SVM для улучшения качества обнаружения аномалий. Этот результат был закреплён авторами и другой статьи [6], в которой представлена модифицированная версия аналогичной комбинации.

Другое направление связано с комбинацией именно классификаторов. В одной из ранних работ в этой области [7] исследуют возможность объединения SVM с другим классификатором – байесовским. Следует отметить, что несмотря на повсеместную известность таких классических алгоритмов, различные варианты их объединения по-прежнему исследуются научным сообществом в области обнаружения атак. Например, в 2016 году вышла обзорная статья [8], исследующая результативность объединения уже упомянутого SVM с прочими классификаторами. Согласно этой работе, наиболее эффективно совместное использование SVM и методики Random Forest [9].

Совсем недавние работы связаны с объединением множества классификаторов. Например, в работе 2018 года [10] предлагается новый подход к определению весов классификаторов, основываясь на функции потерь специального вида, оптимизировав которую можно добиться качественной

классификации даже с использованием примитивных байесовских классификаторов. Более громоздкая, однако позволяющая использовать деревья решений, сходная методика представлена годом ранее в работе [11].

Таким образом, в качестве основных тенденций в обнаружении кибератак с учетом обработки больших данных за последнее время можно выделить комбинирование нескольких классификаторов и объединение классификаторов с другими методиками машинного обучения, преимущественно для отбора признаков.

Данная работа ставит своей целью предложить подход к классификации, сочетающий в себе обе эти тенденции, что говорит в пользу её актуальности, теоретической и практической значимости.

Комбинирование классификаторов

Сама по себе классификация достигла пика своего развития к ранним 1980-ым, сместив научный интерес и фокус развития в сторону комбинирования различных решений и оптимизации не одного конкретного классификатора, а целой совокупности в целом [12].

С точки зрения процесса обучения алгоритмы такой оптимизации, в целом, можно разделить на три большие группы [13]:

– использующие разные данные для обучения, но один алгоритм обучения (как это делается в процессе бустинга [14]);

– использующие различные параметры обучения, но один метод обучения;

– использующие разные методы обучения.

С точки зрения парадигмы комбинирования решений классификаторов, отечественные учёные [12] выделяют две крупные группы: оперирующие так называемой компетентностью классификатора в данной области пространства признаков и объединяющие решения классификаторов, считая их одинаково компетентными.

Особый интерес для авторов данной статьи представляют алгоритмы первой группы, в которых делается предположение, что каждый классификатор компетентен, как минимум, на части данных. Это предположение, в теории, позволяет, скомбинировав несколько компетентных классификаторов получить некоторое качественное решение. Однако, в подобном подходе возникает вопрос о полноте покрытия пространства признаков. В данной работе мы предлагаем возможное решение этого вопроса.

Бикластеризация для отбора признаков

Рассмотрим два множества классификаторов и некоторый набор данных. Затем составим матрицу важностей признаков для решений этих классификаторов на этих данных. Для каждого алгоритма алгоритм вычисления

этой важности специфичен. Например, в случае алгоритмов, основанных на деревьях решений, можно воспользоваться методикой упомянутой в статье [11].

Таким образом можно получить числовую матрицу потенциально высокой размерности, которую возможно проанализировать алгоритмами бикластеризации. Такие алгоритмы популярны в анализе биомедицинских данных [15].

Цель этих алгоритмов упрощённо может быть сформулирована как поиск подматриц в исходной матрице данных, удовлетворяющих определённым свойствам «плотности» [16].

Применение алгоритмов бикластеризации позволяет выявлять кластеры объектов (в нашем случае классификаторов), ведущих себя сходным образом на некотором подмножестве признаков. То есть, найдя бикластер, мы найдём группы классификаторов, учитывающих некоторые признаки сходным образом.

В дальнейшем, выбрав классификаторы из разных бикластеров можно определить оптимальное объединение решений, которое учитывает все особенности данных и добивается, в теории, лучшего качества классификации.

Кроме того, можно оценить множества признаков в силу того, что выполняется двойная кластеризация. «Равноправие» кластеризаций [17] по обоим измерениям (множеству объектов и их признаков) позволяет находить «устойчивые» комбинации признаков, которые важны в нескольких алгоритмах.

Некоторые недавние исследования [18] демонстрируют перспективность применения алгоритмов кластеризации для отбора признаков, а сами алгоритмы бикластеризации могут применяться как вспомогательный инструмент классификации [19], что позволяет делать предположения о возможности применения описанной концепции.

Детальная проработка данной концепции, а также её качественная экспериментальная проверка остаются темой дальнейших исследований нашего коллектива.

Работа выполнена при частичной поддержке бюджетной темы № 0060-2019-0010.

Список используемых источников

1. Guan Z. et al. When Machine Learning meets Security Issues: A survey // 2018 International Conference on Intelligence and Safety for Robotics, ISR 2018. IEEE, 2018. PP. 158–165.

2. da Costa K. A. P. et al. Internet of Things: A survey on machine learning-based intrusion detection approaches // Comput. Networks. Elsevier B.V., 2019. Vol. 151. PP. 147–157.

3. Khraisat A. et al. Survey of intrusion detection systems: techniques, datasets and challenges // Cybersecurity. SpringerOpen, 2019. Vol. 2, No 1. PP. 20.

4. Zamani M., Movahedi M. Machine Learning Techniques for Intrusion Detection. 2013. PP. 1–11.

5. Salama M. A. et al. Hybrid intelligent intrusion detection scheme // Advances in Intelligent and Soft Computing. Springer, Berlin, Heidelberg, 2011. Vol. 96 AISC. PP. 293–303.

6. Dong B., Wang X. Comparison deep learning method to traditional methods using for network intrusion detection // Proceedings of 2016 8th IEEE International Conference on Communication Software and Networks, ICCSN 2016. IEEE, 2016. PP. 581–585.

7. Kamdar A. B., Jay J. M. A survey: classification of huge cloud Datasets with efficient Map - Reduce policy // Int. J. Eng. Trends Technol. 2014. Vol. 18, No 2. PP. 103–107.

8. Chand N. et al. A comparative analysis of SVM and its stacking with other classification algorithm for intrusion detection // 2016 International Conference on Advances in Computing, Communication, & Automation (ICACCA) (Spring). IEEE, 2016. PP. 1–6.

9. Resende P. A. A., Drummond A. C. A survey of random forest based methods for intrusion detection systems // ACM Computing Surveys. ACM, 2018. Vol. 51, No 3. PP. 1–36.

10. Özgür A., Nar F., Erdem H. Sparsity-driven weighted ensemble classifier // Int. J. Comput. Intell. Syst. 2018. Vol. 11, No 1. PP. 962–978.

11. Branitskiy A. A. Hierarchical hybridization of binary classifiers for detecting anomalous network connections // SPIIRAS Proc. 2017. Vol. 3, No 52. PP. 204–233.

12. Городецкий В. И., Серебряков С. В., Петербургский С. Методы и алгоритмы коллективного распознавания : обзор. 2006. Т. 9181, № 3. С. 139–171.

13. Kotsiantis S. B., Zaharakis I. D., Pintelas P. E. Machine learning: A review of classification and combining techniques // Artif. Intell. Rev. 2006. Vol. 26, No 3. PP. 159–190.

14. Schapire R. E. Using output codes to boost multiclass learning problems // Proc. Fourteenth Int. Conf. Mach. Learn. 1997. No 1. PP. 1–9.

15. Pontes B., Giráldez R., Aguilar-Ruiz J.S. Biclustering on expression data: A review // J. Biomed. Inform. Elsevier Inc., 2015. Vol. 57. PP. 163–180.

16. Игнатов Д.И., Кузнецов С.О. Бикластеризация объектно-признаковых данных на основе решеток замкнутых множеств// Труды 12-й национальной конференции по искусственному интеллекту. М. : Физматлит, 2010. Т. 1. С.175–182.

17. Игнатов Дмитрий. Методы бикластеризации для анализа интернет-данных [Electronic resource]. 2008. URL: http://citforum.ru/consulting/BI/biclustering/ (accessed: 22.02.2019).

18. Lohrmann C., Luukka P. Using Clustering for Supervised Feature Selection to Detect Relevant Features // Lecture Notes in Computer Science (including subseries Lecture Notes in Artificial Intelligence and Lecture Notes in Bioinformatics). Springer, 2019. Vol. 11943 LNCS. PP. 272–283.

19. Asgarian N., Greiner R. BIOINFORMATICS Using Rank-1 Biclusters to Classify Microarray Data. 2007. PP. 1–9.

УДК 004.056.3
ГРНТИ 49.33.29

ОРГАНИЗАЦИЯ РЕЗЕРВНОГО КОПИРОВАНИЯ И ВОССТАНОВЛЕНИЯ ИНФОРМАЦИИ В ЛОКАЛЬНЫХ ВЫЧИСЛИТЕЛЬНЫХ СЕТЯХ СИСТЕМ УПРАВЛЕНИЯ СПЕЦИАЛЬНОГО НАЗНАЧЕНИЯ

И. С. Ковалев, В. В. Пащенко

Военная академия связи им. Маршала Советского Союза С. М. Буденного

Рассмотрены проблемы существующих методов резервного копирования и восстановления информации. Предложены варианты резервного копирования и восстановления информации по локальной вычислительной сети.

резервное копирование и восстановление информации; файловая резервная копия; инкрементное, дифференциальное, полное копирование.

В современных условиях в локальных вычислительных сетях (ЛВС) систем управления специального назначения обрабатываются огромные объёмы крайне важной информации [1]. Для исключения потерь этой информации и обеспечения непрерывности собственно процесса управления возникает острая необходимость периодически производить ее резервное копирование и, при необходимости, восстановление.

Сегодня резервное копирование информации в таких сетях обычно осуществляется на специализированном рабочем месте путем подключения к нему извлеченного из рабочей станции жёсткого диска, с которого необходимо произвести резервное копирование. Восстановление информации также производится с использованием этого же специализированного рабочего места. Такая процедура не оказывает особого влияния на сам процесс управление в повседневной деятельности, ибо обычно производится в нерабочее время. В случае же резких изменений обстановки зачастую возникает острая необходимость в круглосуточном производстве множество различных расчётов в локальной вычислительной сети, что исключает возможность прерывания процесса управления. Все это приводит к возникновению проблем, связанных со своевременным копированием информации и, как следствие, проблем восстановления скопированной ранее информации.

Для осуществления собственно процедуры резервного копирования обычно создаются специальные подсистемы, называемые подсистемами резервного копирования и восстановления информации (РКВИ). Обязательным условием успешного функционирования таких подсистем

является хранение информации, предназначенной для восстановления, отдельно от системных файлов. Этот принцип, естественно, относится как к файловым архивам, так и к образам дисков. При коллективном использовании информации должностными лицами органов управления систем специального назначения данный принцип должен реализовываться еще жестче: как минимум одна из копий должна храниться отдельно, чтобы не потерять информацию в случае непредвиденных обстоятельств.

При правильной организации работы подсистемы РКВИ решаются как минимум две задачи. Во-первых, обеспечение защиты всего спектра важной информации от повреждения или разрушения. Во-вторых, организация возможности быстрой «миграции» с одного автоматизированного рабочего места (АРМ) на другое, то есть, фактически обеспечение бесперебойной работы должностных лиц органов управления.

В настоящее время в зависимости от важности хранимой на АРМ информации и от частоты её использования в основу работы подсистем РКВИ положены три известных метода копирования: полное, инкрементное и дифференциальное [2, 3].

Общим для всех этих методов резервного копирования является положение, что первая копия всегда делается полной, т. е. в нее записывается вся информация, предназначенная для сохранения.

Рассмотрим каждый из методов более подробно.

При полном методе в создаваемый файл записываются все данные, выбранные для резервирования. Такие копии требуют много места на носителе, но они и самые надёжные. Ведь для восстановления потребуется только одна последняя копия.

Основа инкрементного метода копирования состоит в том, во всех копиях, начиная со второй, сохраняются только изменения, произошедшие после предыдущего копирования. Естественно, инкрементные копии всегда меньше полных, но здесь для восстановления информации потребуется последняя полная копия, а также вся последовательность инкрементных копий.

В следующие после первой копии помещаются только те файлы, информация в которых была изменена со времени создания предыдущей копии. Такой цикл повторяется снова и снова. Метод инкрементного копирования, безусловно, минимизирует расход свободного места на носителе, выбранном для резервного копирования информации. При этом очевидно, что восстановление информации здесь достаточно продолжительное. Но такой метод резервного копирования наиболее часто используется специалистами, ибо восстановление информации является довольно редкой процедурой в современных, нормально работающих, системах управления.

При дифференциальном методе в копии, следующие за первой, сохраняется только та информация, которая была изменена за время, прошедшее

после полного копирования. Для восстановления данных в данном случае потребуются последняя полная копия и последняя дифференциальная. Очевидно, дифференциальные копии всегда меньше полных, но, при этом, они больше инкрементных.

Все рассмотренные методы позволяют пользователям создавать различные схема резервного копирования и восстановления информации.

Схемы, основанные на методе полного резервного копирования, предполагают создание только полных копий. Естественно, это самые надёжные схемы. Для исключения же необоснованного увеличения места на носителе следует регулярно проводить процедуру очистки, а именно вовремя удалять устаревшие копии.

Основные недостатки данных схем понятны: создание каждой копии требует много времени; каждая копия занимает достаточно много места на носителе; существенное дублирование информации в каждой копии.

В схемах, построенных на основе инкрементного метода, после создания первой полной копии, создается последовательность инкрементных. Эти копии занимают не так много места на диске, а на их создание уходит незначительное время. Но у таких схем есть один очень существенный недостаток – их низкая надёжность. Если по какой-то причине будет повреждена любая копия в последовательности, то все следующие за ней копии просто не нужны. Выход здесь очевиден, создавать новую полную копию после четырех-пяти инкрементных.

При реализации схем на основе дифференциального метода сначала также создаётся первая полная копия, а затем последовательность дифференциальных. Очевидно, что такая схема нивелирует недостатки двух предыдущих. Т.к. дифференциальные копии меньше полных, но больше инкрементных, то у пользователя имеется некая средняя возможность при выборе вариантов точки восстановления, сохраняя при этом достаточно высокую надёжность. Тем не менее, в этом методе также имеется серьезный недостаток: со временем размер дифференциальной копии может даже превысить размер полной. Устранять его рекомендуется, создавая полную копию после двух-пяти дифференциальных.

Авторами предлагается такой способ резервного копирования и восстановления информации, который сочетает преимущества приведенных выше схем и практически исключает их недостатки (рис., см. ниже).

Суть его сводится к следующему: в ЛВС систем управления специального назначения предлагается дополнительно включить сервер РКВИ, который позволит осуществлять резервное копирование и восстановление информации по локальной вычислительной сети без отключения жёстких дисков от рабочих станций пользователей.

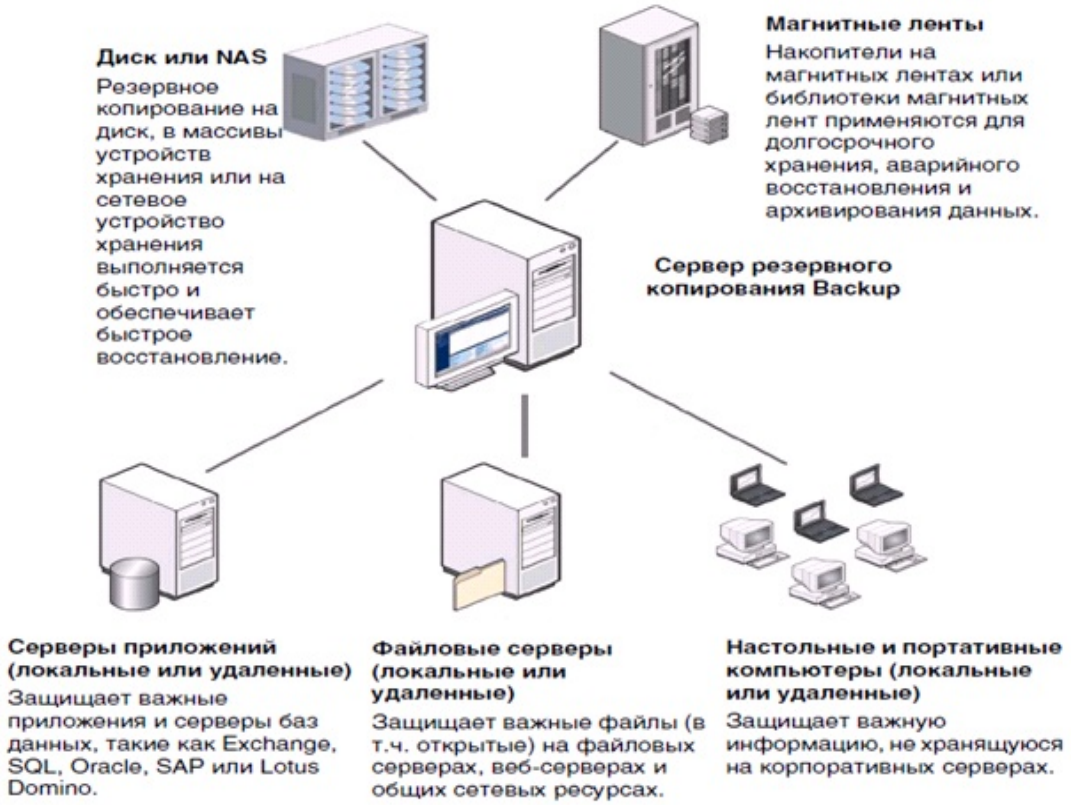


Рис. Организация РКВИ в локальной вычислительной сети

Следует отметить, что для обеспечения успешного функционирования подсистем РКВИ необходимо предусмотреть периодические (согласно разработанному графку) проверки актуальности резервных копий, т. к. сохраненные копии, по той или иной причине, могут не читаться. Например: смещение головки стримера, неправильно настроенная программа резервного копирования, ошибка оператора и т. п. Обычно такая ситуация обнаруживается только лишь при потере данных, когда потребовалась резервная копия для проведения процедуры восстановления информации. По-этому проведение периодических проверок позволит повысить уровень актуальности резервных копий, с которых будет осуществляться восстановление информации.

Данное предложение, конечно же, увеличивает количество серверов в локальной вычислительной сети, но, учитывая важность информации, обрабатываемой в системе управления специального назначения, существенно уменьшает вероятность потери этой информации, а также повышает значение показателей непрерывности собственно процесса управления.

Список используемых источников

1. Анфилатов В. С., Авраменко В. С., Пантюхин О. И. Теоретические основы автоматизации управления войсками и связью. Часть 2. Основы построения и функционирования систем автоматизации управления войсками и связью : учебное пособие. СПб. : ВАС, 2015. 304с.

2. Бережной А. Н. Сохранение данных. Теория и практика. – М. : ДМК Пресс, 2016. 318с.

3. Методика резервного копирования в быту для экономных и осторожных. [Электронный ресурс]. URL: https://www.ixbt.com/storage/backup4home-part1.shtml (дата обращения 25.11.2019).

УДК 004.056
ГРНТИ 81.93.29

ОБЕСПЕЧЕНИЕ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ WEB-ПРИЛОЖЕНИЙ С ИСПОЛЬЗОВАНИЕМ МАШИННОГО ОБУЧЕНИЯ

М. М. Ковцур, А. А. Миняев, П. А. Потемкин, Д. Д. Хамза

Санкт-Петербургский государственный университет телекоммуникаций им. проф. М. А. Бонч-Бруевича

Большинство компаний используют информационные системы для хранения и обработки данных. С ростом применения различных web-приложений увеличивается и количество всевозможных атак, с целью получения закрытой информации, начиная от всевозможных вредоносных программ (вирусов, червей и т. д.), и заканчивая социальным инжинирингом. Поэтому использование машинного обучения позволит повысить эффективность отслеживания и прогнозирования различного рода атак. В данной статье описываются механизмы безопасности web-приложений с использованием машинного обучения, а также приведены примеры успешного использования нейронных сетей в рамках обеспечения безопасности баз данных.

машинное обучение, база данных, web-приложение, мониторинг, угрозы, отслеживание, контролируемое обучение.

Web-security привлекает все больше внимания с каждым годом. Согласно исследованиям безопасности web-приложений, проведенного компанией «Positive Technologies» в период 2017–2019 гг. [1] большинство web-приложений имеют низкий уровень защищенности. Поэтому использование Machine Learning (ML), в перспективе, может решить сразу две задачи – автоматизация процессов, которые ранее требовали участия человека и быстрая обработка, с последующим анализом огромных объемов информации и расчёт параметров, используя множество переменных. Фактически, 71 % предприятий США планируют использовать ML в своих системах безопасности в 2019 году [2]. Основная цель текущей работы – разработать модель машинного обучения, обеспечивающей безопасность web-приложений. Для реализации поставленной цели были определены следующие задачи:

– изучить и сравнить алгоритмы машинного обучения;

– сравнить существующие подходы программного решения в web-security и выявить параметры и подходы, которые будут использоваться в разработке модели;

– разработать модель «Машинного обучения»;

– протестировать разработанную модель и сравнить с существующими программными подходами.

Проанализировав статистику наиболее распространённых направлений атак в 2019 году [3] были определены направления использования Machine Learning: Мониторинг, Фильтрация, Блокирование, Разграничение прав доступа, Защита БД, Защита Сервера, Шифрование, Подмена учётных данных.

Machine Learning (Машинное обучение) – это метод анализа данных, который автоматизирует построение аналитической модели. ML имеет три подкатегории: контролируемое обучение, неконтролируемое обучение и обучение с подкреплением [4]. Контролируемое обучение использует набор данных, помеченный правильными ответами для изучения. Как только модель обучена, она может начать прогнозировать или принимать решения относительно новых данных. При неконтролируемом обучении нет необходимости в таком помеченном наборе данных. Как только модель получает набор данных, она автоматически находит шаблоны и связи, создавая в ней кластеры. Однако такой тип обучения не может ничего предсказать. Усиленное обучение – это способность системы взаимодействовать с окружающей средой и определять наилучший результат. Система либо вознаграждена, либо оштрафована с баллом за правильный или неправильный ответ, и на основе полученных положительных баллов, модель тренируется сама. Точно так же после обучения он готовится предсказать новые данные, представленные ему.

Основные подходы для решения задач:

– Регрессия (или прогноз) – задача прогнозирования следующего значения на основе предыдущих значений.

– Классификация – это задача разделения вещей на разные категории.

– Кластеризация – похожа на классификацию, но классы неизвестны, группируя вещи по сходству.

– Ассоциация правила обучения (или рекомендации) – задача рекомендовать что-то на основе предыдущего опыта.

– Уменьшение размерности – или обобщение – задача поиска общих и наиболее важных признаков в нескольких примерах.

– Генеративные модели – это задача создания чего-либо на основе предыдущих знаний о дистрибуции

Область применения ML в web-security огромна, начиная с выявления аномалий и подозрительных или необычных действий и заканчивая обнаружением уязвимостей нулевого дня и исправлением известных.

Также были рассмотрены следующие примеры использования машинного обучения в web-security:

– Amazon Web Services.
– Demisto SOAR (*Security Orchestration, Automation and Response*).
– Лаборатория Касперского [5].
– Хоум Кредит Банк.
– Apache Accumulo.
– Windows Advanced Threat Protection [5].
– Web application firewall.
– AppSec [6].
– Chronicle [7].

Критериями выбора машинной модели были определены: Бесплатность, Быстродействие, Точность, Время обучения, Линейность, Количество параметров [8].

Таблица сравнения алгоритмов обучения, основанная на работе – «Сравнительный анализ методов машинного обучения для решения задачи классификации документов научно-образовательного учреждения».

Для разработки будущей модели был выбран метод контролируемого обучения – Лес деревьев принятия решений, поскольку Деревья принятия решений быстро обучаются и имеют возможность прогнозирования. Кроме того, их можно использовать для широкого круга задач, при этом не требуется особой подготовки данных [9].

Исходя из анализа существующих подходов, достоинств и недостатков была разработана архитектурная идея модели машинного обучения (рис., см. ниже).

Основным отличием от рассмотренных существующих программных реализаций можно отметить следующее: во-первых, архитектурная модель построена на методе обучения лес деревьев принятия решений, поэтому обучение модели можно контролировать и решить проблему переобучаемости при постоянном сравнении результатов предсказания и решения задач с тестовыми данными, что приведет к более точной оценке данных; во-вторых, данная модель позволяет четко классифицировать любое действие и все объекты web-приложения таким образом, что классификация будет четко определена, в отличии от реализаций основанных на методе «нейронных сетей», таких как модель от Лаборатории Касперского, AppSec и Chronicle.

В данной работе были выполнены следующие задачи:

При внедрении системы, основанной на ML, мы должны помнить, что ML не является панацеей. Ни одна система не является безопасной. При определенных условиях ML защищает уязвимости и создает новые пробелы. ML можно сравнить с собакой: «Машинное обучение может делать

все, что вы могли бы научить собаку, но вы никогда не можете быть полностью уверены, что вы научили собаку делать».

Рис. Архитектурная модель машинного обучения

В заключении, было отмечено, что последствия, которые могут привести к более активному внедрению ML [10]: во-первых, автоматизация и связанная с этим потеря рабочих мест, а во-вторых, неизбежный конфликт с существующей правовой базой, например, при использовании технологий для предотвращения киберпреступности [11] или кибертерроризма [12]. В такой ситуации обвиняемый замешан в преступлениях, которые еще не были совершены и которые не регулируются никакими правовыми нормами. Более того, некоторая информация, полученная ML, может быть частной или конфиденциальной, что нарушает законы некоторых стран. Аналогичным образом, низкое качество или недостаточное количество ОД в кибербезопасности данных на основе прогнозов может привести к неправильным решениям и непоправимым ошибкам.

Список используемых источников

1. Positive Technologies [Электронный ресурс]. URL: http://www.tadviser.ru/index.php (дата обращения 08.02.2020).

2. Businesses recognize the need for AI & ML tools in cybersecurity. Helpnetsecurity.com. Accessed: Sep. 10, 2019. [Online] Available at: https://www.helpnetsecurity.com/2019/03/14/ai-ml-tools-cybersecurity/ (дата обращения 08.02.2020).

3. Исследование безопасности больших компаний [Электронный ресурс]. URL: http://www.tadviser.ru/index.php (дата обращения 08.02.2020).

4. Котенко И. В., Левшун Д. С., Чечулин А. А., Ушаков И. А., Красов А. В. Комплексный подход к обеспечению безопасности киберфизических систем на основе микроконтроллеров // Вопросы кибербезопасности. 2018. № 3 (27). С. 29–38.

5. Advanced Threat Protection в Microsoft Defender [Электронный ресурс]. URL: https://docs.microsoft.com/ru-ru/windows/security/threat-protection/microsoft-defender-atp/microsoft-defender-advanced-threat-protection (дата обращения 10.02.2020).

6. SPEED, SMARTS, AND SCALE [Электронный ресурс]. URL: https://chronicle.security/technology/ (дата обращения 12.02.2020).

7. Краснянский М. Н., Обухов А. Д., Соломатина Е. М., Воякина А. А. Сравнительный анализ методов машинного обучения для решения задачи классификации документов научно-образовательного учреждения. Тамбов : Компьютерная лингвистика и обработка естественного языка. 2018. URL: http://www.vestnik.vsu.ru/pdf/analiz/2018/03/2018-03-19.pdf

8. Sqrrl [Электронный ресурс]. URL: https://ru.bmstu.wiki/Sqrrl (Дата обращения. 18.02.2020)

9. Безопасность облака AWS [Электронный ресурс]. URL: https://aws.amazon.com/ru/security/.

10. Виткова Л. А. Исследование распределенной компьютерной системы адаптивного действия // Наукоемкие технологии в космических исследованиях Земли. 2015. Т. 7. № 5. С. 44–48.

11. Штеренберг С. И., Виткова Л. А., Просихин В. П. Методика применения концепции адаптивной саморазвивающейся системы // Информационные технологии и телекоммуникации. 2014. Т. 2. № 4. С. 126–133.

12. Красов А. В., Штеренберг С. И., Фахрутдинов Р. М., Рыжаков Д. В., Пестов И. Е. Анализ информационной безопасности предприятия на основе сбора данных пользователей с открытых ресурсов и мониторинга информационных ресурсов с использованием машинного обучения // T-Comm: Телекоммуникации и транспорт. 2018. Т. 12. № 10. С. 36–40.

УДК 004.056
ГРНТИ 49.38.49

ЭКСПЕРИМЕНТАЛЬНАЯ ОЦЕНКА ВЕРОЯТНОСТНО-ВРЕМЕННЫХ ХАРАКТЕРИСТИК RADIUS-АВТОРИЗАЦИИ ДЛЯ СЕРВИСА IP-TB

М. М. Ковцур, А. В. Козьмян, Н. И. Малинин, Ю. В. Твердохлебова

Санкт-Петербургский государственный университет телекоммуникаций им. проф. М. А. Бонч-Бруевича

В исследовании рассматриваются клиентские авторизации для доступа к услуге IP-TV с использованием сервера RADIUS. Определены основные параметры канала связи, которые оказывают влияние на время доступа к услуге. Построены графики, демонстрирующие зависимость времени доступа к услуге IP-TV от параметров канала связи, а также вероятностные зависимости. Приводятся результаты практического

эксперимента, выполненного с целью доказательства сформированной математической модели. Выполнено сравнение результатов практического эксперимента и теоретического расчета, по итогу которого сделаны выводы.

авторизация, IGMP, IP-TB, multicast, RADIUS, математическая модель.

IP-TV – технология (стандарт) цифрового телевидения в сетях передачи данных по протоколу IP, новое поколение телевидения. Как правило, при организации вещания IP-TV по сетям с коммутацией пакетов используется многоадресная передача. Многоадресный трафик (многоадресные пакеты) используется для потоковой передачи видео [1]. Многоадресная рассылка доставляет видеоконтент неограниченному количеству подписчиков без перегрузки сети. При организации службы каждый канал представляется как отдельная многоадресная группа.

При внедрении RADIUS-авторизации для IP-TV возникают дополнительные временные затраты, вызванные необходимостью коммутатора запросить разрешение для подключения в группу каждого отдельного клиента. Параметр Radius Timeout также может оказать влияние на время получения доступа к услуге. Он задает время ожидания коммутатором ответа RADIUS Response от RADIUS-сервера, прежде чем признать попытку авторизации неудачной. Некоторые задержки в канал связи вносят периодические опросы клиентов от коммутатора IGMP General query. Все эти задержки влияют на время подключения канала. Исследование посвящено оценке влияния параметров канала связи на скорость предоставления доступа к услуге IP-TV.

Пусть используется канал связи со следующими параметрами: задержка D_{dist}, вероятность битовой ошибки P_0 и скорость C_{dist}.

Модель процесса авторизации пользователя представлена на рис. 1 и более детально описывается в работе [2].

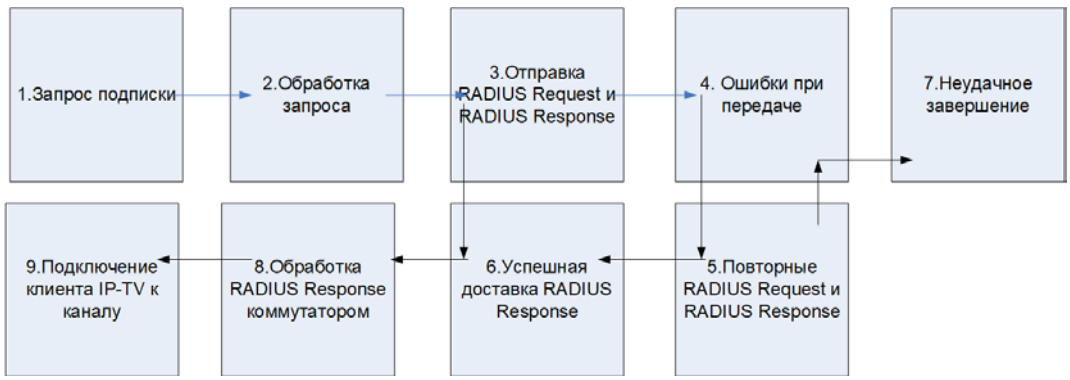


Рис. 1. Модель процесса авторизации клиента

Далее построим графики зависимостей успешного получения доступа к услуге IP-TV и времени выполнения от основных параметров канала связи [3, 4].

График зависимости времени выполнения от задержки в канале связи при битовой ошибке $P_0 = 10^{-7}$ представлен на рис. 2.

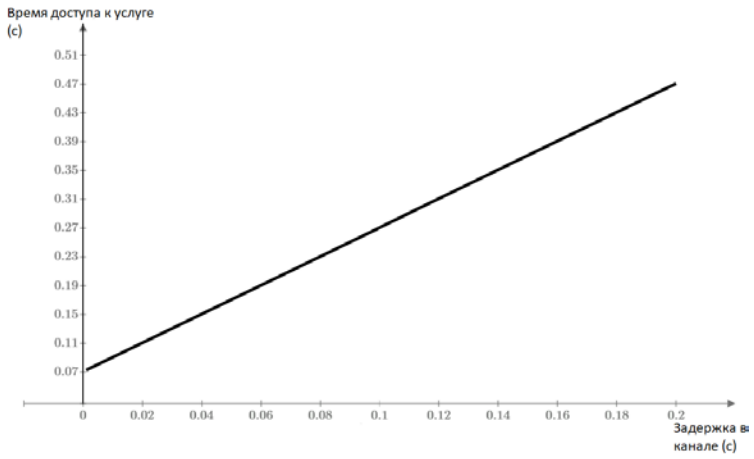


Рис. 2. График зависимости времени доступа к услуге от задержки в канале

Графики зависимости времени выполнения от битовой ошибки в канале при нескольких различных значениях задержки представлены на рис. 3.

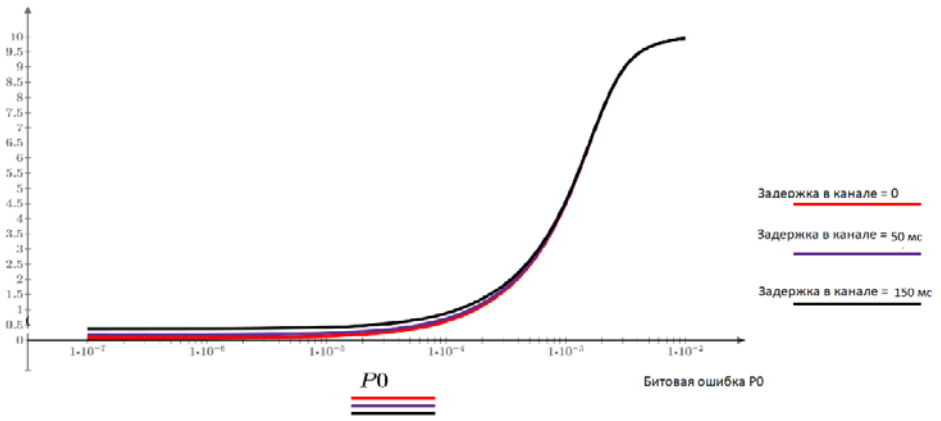


Рис. 3. График зависимости времени доступа к услуге от битовой ошибки в канале

Полученные графики позволяют предсказывать значение времени доступа к услуге при известных параметрах битовой ошибки и задержки в канале связи [5, 6]. Далее проверим полученные зависимости с помощью практического эксперимента.

Для исследования данного метода был организован стенд с оборудованием, схема которого представлена на рис. 4 (см. ниже). Оборудование было настроено на предоставление услуги IP-TV с использованием RADIUS-авторизации. Эксперимент показал, что при внедрении RADIUS-авторизации возникают дополнительные временные затраты, вызванные необходимостью коммутатора запросить разрешение для подключения в группу каждого отдельного клиента.

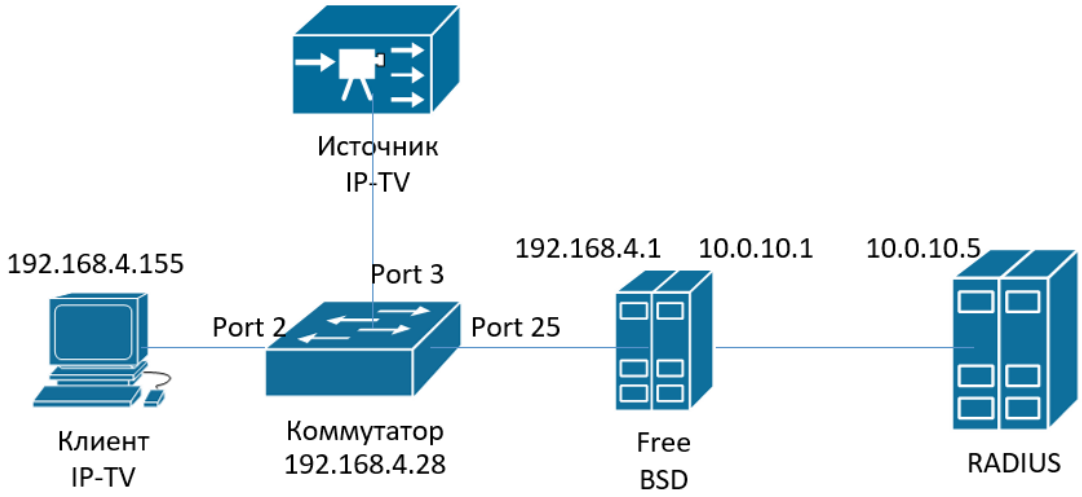


Рис. 4. Схема тестового стенда

Коммутатор настроен на обработку подписок на канал с IP-адресом 239.1.1.2, который передается источником multicast трафика на 3 порт. Была настроена RADIUS-авторизация для подписок на канал на 2 порту, к которому подключен клиентский компьютер. При запросе подписки на канал коммутатор будет отправлять запрос RADIUS-серверу, расположенному в сети 10.0.10.0 за программным маршрутизатором m0n0wall на базе операционной системы Free BSD. m0n0wall – программный межсетевой экран, который может выполнять различные манипуляции с проходящими через него пакетами с помощью специальных правил [7, 8]. Одной из его возможностей является создание правил задержки пакетов на указанное время, благодаря чему можно эмулировать наличие любых задержек в канале связи. В тестовом стенде m0n0wall выступает в роли маршрутизатора между сетями 10.0.10.0 и 192.168.4.0, при этом все пакеты, проходящие из одной сети в другую, задерживаются. В данном исследовании рассматривается влияние задержки в канале связи между коммутатором и RADIUS-сервером на время доступа к услуге IP-TV, задержка в канале связи между пользователем и коммутатором принимается нулевой.

Для расчета времени доступа к услуге IP-TV вычислялась разница во времени между пакетами с IGMP запросом на подключение к каналу и первым UDP пакетом с multicast трафиком, пример продемонстрирован на рис. 5.

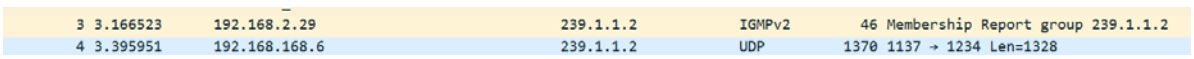


Рис. 5. Пример пакетов сетевого трафика

В таблице приводятся сводные результаты по итогам проведения эксперимента, которые отражены на графике (рис. 6).

ТАБЛИЦА. Результаты измерений

Задержка (мс)	Количество испытаний	Время доступа к услуге (мс)	Задержка Radius (мс)
0	3	80	47
5	3	92	53
25	3	130	91
50	10	182	141
75	3	223	192
100	10	283	242
150	3	419	342

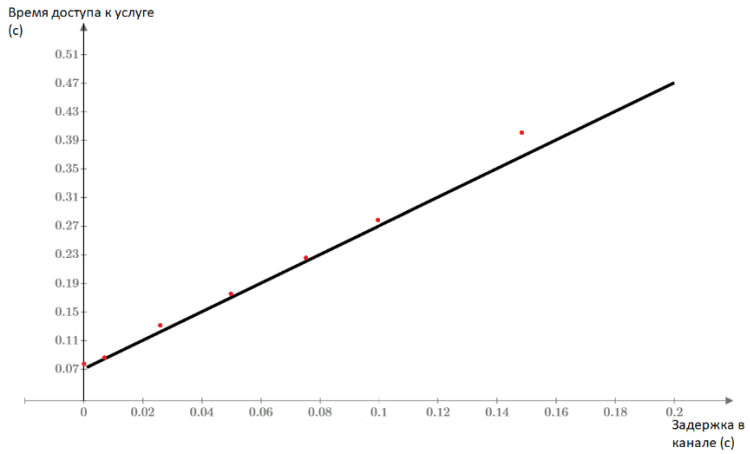


Рис. 6. Сравнение теоретической и экспериментальной зависимости времени доступа к услуге

Результаты проведенного эксперимента совпадают с теоретическими расчетами. Это позволяет применять разработанную математическую модель для определения времени доступа к услуге при использовании RADIUS-авторизации при разработке IP-TV решений. Ошибки в канале связи наиболее сильно влияют на время доступа к услуге.

Одним из возможных путей сокращения времени доступа к услуге является кеширование предыдущих RADIUS-ответов на коммутаторе, что позволит снизить нагрузку на RADIUS-сервер и сэкономить время, которое обычно тратится им на обработку запросов авторизации.

В статье показано, что применение RADIUS-авторизации позволяет обеспечить гибкий подход, однако требует дополнительных временных затрат.

Список используемых источников

1. Ковцур М. М., Поляничева А. В. Исследование механизма авторизации пользователей для доступа к IP-ТВ сервисам с применением RADIUS-сервера // Актуальные

проблемы инфотелекоммуникаций в науке и образовании (АПИНО 2018). VII Международная научно-техническая и научно-методическая конференция : сб. науч. ст. в 4-х т. 2018. С. 466–471.

2. Ковцур М. М., Козьмян А. В., Твердохлебова Ю. В. Исследование RADIUS-авторизации пользователей для сервиса IP-ТВ // Цифровой регион: опыт, компетенции, проекты. Труды II Международной научно-практической конференции. 2019. С. 351–354.

3. Гольдштейн Б. С., Елагин В. С., Сенченко Ю. Л. Протоколы AAA: RADIUS и DIAMETER. Серия «Телекоммуникационные протоколы». Книга 9. СПб. : БХВ-Петербург, 2014. 352 с.

4. Никитин В. Н., Юркин Д. В. Улучшение способов аутентификации для каналов связи с ошибками // Информационно-управляющие системы. 2010. № 6. С. 42–46.

5. Ковцур М. М., Никитин В. Н., Юркин Д. В. Оценка вероятностно-временных характеристик защищенной IP-телефонии // Защита информации. Инсайд. 2012. № 4. С. 64.

6. Красов А. В., Лосин Е. П., Ушаков И. А. Проблема безопасности передачи групповых рассылок в IP-сетях // Актуальные проблемы инфотелекоммуникаций в науке и образовании. VI Международная научно-техническая и научно-методическая конференция : сб. науч. ст. в 4-х т. 2017. С. 295–301.

7. Красов А. В., Сахаров Д. В., Ушаков И. А., Лосин Е. П. Обеспечение безопасности передачи multicast-трафика в IP-сетях // Защита информации. Инсайд. 2017. № 3 (75). С. 34–42.

8. Сахаров Д. В., Штеренберг С. И., Левин М. В., Колесникова Ю. А. Разработка модели обеспечения отказоустойчивости сети передачи данных // Известия высших учебных заведений. Технология легкой промышленности. 2016. Т. 34. № 4. С. 14–20.

УДК 004.51
ГРНТИ 81.93.29

АРХИТЕКТУРА И РЕАЛИЗАЦИЯ ВИЗУАЛЬНЫХ ИНТЕРФЕЙСОВ ДЛЯ ВЫЯВЛЕНИЯ И ПРОТИВОДЕЙСТВИЯ НЕЖЕЛАТЕЛЬНОЙ, СОМНИТЕЛЬНОЙ И ВРЕДОНОСНОЙ ИНФОРМАЦИИ

М. В. Коломеец[1,2], И. В. Котенко[1], А. А. Чечулин[1]
[1]Санкт-Петербургский институт информатики и автоматизации Российской Академии Наук
[2]Национальный исследовательский университет ИТМО

Системы противодействия нежелательной, сомнительной и вредоносной информации включают в себя экспертное принятие решений, для поддержки которого используется средства визуальной аналитики. В работе представлена архитектура и пример реализации программно-аппаратного стенда визуализации для решения задач противодействия информации. Интерфейс системы предназначен для подтверждения работы

классификатора веб-ресурсов. Интерфейс оператора включает в себя предпросмотр ресурса, статистика соответствия сайта определённой категории, средства навигации по базе данных, а также распределения количества ресурсов по категориям.

противодействие информации, информационная безопасность, пользовательские интерфейсы, визуализация данных, визуальная аналитика.

В рамках процесса выявления и противодействия нежелательной, сомнительной и вредоносной информации на определенном этапе необходимо вмешательство оператора для принятия того или иного решения [1]. Заключение о противоправности или вредоносности информации не может приниматься системой в виду большого абсолютного числа ложных срабатываний классификаторов даже при большой точности. Кроме того, существует этический аспект противодействия информации – конечное решение должно приниматься оператором-человеком.

Таким образом возникает необходимость снабдить оператора удобными инструментами, которые смогут облегчить визуальный анализ и тем самым повысить скорость и качество принимаемых решений [2].

В данной работе мы рассматриваем реализацию визуальных интерфейсов для поддержки и принятия решений в рамках следующих процессов выявления и противодействия информации [3]:

– визуальная оценка оператором ресурса, который был распознан системой классификации как нежелательный, сомнительный либо вредоносный;

– визуальная оценка статистических данных анализируемого ресурса или группы ресурсов;

– фильтрация и выбор ресурсов из базы данных проанализированных и классифицированных ресурсов;

– визуальная оценка результатов работы классификатора для определённой группы ресурсов.

Для поддержки данных процессов визуальной аналитики был разработан программно-аппаратный стенд визуализации.

Стенд разработан как клиент-серверное приложение с использованием фреймворков node.js [4] и d3.js [5]. Визуализация запускается на клиенте посредством браузера. Таким образом клиент может быть запущен как на ПК, так и на мобильный устройствах и планшетах.

Интерфейс изображен на рис. (см. ниже) включает в себя следующие модели.

Предпросмотр анализируемого ресурса. Необходим для конечной оценки ресурса. Для предпросмотра используется html-фрейм в который загружается ресурс.

Столбчатый график – оценка соответствия категории, анализируемого для ресурса. График отображает результат работы классификатора.

Столбцы подсвечены цветом категорий: красный – для потенциально нежелательной информации, синий – для потенциально безвредной информации.

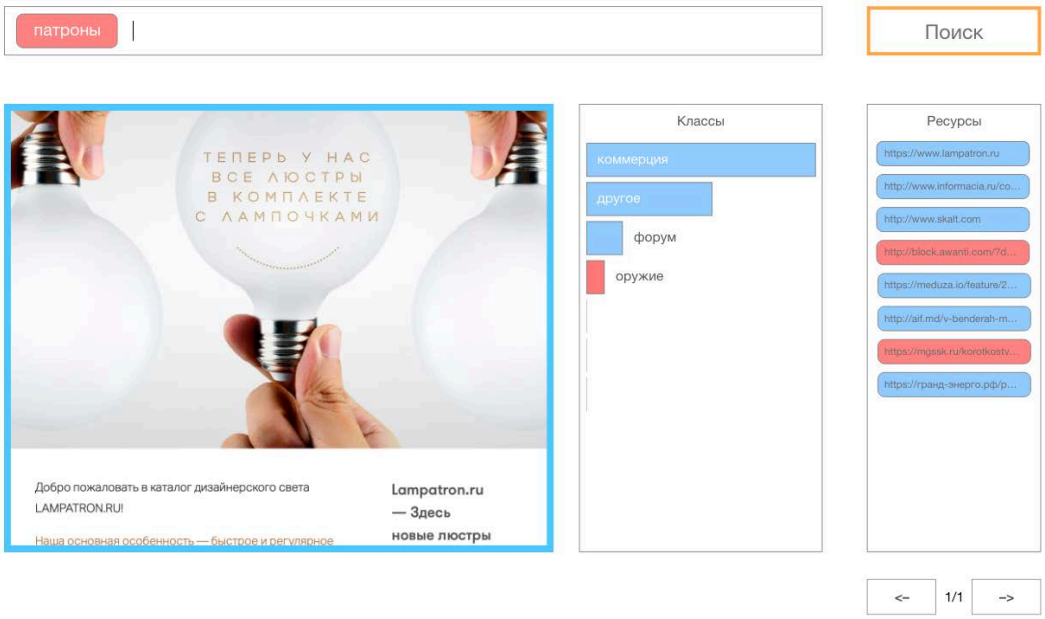


Рис. Интерфейс оператора

Строка поиска по ключевому слову. При вводе ключевого слова осуществляется поиск и писок ресурсов обновляется. Поиск производится по текстовому содержимому. Возможны варианты поиска по частям слова: необходимы как минимум первые три буквы и символ * на конце, для указания, что выполняется поиск по части слова.

Список ресурсов из базы данных с цветовой меткой. Список обновляется при нажатии на кнопку *Поиск*. Элементы списка подсвечиваются цветом категорий по наиболее вероятному классу: красный – для потенциально нежелательной информации, синий – для потенциально безвредной информации. При нажатии на элемент списка открывается пересмотр ресурса и обновляется столбчатый график.

Таким образом интерфейс позволяет осуществлять поиск ресурсов, по ключевым словам, с предварительным просмотром результатов классификации. А также визуальный анализ содержимого с более подробным анализом распределения оценок классификатора по категориям.

Данный интерфейс используется на последнем этапе выявления нежелательной, сомнительной и вредоносной информации, а также для принятия решений по выбору цели при выработке контрмер.

Выводы

Данная работа содержит описание разработки интерфейса системы выявления и противодействия нежелательной, сомнительной и вредоносной информации.

Интерфейс позволяет оператору решать следующий ряд задач визуальной аналитики: визуальная оценка оператором ресурса, визуальная оценка статистических данных анализируемого ресурса; фильтрация и выбор ресурсов из базы данных; визуальная оценка результатов работы классификатора. Интерфейс используется на этапе выявления нежелательной, сомнительной и вредоносной информации, а также для принятия решений по выбору цели при выработке контрмер.

Работа выполнена при частичной финансовой поддержке РНФ (проект 18-11-00302).

Список используемых источников

1. Jacobs J., Rudis B. Data Driven Security. John Wiley & Sons, Inc., 2014.

2. Коломеец М. В., Чечулин А. А., Дойникова Е. В., Котенко И. В. Методика визуализации метрик кибербезопасности // Изв. вузов. Приборостроение. 2018. Т. 61, № 10. С. 873–880.

3. Тушканова О. Н., Саенко И. Б. Методика обеспечения своевременности многоклассовой классификации нежелательной информации в сети интернет с привлечением параллельных вычислений // XI Санкт-Петербургская межрегиональная конференция «Информационная безопасность регионов России» (ИБРР-2019). 2019. С. 153–155.

4. Cantelon M. et al. Node. js in Action. – Greenwich : Manning, 2014. – 396 p.

5. Teller S. Data Visualization with D3. js. – Packt Publishing Ltd, 2013.

УДК 004.056
ГРНТИ 81.93.29

МЕТОДЫ ОБНАРУЖЕНИЯ КОМПЬЮТЕРНЫХ АТАК В СЕТЯХ С ВЫСОКОЙ НАГРУЗКОЙ

Н. А. Комашинский, И. В. Котенко

Санкт-Петербургский институт информатики и автоматизации Российской академии наук

Рассматриваются проблема построения современных систем обнаружения атак в сетях с большим объемом трафика. Описываются основные методы обнаружения атак и аномалий в сетях с большим объемом циркулирующего трафика. Анализируются используемые методы и состав систем обнаружения вторжений в соответствии с выделенными основными группами. Предлагается подход к обработке событий безопасности для выявления компьютерных атак в сетях с высокой нагрузкой с помощью использования технологии больших данных. Он основывается на использовании системы Spark Structured Streaming, балансировщиков нагрузки и компонентов обнаружения Snort.

компьютерные сети, информационная система, вредоносное программное обеспечение, Snort, большие данные.

Введение

Быстрое становление вычислительной техники привело к тому, что компьютерные сети стали применяться как полнофункциональный распределённый вычислительный инструмент для обработки и передачи данных. В настоящее время ведется огромное число исследований, имеющих целью выявление различных характеристик технологий и систем передачи данных, а также проработка методик обнаружения вторжений в работе компьютерных сетей. На фоне быстрого становления и трансформации вредоносного программного обеспечения и увеличения киберпреступности, существующее программное обеспечение (ПО) для обнаружения атак в сетях с большим объемом трафика не является эффективным. Поэтому ведутся исследования различных подходов по повышению эффективности обнаружения атак. Все чаще в одном ряду с сигнатурными способами, анализирующими шаблон определенного воздействия в сети по записям журналов логов, для анализа трафика во время работы сети используются более развитые методы сигнатурного анализа и различные методы машинного обучения.

Обзор существующих работ

Анализ существующих работ в области защиты информации и, в частности, обнаружения атак показывает, что проблема обнаружения атак (вторжений) в компьютерных сетях является достаточно актуальной. Многие научные статьи, в том числе статьи [1, 2, 3, 4, 5], описывают различные подходы в области разработки методов обнаружения инцидентов в сети, которые выявляют наличие уже совершающейся атаки или указывают на некорректную работу оборудования.

В общем случае методы обнаружения вторжений [4] можно классифицировать с помощью схемы, представленной на рис. 1 (см. ниже).

Отдельное внимание стоит уделить тому, что зачастую за короткий промежуток времени могут встречаться атаки различных типов, относящиеся к различным цепочкам действий разных злоумышленником, как связанных единой целью, так и независимых. Кроме того, эти действия происходят на фоне огромного потока событий. Поэтому очень важно уметь своевременно реагировать на конкретный вид и успевать обрабатывать большие потоки трафика. Для решения данной проблемы с целью обработки сетевого трафика большого объема, поступающего с высокой скоростью, предлагается использовать технологии больших данных.

Рис. 1. Общее представление методов обнаружения вторжений

В настоящее время предложено достаточно большое число подходов к обнаружению вторжений в таких условиях [6, 7, 8, 9, 10, 11, 12]. Например, в [11] представлена система обнаружения вторжений в реальном времени на основе Apache Storm. В этой работе применяются машины опорных векторов (SVM) для потоковой передачи данных. В качестве набора данных для тестов используется набор данных KDD Cup 1999 Data. Система может обрабатывать до 13 600 пакетов в секунду на одном компьютере с точностью 92,6 %. В этой работе представлены метрики производительности только для одной машины, и использование этого подхода не было протестировано на многоузловом кластере. Отсутствие использования распределенной среды – недостаток данной работы.

В [12] применена технология Apache Spark Streaming для обнаружения атак нулевого дня. Предложенная система основана на использовании алгоритма *k*-ближайших соседей, который показал точность 99,57 %. Кроме того, система была протестирована в распределенной среде для проверки ее масштабируемости. Хотя эта работа показывает, что входящие данные классифицируются практически в реальном времени, в ней использовался только сравнительно небольшой набор тестовых данных для оценки своей системы, что не совсем соответствует реальному сценарию.

Предлагаемый подход

На основе анализа существующих подходов к обнаружению вторжений, для решения проблем с потоковыми системами на основе применения простого в использовании и высокопроизводительного механизма обработки потоков в реальном времени, предлагается использовать механизмы Spark Structured Streaming, построенные на основе Spark и набора компонентов (систем) обнаружения Snort (рис. 2) в качестве сенсоров.

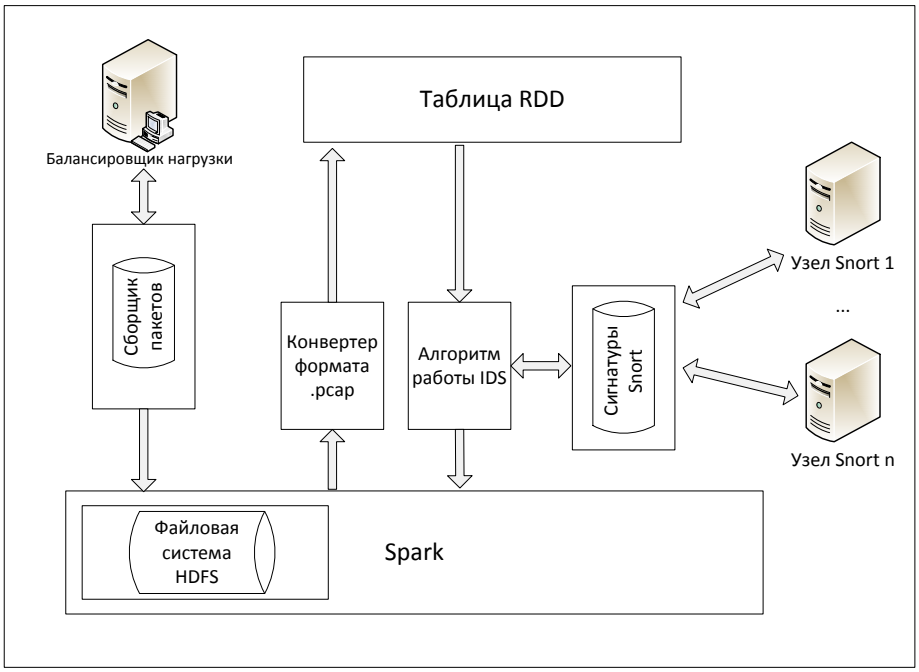


Рис. 2. Общее представление предлагаемого подхода

На рис. 2 использованы следующие обозначения компонентов: RDD – Resilient Distributed Dataset (эластичный распределенный набор данных), IDS – (интегрированная) система обнаружения вторжений, HDFS – Hadoop Distributed File System (распределенная файловая система Hadoop).

С целью оптимизации использования ресурсов, сокращения времени обслуживания запросов, горизонтального масштабирования кластера динамического добавления или удаления устройств, а также обеспечения отказоустойчивости используется балансировщик нагрузки.

Сборщик пакетов захватывает входящий пакет с фиксированным временным окном каждые 1000 пакетов и генерирует файл трассировки пакетов. Затем извлекается информация из шести полей IP-заголовка, которая содержит IP-адрес источника, IP-адрес назначения, интервал времени и длину файла трассировки пакетов, который будет храниться в RDD. Spark Resilient Distributed Dataset (RDD) используется для хранения больших данных. Эластичные распределенные наборы данных (RDD) – это фундаментальная структура данных Spark, неизменяемая распределенная коллекция объектов. Каждый набор данных в RDD разделен на логические разделы, которые могут быть вычислены на разных узлах кластера. RDD могут содержать любой тип объектов Python, Java или Scala, включая определяемые пользователем классы.

Распространенный формат Spark – это текстовый файл. Но файл трассировки пакетов (.pcap) – это двоичный формат. Поэтому необходимо преобразовать пакет в файл трассировки в текстовый файл и разбить каждую строку на процессор данных, для этого используется конвертер.

Фаза обработки данных использует алгоритм работы IDS для распределенного набора данных (RDD) для вычисления некоторых необходимых свойств пакетов. Должны быть выполнены процедуры группировки пакетов и вычисления объектов, которые имеют одинаковые IP-адрес источника и IP-адрес назначения.

Распределенные узлы Snort 1 … Snort *n*, выполняют задачу выявления подозрительных событий, обрабатывая объекты из файловой системы HDFS. Также база данных сигнатур для IDS Snort всегда доступна для ее пополнения и обновления актуальными данными.

Заключение

В данной статье проведен сравнительный анализ основных методов обнаружения и классификации сетевых атак. Рассмотренные подходы в настоящее время наиболее часто используются научным сообществом при разработке систем обнаружения атак.

Представлена классификационная схема рассмотренных подходов. Предложена общая модель для обработки событий в потоковых системах. Внедряя представленную систему обнаружения вторжений с использованием масштабируемого кластера, балансировщиков нагрузки трафика, фреймворка Spark, можно получить интегрированную систему обнаружения вторжений, позволяющую обрабатывать большие потоки трафика. Для реализации данной системы использованы языки Python / Java. В дальнейших исследованиях планируется представить экспериментальные результаты и провести сравнение системы обнаружения вторжений, основанной на Spark и Hadoop.

Исследование проводится при поддержке Минобрнауки России в рамках Соглашения № 05.607.21.0322 (идентификатор RFMEFI60719X0322).

Список используемых источников

1. Komashinskiy D., Kotenko I. Malware Detection by Data Mining Techniques Based on Positionally Dependent Features // Proceedings of the 18th Euromicro International Conference on Parallel, Distributed and network-based Processing (PDP 2010). Pisa, Italy, 17–19 February, 2010. Los Alamitos, California. IEEE Computer Society. 2010. PP. 617–623.

2. Котенко И.В., Степашкин М.В. Анализ защищенности компьютерных сетей на основе моделирования действий злоумышленников и построения графа атак // Труды Института системного анализа Российской академии наук. 2007. Т. 31. С. 126–207.

3. Kotenko I., Konovalov A., Shorov A. Agent-based simulation of cooperative defence against botnets // Concurrency and Computation: Practice and Experience, Vol. 24, Issue 6, 2012. PP. 573–588.

4. Браницкий А. А., Котенко И. В. Анализ и классификация методов обнаружения сетевых атак // Труды СПИИРАН. 2016. № 2 (45). С. 207–244.

5. Козленко А. В., Авраменко В. С., Саенко И. Б., Кий А. В. Метод оценки уровня защиты информации от НСД в компьютерных сетях на основе графа защищенности // Труды СПИИРАН. 2012. № 2 (21). С. 41–55.

6. Cardenas A. A., Manadhata P. K., Rajan S. P. Big data analytics for security // IEEE Security & Privacy, 2013, 11 (6). PP. 74–76.

7. Zhao S., Leftwich K., Owens M., Magrone F., Schonemann J., Anderson B., Medhi D. I-can-mama: Integrated campus network monitoring and management // Network Operations and Management Symposium (NOMS), 2014. PP. 10–14.

8. Bajpai A., Dayanand, Arya A. Big Data Analytics in Cyber Security // International Journal of Computer Sciences and Engineering, Vol.6, no.7, 2018. PP. 1–5.

9. Kotenko I., Kuleshov A., Ushakov I. Aggregation of Elastic Stack Instruments for Collecting, Storing and Processing of Security Information and Events // The 14th IEEE Conference on Advanced and Trusted Computing (ATC 2017). San Francisco, August 4–8, 2017, USA. Los Alamitos, California. IEEE Computer Society. 2017. PP. 1550–1557.

10. Kotenko I., Saenko I., Branitskiy A. Framework for Mobile Internet of Things Security Monitoring based on Big Data Processing and Machine Learning // IEEE Access, 2018, Vol. 6. PP. 72714–72723.

11. Manzoor, M. A., Morgan Y. Real-time Support Vector Machine based Network Intrusion Detection system using Apache Storm // In Proceedings of the IEEE 7th Annual Information Technology, Electronics and Mobile Communication Conference (IEMCON), Vancouver, BC, Canada, 13–15 October 2016.

12. Pallaprolu, S. C., Sankineni R., Thevar M., Karabatis, G., Wang, J. Zero-Day Attack Identification in Streaming Data Using Semantics and Spark // In Proceedings of the IEEE International Congress on Big Data (BigData Congress), Honolulu, HI, USA, 25–30 June 2017.

УДК 004.94
ГРНТИ 47.63

ИССЛЕДОВАНИЕ ПОЛИТИКИ ВНЕДРЕНИЯ LCD KEYPAD SHIELD ДЛЯ МИКРОКОНТРОЛЬНОЙ СИСТЕМЫ ARDUINO

В. В. Коновалова, С. И. Штеренберг

Санкт-Петербургский государственный университет телекоммуникаций им. проф. М.А. Бонч-Бруевича

Данная статья сфокусирована на изучении назначения неизвестного устройства, способах его применения, нахождения его плюсов и минусов, а также приведение собственного примера его использования. Главная особенность, это изучение устройства на уровне обычного пользователя.

Arduino, LCD Keypad Shield, микроконтроллер, LiquidCrystal, LCD 1602.

Введение

XXI век не зря называют веком информационных технологий, на рынке все чаще появляются различные изобретения и еще чаще желающие скопировать эти технологии и присвоить себе. Конечно, в этом можно найти как плюсы, так и минусы, например, очень удобно в короткие сроки приобрести необходимый элемент через стороннюю организацию, если эта реплика полностью повторяет функции и строение оригинала, или найти то, что нам нужно по сниженной цене. Но из-за того же огромного количества производителей качество некоторых товаров оставляет желать лучшего. Конкретно потому было бы хорошо уметь различать доброкачественную реплику от плохой и осознавать, верно ли она устроена и точно ли она делает нужные нам функции.

Перед началом стоит ознакомиться с некоторыми понятиями, которые часто будут встречаться в тексте:

Шилд – это подвид плат расширения, а именно плат, устанавливаемых для дополнительных способностей, которые состыкуется с Arduino.

Пин – контакт (ножка) в автоматике для соединения двух элементов схемы.

Изучение устройства

Многим ли из нас встречались в руках приспособления, в производстве которых мы сомневались, а что еще хуже, вообще не воображали, как они устроены и что с ними делать? На примере попавшегося шилда докажем, что любой, даже некомпетентный в вопросе электроники, пользователь способен определить его назначение и качество сборки [3].

На первый взгляд устройство, попавшее в наши в руки, имеет 6 кнопок, 5 из них – кнопки управления и последняя – Reset. Ещё более детально изучив шилд, заметим, что кнопки управления выходят на A0 аналоговый пин [4]. В глаза так же бросается LCD-экран, что является главной составляющей его частью, и резистор. Исследовав оборотную сторону, приметно внедрение в работе пинов D4, D5, D6 D7, VDD, V0, RS. Также самая основная изюминка, которая посодействовала в исследовании устройства и стала главной точкой отсчета проделанной работы – заглавие, которое было написано на устройстве и веб-сайт производителя.

Еще одной тайной в исследовании шилда стал поиск по фото в поисковых системах, при помощи чего я смогла найти детализированное описание схожих продуктов и выяснить их номер (рис. 1–2).

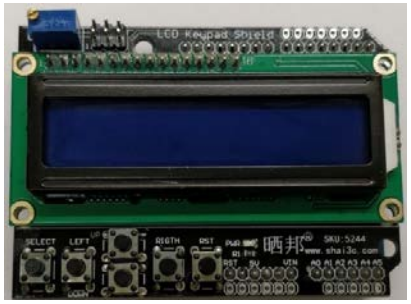


Рис. 1. Изучаемый шилд

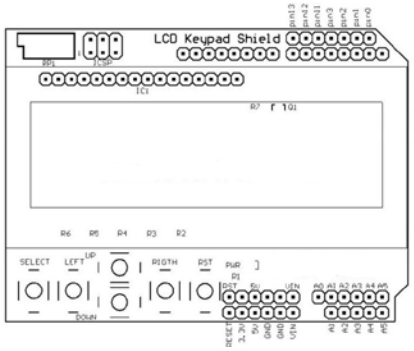


Рис. 2. Схема шилда

Описание шилда LCD Keypad Shield

Изучаемый шилд представляет собой плату со встроенными модулями индикации и управления. Индикация производится при помощи LCD-монитора, а управление – через интегрированные клавиши. Есть возможность регулировки яркости монитора прямо на плате при помощи подстроечного резистора. Подстроечный резистор – переменный резистор, пассивный электронный элемент, созданный для четкой опции данных характеристик радио- и электронных устройств в процессе их выпуска из производства при настройке после монтажа. Плата снабжена разъемами, в которые могут быть подключены остальные устройства, к примеру, датчики. Для работы с экраном употребляются пины 4–10, для определения нажатия клавиш – лишь один аналоговый пин A0 (табл. 1).

ТАБЛИЦА 1. Использование пинов D4-D10 и аналогового A0

Пин	Использование
D4	Старшие двунаправленные контакты шины данных. Употребляются для передачи и приема данных MPU и LCD
D5	
D6	
D7	
D8	Скрыть данные либо отображение сигнала
D9	Чтение и запись данных
D10	Управление подсветкой LCD
A0	Кнопки управления: выбор, вверх, вправо, вниз и влево

Основные области применения шилда: создание управляющих модулей, которые реализуют опции устройства при помощи интерфейса меню (табл. 2). Экран шилда можно использовать для вывода информации, получаемой с датчиков, с возможностью выполнения пользователем каких-либо действий путем нажатия на интегрированные клавиши. Конечно же,

можно найти и иные методы использования платы: к примеру, воплотить игру типа тетрис [4].

ТАБЛИЦА 2. Описание используемых контактов

Контакт дисплея LCD 1602	Описание	Контакт на LCD Shield
Пины LCD экрана		
GND	Земля	
VDD	Питание 5В	
Contrast	Управление контрастом	Потенциометр
RS	Команды/Данные	8
R/W	Чтение/Запись	
Enable	Включение (активирование)	9
DB0	Не используется	
DB1	Не используется	
DB2	Не используется	
DB3	Не используется	
DB4	Дата 1	4
DB5	Дата 2	5
DB6	Дата 3	6
DB7	Дата 4	7
Back LED +	Включение подсветки	10
Back LED –	Питание подсветки	
Пины для кнопок		
Кнопка UP	Управляющая кнопка	A0
Кнопка DOWN	Управляющая кнопка	A0
Кнопка LEFT	Управляющая кнопка	A0
Кнопка RIGHT	Управляющая кнопка	A0
Кнопка SELECT	Управляющая кнопка	A0
Reset	Перезагрузка платы	Reset
ICSP	ICSP для перепрошивки встроенного микроконтроллера HD44780U	
UART	Контакты для UART соединения	0, 1

Технические характеристики:

– тип дисплея: LCD 1602, символьный, 4-х битный режим;
– разрешение: 16×2 (две строки по 16 символов каждая);
– знакоместо 5×8 точек;
– цвет дисплея: синий Буквы белого цвета;
– контроллер дисплея: HD44780U;
– предельная частота обновления экрана: 5 Гц;
– питание дисплея: 5 Вольт;
– дополнительные элементы: регулировка яркости подсветки.

Распиновка LCD shield для подключения к Arduino (рис. 3).

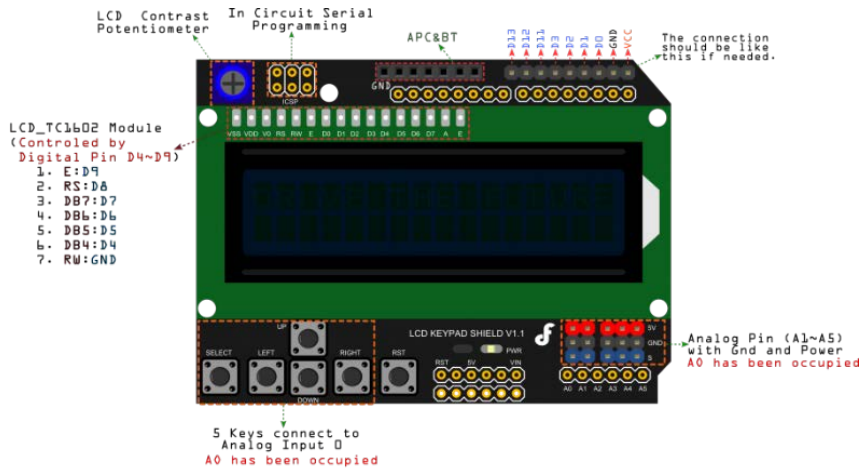


Рис. 3. Расположение пинов

Дополнительные элементы шилда:

– индикаторный светодиод (включается при подключении питания к плате);

– контактные площадки для подключения аналоговых устройств (GND, VSS, пин данных);

– потенциометр для регулирования контрастностью экрана.

Подключение платы LCD Shield к Arduino: подключение шилда чрезвычайно обычное – необходимо попасть ножками в надлежащие разъемы платы ардуино и аккуратненько скооперировать их. Подключив шилд, можно работать с экраном и клавишами на нем так же, как с некоторыми устройствами, беря во внимание лишь номера пинов, к которым припаяны надлежащие контакты. Скетч для экрана на Arduino LCD shield.

Для работы с LCD экранами обычно употребляют пользующуюся популярностью библиотеку LiquidCrystal. На шаге инициализации создается объект класса LiquidCrystal, в конструкторе которого мы указываем пины с присоединенными контактами экрана. Для нашего шилда требуется использовать такой вариант: LiquidCrystal lcd (8, 9, 4, 5, 6, 7).

Кнопки LCD Keypad Shield: на плате находятся 5 управляющих клавиш, работа с которыми ведется через один аналоговый пин A0. В шилде применен довольно распространенный метод обычного кодировки сигнала, при котором любая клавиша сформировывает определенное значение напряжения, которое после АЦП преобразуется в соответственное значение от 0 до 1023. В итоге, мы можем передавать данные о нажатии различных клавиш через один пин, считывая его с помощью функции analogRead().

Краткие выводы по плате расширения LCD keypad shield

Плата расширения LCD Keypad достаточно популярная, она проста и удобна для использования в проектах Arduino [5, 6, 7].

Плюсы LCD Shield: облегчает подключение жидкокристаллического экрана; уменьшает общие размеры устройства, т.к. убирает выступающие провода и монтажные платы; уменьшает число просчетов, которые связаны с неверным монтажом и подключением; добавляет функциональность кнопочного управления, если на плате установлены клавиши (LCD Keypad shield).

Недостатки: цена шилда выше, чем цена некоторого экрана; не постоянно необходима дополнительная функциональность в виде клавиш; шилд потребляет больше энергии, чем некоторые элементы платы.

Список используемых источников

1. Что такое Arduino: 2010–2019. [Электронный ресурс] // ООО «Амперка». URL: https://amperka.ru/page/what-is-arduino (дата обращения: 25.11.2019)/

2. Красов А. В. Программирование на языке Си. Часть 1. Основные конструкции языка. – СПб.: Лицей при СПбГУТ, 2000. – 44 с.

3. Аль-Ани Н. М., Бусов С. В., Кузнецова В. В., Милославов А. С., Панкратьев О. В., Пешков А. И. Информационно-компьютерные технологии в социально-гуманитарном образовании. философско-социологический анализ : коллективная монография. – М. : Спецкнига, 2012. – 192 с.

4. Котенко И. В., Левшун Д. С., Чечулин А. А., Ушаков И. А., Красов А. В. Комплексный подход к обеспечению безопасности киберфизических систем на основе микроконтроллеров // Вопросы кибербезопасности. 2018. № 3 (27). С. 29–38.

5. Новолодская Т. А., Пешков А. И. Аналитика образовательных парадигм в контексте запросов информационной цивилизации // Вестник Ленинградского государственного университета им. А. С. Пушкина. 2010. Т. 2. № 2. С. 166–175.

6. Красов А. В., Ушаков И. А. Подготовка специалистов в области информационной безопасности в санкт-петербургском государственном университете телекоммуникаций им. проф. М. А. Бонч-Бруевича // Инновации. 2013. № 7 (177). С. 92–97.

7. Зыков А. Г., Кочетков И. В., Чистиков Е. Г., Швед В. Г. Автоматизация генерации описания графоаналитической модели программы // Защита информации. Инсайд. 2017. № 4 (76). С. 60–65

УДК 004.942
ГРНТИ 28.17.19

МОДЕЛИРОВАНИЕ ПРОЦЕССОВ ОБРАБОТКИ ЗАПРОСОВ В РАСПРЕДЕЛЕННЫХ СИСТЕМАХ ХРАНЕНИЯ БОЛЬШИХ ДАННЫХ

И. В. Котенко, А. П. Проничев

Санкт-Петербургский институт информатики и автоматизации Российской академии наук

В системах хранения больших данных информация распределяется по нескольким узлам для обеспечения производительности, масштабируемости, доступности и целостности. Разработка масштабируемой распределенной системы хранения является сложной и ресурсоемкой задачей. Поэтому при проектировании подобных систем используется моделирование для предварительной оценки общей производительности и выявления недостатков. В работе представлены особенности моделирования процесса обработки клиентских запросов в системе хранения и основные факторы, влияющие на скорость обработки запросов между узлами системы и между системой и клиентом. Предложен подход к моделированию процесса обработки запросов. Данный подход позволяет измерить параметры оперативности обработки как клиентских запросов, так и взаимодействия между модулями распределенной системы хранения. Данный подход предполагается использовать для обработки больших объемов трафика для решения задач обнаружения вторжений.

большие данные, распределенные системы, моделирование процессов.

По мере внедрения информационных технологий в различные сферы деятельности, возрастают требования к хранению информации, формируется постановка новых задач по обработке большого количества данных, возникает проблема, когда такие объемы невозможно обрабатывать традиционными способами.

Обсуждение проблемы больших данных началось в 2000-х годах [1]. Проблему больших данных обычно связывают с анализом неструктурированных данных больших объемов. Для характеристики больших данных используются критерии «три V» [2]:

– объем (*Volume*) – большой объем, являющийся проблемой для средств обработки;

– скорость (*Velocity*) – высокая скорость обработки, недоступная для средств обработки;

– разнообразие (*Variety*) – многообразие данных, представляющие сложность для методов анализа на имеющихся средствах обработки.

Важным элементом систем обработки Больших данных являются подсистемы хранения, так как от них напрямую зависят характеристики обработки, логическая структура хранения данных. Примером могут являться поисковые системы, обрабатывающие большие потоки данных для нахождения необходимой информации. Свойства Больших данных обуславливают требования к системам их обработки и хранения. Так, для хранения Больших данных используются сложные распределенные файловые системы, такие как HDFS [3], GFS [4], Amazon S3 [5].

Схема работы таких систем рассмотрена на рис.

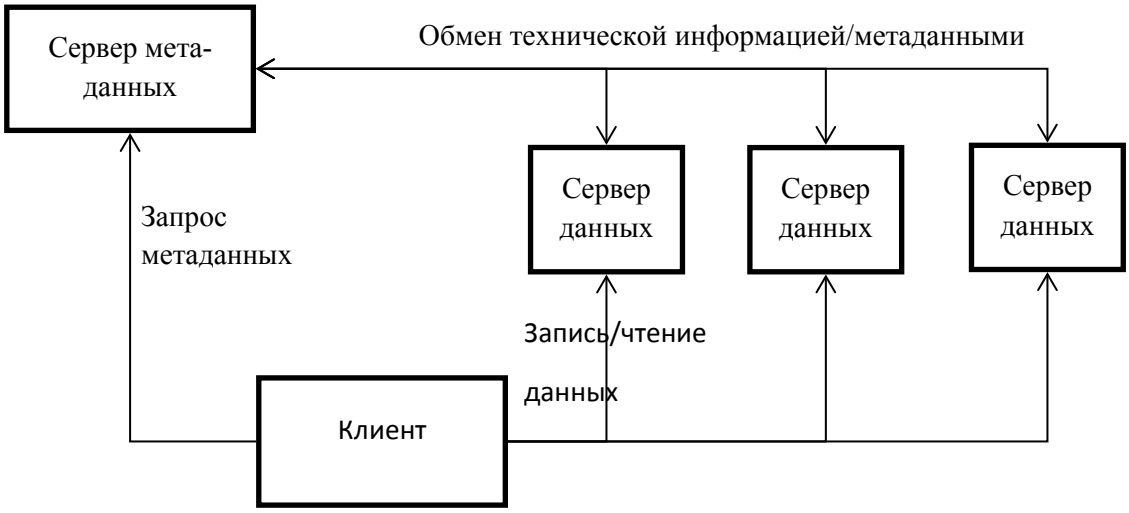


Рис. Взаимодействие узлов в распределенной файловой системе

Кроме распределенных файловых систем можно выделить следующие типы таких хранилищ [6]:

– хранилища ключ – значение (*DynamoDB, Berkeley DB, Redis*);
– документные хранилища (*MongoDB, Couchbase*);
– колоночные хранилища (*BigTable, Hbase, Cassandra*);
– графовые хранилища (*Neo4j, OrientDB*).

При проектировании распределенных систем обработки больших данных правильный выбор типа подсистемы хранения очень важен, так как от этой подсистемы в дальнейшем будут в значительной степени зависеть и характеристики самой системы обработки [7]. Ошибки на этапе проектирования могут привести к тому, что система вообще не сможет выполнять свои задачи или будет обрабатывать данные в сроки не соответствующим требованиям для данной системы [8].

Таким образом, актуальной задачей является оценка систем обработки в целом, и подсистем хранения в частности с точки зрения необходимых ресурсов и времени выполнения запросов на этапе проектирования и разработки (т. е. до этапа эксплуатации).

Существуют различные подходы к оценке систем на этапе проектирования. Одним из перспективных направлений, является применение подходов, основанных на моделировании. Рассмотрим **основные подходы к моделированию**, которые могут применять для решения задачи оценки подсистем хранения.

Аналитическое моделирование. Характерной чертой при использовании аналитического моделирования является запись процессов функционирования подсистем в виде функциональных соотношений или логических условий.

Имитационное моделирование. Заключается в разработке моделей отдельных элементов системы и воспроизведению процесса функционирования системы с имитацией основных событий.

Полунатурное моделирование. Представляет собой построение модели на оборудовании меньших мощностей и с имитацией отдельных функций для анализа процессов, происходящих между узлами распределенной файловой системы.

Натурное моделирование. Отображение системы, используя аналогичные программно-аппаратные средства.

Эти подходы отличаются по ресурсам, требуемым для их реализации и характеристиками системы, которые они позволяют оценить.

Рассмотрим **особенности применения вышеизложенных подходов** к моделированию в части их применения для задачи оценки подсистем хранения Больших данных.

Аналитическое моделирование позволяет рассмотреть систему в целом и проанализировать ее отдельные сегменты Основная сложность при использовании данного подхода, что без знания явных зависимостей между начальными условиями, параметрами и переменными не получится создать математическую модель, что затрудняет ее использование при рассмотрении логических связей в системе функционирования.

Имитационное моделирование подходит для рассмотрения взаимодействия в сегменте системы. При таком подходе сохраняется логическая структура и последовательность этих явлений, что позволяет, имея исходные параметры, получить данные о состоянии системы в различные моменты времени. В меньшей степени подходит для рассмотрения всей системы.

Полунатурное моделирование будет полезно для рассмотрения отдельного узла распределенной системы, оценить распределение нагрузки на нем.

Натурное моделирование может использоваться для моделирование всей системы, но ввиду затрат большого количества ресурсов может быть применено лишь для выделения отдельных процессов и локальных особенностей в узле распределенной системы хранения.

Обобщая анализ подходов, можно отметить, что каждый из них обладает своими преимуществами и недостатками и по отдельности не может провести оценку всей системы в условиях ограниченности ресурсов. Кроме того, каждый уровень системы может быть рассмотрен с использование определенного подхода (табл.).

ТАБЛИЦА. Соответствие исследуемых параметров и типа моделирования

Уровень / подход	Аналит.	Имитац.	Полунарн.	Натурное
Система хранения в целом	+	+	+	+
Сегмент системы хранения	+	+	+	+
Отдельный элемент системы хранения (узел)	–	–	+	+
Программные компоненты на узле	–	–	–	+

В таблице рассмотрены возможности моделирования элементов системы на основе разных подходов. Цветом обозначено потребление ресурсов на использование этих подходов. Темно-серым выделен высокий уровень потребления ресурсов, светло-серым средний, белым – низкий.

В настоящем исследовании предлагается использовать комплексный подход к моделированию, который позволит объединить все проанализированные подходы в единое комплексное решение, позволяющие динамически выбирать необходимые подходы к моделированию и за счет их взаимодействия объединять их достоинства и нивелировать недостатки.

Выводы

В работе рассмотрены различные подходы к оценке систем хранения больших данных, проведен их анализ, выявлены достоинства и недостатки и предложен комплексный подход к моделированию системы.

В будущих работах планируется более глубокое рассмотрение данного подхода, разработка программного прототипа, реализующего данный подход и проведение экспериментов.

Работа выполнена при частичной финансовой поддержке бюджетной темы 0060-2019-0010.

Список используемых источников

1. Jacobs A. The pathologies of big data // Communications of the ACM, 2009, Vol. 52, No 8. PP. 36–44.

2. Laney D. 3D data management: Controlling data volume, velocity and variety // META group research note, 2001, Vol. 6, No 70. PP. 1–3.

3. Shvachko K., Kuang H., Radia S., Chansler R. The Hadoop Distributed File System // MSST '10 Proceedings of the 2010 IEEE 26th Symposium on Mass Storage Systems and Technologies (MSST), 2010. PP. 1–10.

4. Ghemawat S., Gobioff H., Leung S. T. The Google file system // Proceedings of the nineteenth ACM symposium on Operating systems principles, 2003. PP. 29–43.

5. Palankar M. R., Iamnitchi A., Ripeanu M., Garfinkel S. Amazon S3 for science grids: a viable solution? // Proceedings of the 2008 international workshop on Data-aware distributed computing, 2008. PP. 55–64.

6. Cattel R. Scalable SQL and NoSQL data stores // ACM SIGMOD Record, 2010, 39 (4). PP. 12–27.

7. Десницкий В. А., Чечулин А. А., Котенко И. В., Левшун Д. С., Коломеец М. В. Комбинированная методика проектирования защищенных встроенных устройств на примере системы охраны периметра // Труды СПИИРАН. 2016. Вып. 5 (48). С. 5–31.

8. Котенко И. В., Десницкий В. А., Чечулин А. А. Исследование технологии проектирования безопасных встроенных систем в проекте Европейского сообщества SecFutur // Защита информации. Инсайд. 2011. № 3 (39). С. 68–75.

УДК 519.876.2
ГРНТИ 81.93.29

МОДЕЛЬ И АРХИТЕКТУРА СИСТЕМЫ UEBA ДЛЯ ОБЛАЧНОГО СЕРВИС-ПРОВАЙДЕРА

И. В. Котенко[1], Б. А. Тынымбаев[2]

[1]Санкт-Петербургский институт информатики и автоматизации Российской академии наук
[2]Евразийский национальный университет Республики Казахстан

В работе описывается модель и архитектура разрабатываемой системы UEBA, предназначенной для защиты информационных ресурсов облачного сервис-провайдера. Рассмотрена схема взаимодействия системы с источниками событий информационной безопасности. Представлен пример использования системы для решения задач обеспечения безопасности пользователей провайдера облачных услуг.

аналитика кибербезопасности, поведение пользователей, информационная безопасность, UEBA.

Введение

В настоящее время становятся все более популярными услуги облачных сервис-провайдеров. Многие организации предпочитают пользоваться сторонними приложениями, не развивая парк технологий у себя. Сервисы, предоставляемые в облаках, могут быть различными – от услуг документооборота до предоставления финансовых услуг. Соответственно, уровень

обеспечения информационной безопасности могут быть различным по степени критичности, но при этом без ограничения общности можно считать наличие инструментов по обеспечению защищённости облаков обязательным.

Для предоставления качественных сервисов облачному провайдеру необходима постоянно развивающаяся система управления информационной безопасности, позволяющая гарантировать конфиденциальность, целостность и доступность [1, 2]. Если ранее, корпоративную сеть можно было обеспечить стандартными инструментами, такими как файервол, антивирусное программное обеспечение, системы класса SIEM, прокси-сервер, то сейчас наступает необходимость применения аналитических инструментов для обеспечения безопасности компаний, и тем более облачных сервисов. Одним из классов аналитических инструментов являются системы класса UEBA (user entity and behavioral analytics) [3].

Риски информационной безопасности для облачных сервис-провайдеров – схожи с рисками для корпоративных сетей, и отличаются отдельными видами угроз. В работе [4] представлены примеры сценариев обнаружения угроз для облачных сервис-провайдеров.

Пример использования системы UEBA

Пункт CLD.12.4.5 стандарта ISO/IEC 27017 [5] определяет возможности провайдера, которые позволяют клиенту проводить мониторинг активности в облачной среде. Таким образом, предоставляется возможность использования аналитических инструментов. В качестве тестового стенда в облачном сервис-провайдере Qazcloud использовалась система класса UEBA производителя IBM Qradar.

Согласно [6], основу системы UEBA составляют сценарии обнаружения угроз, наиболее критичные и значимые для любой организации. Для определения угроз были использованы, в первую очередь, стандартные сценарии: обнаружение компрометации учётных записей пользователей, обнаружение скомпрометированного конечного устройства, обнаружение утечки данных, использование несанкционированного внутреннего доступа, включая привилегированные доступы, предоставление дополнительной информации и контекста для исследования. Кроме того, должны использоваться специфичные сценарии угроз, свойственные конкретному облачному провайдеру.

При тестировании используемой системы возникла следующая задача. Для каждого пользователя в настройках составляется порог рейтинга, при превышении которого, фиксируется событие аномального поведения, несвойственное нормальному поведению. Модель, используемая в системе, схожа с работой [7].

Рейтинг пользователя составляется на основе включенных, настроенных правил детектирования аномального поведения пользователя, которых в системе насчитывается порядка 157. В таблице представлены правила с наибольшим количеством зафиксированных срабатываний.

ТАБЛИЦА. Правила детектирования аномального поведения

Правило детектирования	Описание и результаты
Подключение пользователя в нетипичное время суток	После обучающего периода было установлено, что стандартные часы подключения пользователей с 9:00 до 19:00
Соединение с зловредными веб-сайтами	Логи прокси-сервера, указывающие на попытки соединения с зловредными веб-сайтами
Повышение прав пользователя или группы пользователя	Предоставление записи файлов, вместо чтения

В тестовой среде для 100 пользователей в рамках обучающего периода был выставлен порог в 20 баллов. Соответственно, согласно настройкам, при превышении указанного порога, система оповещала об инцидентах кибербезопасности для каждого пользователя, на рис. представлены пороговые значения.

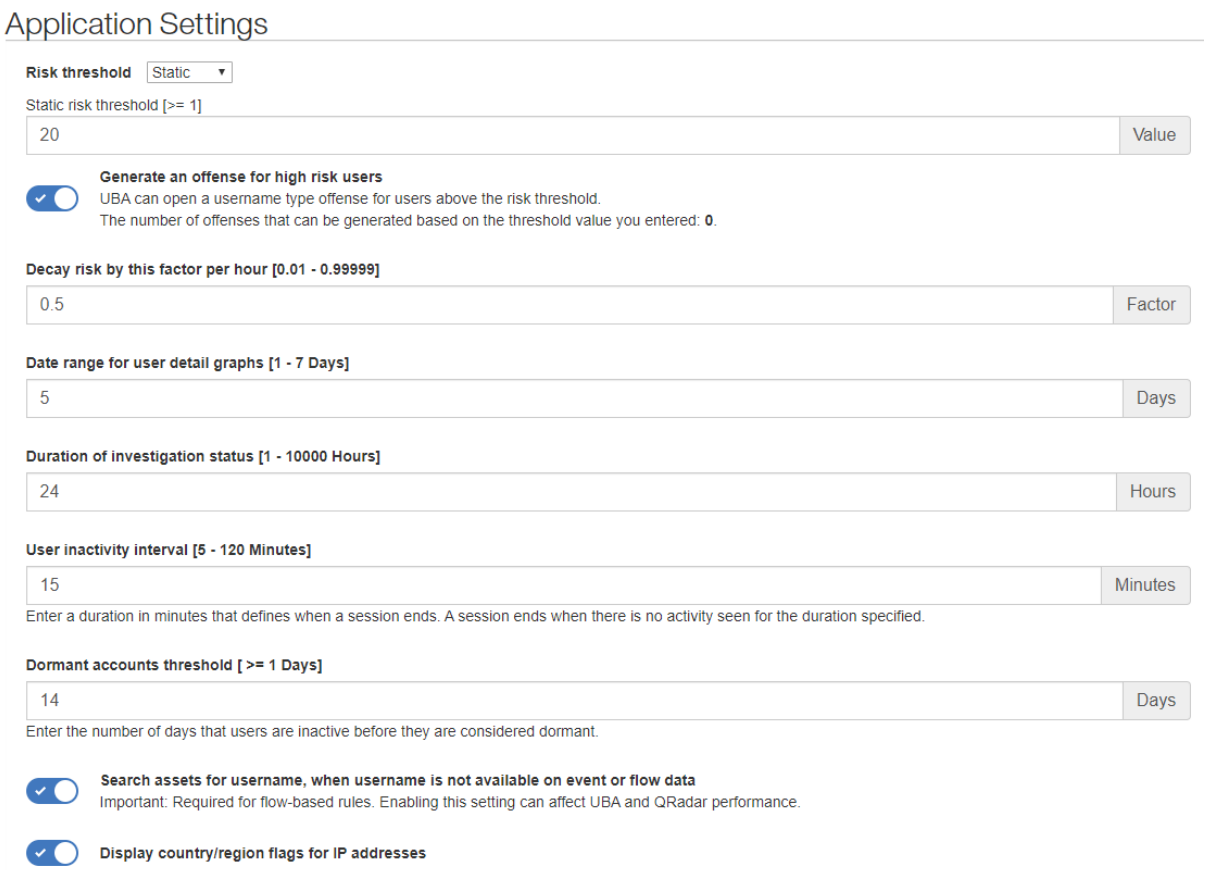


Рис. Настройки UBA IBM Qradar

При внедрении системы для крупного облачного сервис-провайдера рассматриваемая система оказалась неэффективна. Система UBA использовала для анализа и обработки порядка 23000 пользователей.

Для указанного порога рейтинга пользователя в 20 баллов за период с 29 июня по 25 сентября 2019 года было сгенерировано 37733448 срабатываний правил, и 3265 событий превышения указанного порога. Поэтому возникают сложности при обработке такого количества инцидентов, при этом для таких пользователей необходимо проводить обучающие курсы, повышать их осведомлённость. Логично разбиение пользователей на отдельные группы по типу поведения, однако разделение порядка 23000 облачных пользователей является трудоёмкой задачей.

Постановка задачи

Основной задачей для любой системы аналитики поведения пользователей, является создание математической модели, обеспечивающей решение комплекса необходимых задач, при этом генерируя как можно меньше ложных срабатываний. Предлагается использование модели для анализа поведения пользователей и подсчёта рейтинга пользователей. Требованием к данной модели является способность избежать генерации большого количества инцидентов, на которые физически невозможно среагировать. Более высокий порог для рейтинга приведёт к меньшему количеству истинных и ложных положительных результатов, а низкий порог может дать больше ложных срабатываний. Таким образом необходима система UEBA, которая позволяет реализовать гибкую настройку рейтингов пользователей. Имеющиеся модели машинного обучения в системе – это следующие модели: привязки пользователя к локальному IP-адресу; соединенных сетевых портов в локальной сети; обнаруженных процессов в операционной системе Windows или Linux; проведённого времени в браузере на нерабочих сайтах; событиях приложения; соединений с рискованными веб-приложениями.

Модель потенциальной системы класса UEBA

В результате анализа использования системы UBA Qradar и готовых шаблонов моделей для потенциальной системы класса UEBA предлагается использование аналога рейтинга ЭЛО [8] для оценки поведения пользователя облачного сервис-провайдера. Оценки рейтинга ЭЛО, который используется в шахматных соревнованиях, для анализа поведения пользователей формируются следующим образом: вычисляется математическое ожидание количества баллов рейтинга, которое получит пользователь за день N в сравнении с предыдущим днём $N-1$ согласно следующей формуле:

$$E_N = \frac{1}{1+10^{\frac{R_N - R_{No}}{400}}}$$

где E_N – математическое ожидание количества баллов, которое наберёт пользователь за день N в сравнении с рейтингом ожидаемого поведения пользователя (R_{N_0}) в данной группе, где R_N – рейтинг пользователя за день N.

Новый рейтинг пользователя считается по формуле:

$$R_N = R_{n-1} + K * (S_N - E_N),$$

где К – значение, которое равно 10 для опытных пользователей (рейтинг 2400 и выше), 20 – для пользователей с рейтингом меньше, чем 2400, и 40 – для новых пользователей (первые 30 дней с момента регистрации).

Как и во всех моделях, предполагающих случайную переменную, система оценки Эло уязвима к избирательным парам и непредставительным популяциям, что делает модель неточной. Указанные k-факторы не окончательные, и в рамках будущего тестирования модели могут измениться аналогично [9].

Также важным моментом для последующей настройки является определение отдельных весов, которые используются для подсчета рейтинга нарушителя. Имеет смысл и комбинирование указанных методов по аналогии с работой [10].

Архитектура потенциальной системы класса UEBA

Архитектура потенциальной системы класса UEBA представлена в [6]. Основные данные для систем подобного класса: собранные логи информационных активов, для которых проводится нормализация логов; сценарии определения угроз и фактов аномального поведения; выявленные инциденты аномального поведения.

Заключение

В работе представлена модель и архитектура разрабатываемой системы UEBA, предназначенной для защиты информационных ресурсов облачного сервис-провайдера. Предложена модель подсчета рейтинга поведения пользователей, которая может быть применима для большого количества пользователей облачного сервис-провайдера. Данная модель также позволяет разделять группы пользователей по группам. Разделение пользователей по группам позволяет быстрее реагировать на схожие типы инцидентов, а также проводить мероприятия по повышению осведомлённости пользователей.

Исследование проводится при поддержке Минобрнауки России в рамках Соглашения № 05.607.21.0322 (идентификатор RFMEFI60719X0322).

Список используемых источников

1. Саенко И. Б., Агеев С. А., Бушуев А. С., Егоров Ю. П. Концепция автоматизации управления информационной безопасностью в защищенных мультисервисных сетях специального назначения // Автоматизация процессов управления. 2011. № 1 (23). С. 50–57.

2. Котенко И. В., Десницкий В. А., Чечулин А. А. Исследование технологии проектирования безопасных встроенных систем в проекте Европейского сообщества SecFutur // Защита информации. Инсайд. 2011. № 3 (39). С..68–75.

3. Котенко И. В. Аналитика кибербезопасности: анализ современного состояния и перспективные направления исследований // Актуальные проблемы инфотелекоммуникаций в науке и образовании (АПИНО 2018). VII Международная научно-техническая и научно-методическая конференция : сб. науч. ст. в 4-х т. 2018. Т. 1. С. 10–19.

4. Тынымбаев Б. А., Котенко И. В. Обзор решений класса UEBA // Актуальные проблемы инфо-телекоммуникаций в науке и образовании (АПИНО 2019). VIII Международная научно-техническая и научно-методическая конференция: сб. науч. ст. в 4-х т. 2019. Т. 1. С. 586–590.

5. Information technology. Security techniques. Code of practice for information security controls based on ISO/IEC 27002 for cloud services: BS ISO/IEC 27017:2015, 2015. 30 p.

6. Котенко И. В., Тынымбаев Б. А. Архитектура перспективной системы UEBA для провайдеров облачных услуг // Актуальные проблемы инфо-телекоммуникаций в науке и образовании (АПИНО 2019). VIII Международная научно-техническая и научно-методическая конференция: сб. науч. ст. в 4-х т. 2019. Т. 1. С. 581–585.

7. Chen Z., Tian L., Lin Ch. Trust evaluation model of cloud user based on behavior data // Procedia Computer Science, 2013, V. 17. PP. 1170–1177.

8. Veisdal J. The mathematics of Elo Ratings // Medium, September 2019. URL: https://medium.com/cantors-paradise/the-mathematics-of-elo-ratings-b6bfc9ca1dba.

9. Sonas J. The Sonas Rating formula – better than Elo? // Chess News, October, 2002. URL: https://en.chessbase.com/post/the-sonas-rating-formula-better-than-elo.

10. Котенко И. В., Чечулин А. А. Комбинирование механизмов защиты от сканирования в компьютерных сетях // Защита информации. 2010. № 6. С. 21–27.

УДК 519.876.2
ГРНТИ 81.93.29

СРАВНИТЕЛЬНЫЙ АНАЛИЗ РЕШЕНИЙ ПО ПОСТРОЕНИЮ ПЕРСПЕКТИВНЫХ СИСТЕМ UBA И UEBA

И. В. Котенко[1], Б. А. Тынымбаев[2]

[1]Санкт-Петербургский институт информатики и автоматизации Российской академии наук
[2]Евразийский национальный университет Республики Казахстан

Одной из актуальных задач в области кибербезопасности является создание систем (компонентов), реализующих обнаружение и противодействие кибератакам

на основе анализа поведения пользователей. В работе проводится анализ текущих практических решений по построению систем и компонентов анализа поведения пользователей - систем UBA и UEBA. Также анализируются научные исследования по аналитике поведения пользователей. Систематизируются сведения об использовании математических моделей в системах UBA и UEBA.

аналитика кибербезопасности, поведение пользователей, информационная безопасность, UEBA.

Введение

Ввиду роста угроз в сфере кибербезопасности, а также наличия большого количества данных, требуемых для анализа в системах кибербезопасности, одним из актуальных направлений развития в области кибербезопасности является обеспечение эффективной ситуационной осведомленности, в том числе определение с какими угрозами необходимо бороться, и какими рисками кибербезопасности необходимо управлять [1].

В связи с этим, аналитические инструменты начинают активно использоваться в решениях кибербезопасности [2, 3].

Одними из таких решений является системы аналитики поведения пользователей, сокращенно UBA (*user entity behavior analytics*) и системы аналитики поведения пользователей и сущностей, сокращенно UEBA (*user entity behavior analytics*).

Сравнение существующих систем

В работе [4] осуществляется анализ имеющихся систем класса UEBA. Из последних обзоров стоит обратить внимание на статью [5]. В качестве ключевых тенденций стоит отметить следующие:

– ввиду того, что средний бизнес начал использовать системы подобного рода, можно утверждать, что уровень зрелости растёт;

– функциональность UEBA встроена в примыкающих технологиях кибербезопасности, таких как CASB (*cloud access security brokers*), системы контроля действий пользователями и другие системы защиты информации, так, что происходит объединение систем класса UEBA и SIEM;

– потенциальные клиенты считают, что усилия, направленные на внедрение UEBA и текущие операции, могут быть очень затратны в плане времени и достаточно трудоёмкими, чем это обещают вендоры, даже для основных сценариев определения угроз;

– добавление отдельных или основных сценариев может быть трудным процессом в плане исполнения, требующим экспертизы в управлении данными и аналитики.

Из статьи [6] на примере анализа системы FortiInsight обращается внимание на применение агентов, которые собирают данные о действиях на конечных устройствах.

Наиболее используемые сценарии обнаружения угроз для облачных сервис-провайдеров представлены в таблице.

ТАБЛИЦА. Сценарии обнаружения угроз

Сценарий	Описание
Обнаружение компрометации учётной записи	Решение UEBA определяет ситуации, когда учётные данные были украдены и используются кем-то иным. Выявление использования учётной записи или злоупотребления учётной записи - одни из примеров данного сценария
Обнаружение скомпрометированного конечного устройства	Решение класса UEBA используется для обнаружения сетевых устройств, которые были скомпрометированы / заражены вредоносным ПО или демонстрируют подозрительное поведение
Обнаружение утечки данных	UEBA также используется для выявления утечки данных. Неавторизованная или целенаправленная утечка данных может случиться даже в действиях авторизованного пользователя. В результате данный сценарий сфокусирован на определении такого типа активности, которая необходима для выявления скомпрометированных учётных записей и конечных устройств.
Использование злонамеренно внутреннего доступа, включая привилегированный доступ	Инструменты UEBA могут быть использованы для выявления пользователей (работники и доверенные третьи лица), злоупотребляющих своими привилегиями доступа, которые во многих случаях связаны с злонамеренным событием. Примеры типов активности с превышением привилегий или неавторизованного доступа к данным (например, получение доступа к базе данных с персональной информацией) или в случае злоупотребления системными привилегиями (например, создание новой пользовательской учётной записи или присваивание дополнительных привилегий в разрез политики безопасности).
Предоставление дополнительной информации и контекста для исследования	Технологии UEBA основаны на анализе больших объемов информации касательно пользователей и сущностей в организации для определения аномалий, связанных с угрозами. Эта информация используется аналитиками для приоритезации предупреждений и расследования инцидентов. Если аналитик подозревает, что конечная станция была скомпрометирована, он может использовать решение UEBA для получения информации о пользователях данной рабочей станции, их регулярном поведении и роли конечной станции в сети

Сценарий	Описание
Разработка отдельных сценариев	Вендоры UEBA часто упоминают сценарии, где их решения используются в виде, отличающемся от оригинального назначения, начиная с обнаружения мошенничества до трекинга наркотиков в организациях здравоохранения. Достаточно важным является обеспечение возможности собирать отдельные данные и создавать типичные модели машинного обучения для таких сценариев

Используемые модели и алгоритмы

Как известно, существуют два основных подхода для выявления кибер-атаки: распознавание атаки по примеру/шаблону; выявление аномальной активности.

Выявление аномального поведения – основная функция систем класса UEBA. Для данного функционала могут использоваться различные методы, основными из которых являются методы машинного обучения [7], например, [8]. В работе [9] приведены примеры использования алгоритмов OCSVM: репликатор нейронной сети, изолированного леса, а также комбинации данных методов.

Перспективным является подход к обнаружению, основанный на моделях Маркова. В работе [10] представлены подход к использованию цепей Маркова для обнаружения атак и результаты экспериментов по анализу устойчивости модели.

Также уместно использование скрытых моделей Маркова на основе анализа системных вызовов [11].

Одним из минусов использования данных моделей является их вычислительная сложность. Теоретическая оценка вычислительной сложности с учетом прохождения каждого пути в каждом направлении, используя данные для обучения, составляет $O(TS^2)$, где T – длина каждого пути системных вызовов, S – число состояний. Также достаточно высоки требования по объему хранимых данных.

В работе [12] описаны методы определения аномального поведения объектов/сущностей компьютерной сети. Текущее поведение наблюдаемого процесса определяется следующим образом:

$$D(k) = \frac{1}{e} \sum_{i=k-e+1}^{k} C_{normal}(\overline{s_i}),$$

где e – длина окна, наблюдаемого процесса, s_i – системные вызовы, C_{normal} – измеряемый поток нормального поведения.

Для принятия решения об обнаружении аномалии вводится весовой коэффициент λ. Если $D(k) \geq \lambda$, текущее поведение наблюдаемого процесса принимается как нормальное. Если же $D(k) < \lambda$, поведение – аномальное.

Текущее поведение соответствует системным вызовам, которые определяются с учетом наблюдаемых процессов.

Используемые архитектуры

В плане архитектуры стоит обратить внимание на работу [13], где представлена архитектура системы UEBA. Основная идея, лежащая в основе этой системы, состоит в том, что вся информация, связанная с конкретным объектом (пользователем, IP-адресом или устройством) объединяется из различных источников данных в комплексный профиль риска. Он обеспечивает связное визуальное представление всей интегрированной информации, связанной с данным объектом.

В работе [14] описан эксперимент для определения аномального поведения на основе стандартных событий аудита операционной системы Windows 7. Статистика по количеству событий входа пользователя в определенном интервале времени используется для создания модели обнаружения аномалий. Поскольку данные описывают дискретное количество событий, автор делает предположение о возможности создания модели с помощью распределения Пуассона.

Заключение

В работе проведен анализ текущих практических решений и исследовательских работ по построению систем и компонентов анализа поведения пользователей. Выделен ряд перспективных моделей и архитектур для построения систем класса UBA и UEBA. Направления будущих исследований связаны с построением моделей аналитики кибербезопасности, реализацией исследовательского прототипа и проведения экспериментов.

Исследование проводится при поддержке Минобрнауки России в рамках Соглашения № 05.607.21.0322 (идентификатор RFMEFI60719X0322).

Список используемых источников

1. Котенко И. В., Кулешов А. А., Ушаков И. А. Система сбора, хранения и обработки информации и событий безопасности на основе средств Elastic Stack // Труды СПИИРАН. 2017. № 5 (54). С. 5–34.

2. Котенко И. В., Саенко И. Б, Кушнеревич А. Г. Архитектура системы параллельной обработки больших данных для мониторинга безопасности сетей Интернета вещей // Труды СПИИРАН. 2018. № 4 (59). С. 5–30.

3. Котенко И. В. Аналитика кибербезопасности: анализ современного состояния и перспективные направления исследований // Актуальные проблемы инфотелекоммуникаций в науке и образовании (АПИНО 2018). VII Международная научно-техническая и научно-методическая конференция : сб. науч. ст. в 4-х т. 2018. Т. 1. С. 10–19.

4. Котенко И. В., Тынымбаев Б. А. Обзор решений класса UEBA // Актуальные проблемы инфо-телекоммуникаций в науке и образовании. VIII Международная научно-техническая и научно-методическая конференция: сб. науч. ст. в 4-х т. 2019. Т. 1. С. 586–590.

5. Sadovski G., Care J., MacDonald N., Teixeira H. Market guide for User and entity behavior analytics. Gartner, May 2019.

6. Панасенко А. Обзор FortiInsight для анализа поведения сотрудников (UEBA). URL: https://www.anti-malware.ru/reviews/Fortinet-FortiInsight#part4, February 2020.

7. Браницкий А., Котенко И. Анализ и классификация методов обнаружения сетевых атак // Труды СПИИРАН. 2016. № 4. С. 207–244.

8. Komashinskiy D., Kotenko I. Malware Detection by Data Mining Techniques Based on Positionally Dependent Features // Proceedings of the 18th Euromicro International Conference on Parallel, Distributed and network-based Processing (PDP 2010). Pisa, Italy, 17–19 February, 2010. Los Alamitos, California. IEEE Computer Society. 2010. P.617–623.

9. Xiangyu X., Zhang T., Zhao G., Du D., Ga Q., Zhao W., Zhang S. Method and system for detecting anomalous user behaviors: an ensemble approach // International Journal of Software Engineering and Knowledge Engineering. 2018. V. 28. N. 11n12. PP. 1637–1656.

10. Ye N., Zhang Y., Borror C. M. Robustness of the Markov-Chain Model for Cyber-Attack Detection // IEEE Transactions on Reliability. April 2004. PP. 116–123.

11. Warrender C., Forrest S., Pearlmutter B. Detecting Intrusions Using System Calls: Alternative Data Models // Proceedings of the 1999 IEEE Symposium on Security and Privacy (Cat. No.99CB36344), May 1999. PP. 133–145.

12. Xinguang T., Miyi D., Chunlai S., Xin L. Detecting network intrusions by data mining and variable-length sequence pattern matching // Journal of Systems Engineering and Electronicsю 2009. V. 20. N. 2. PP. 405–411.

13. Shashanka M., Shen M., Wang S. User and entity behavior analytics for enterprise security // 2016 IEEE International Conference on Big Data. PP. 1867–1874.

14. Sapegin A. High-Speed Security Log Analytics Using Hybrid Outlier Detection: Dissertation PhD: 13.03.2019 / Sapegin Andrey. The University of Potsdam. 2019. 166 p. URL: https://doi.org/10.25932/publishup-42611

УДК 004.043
ГРНТИ 81.93.29

МОДЕЛЬ ПРЕДСТАВЛЕНИЯ БОЛЬШИХ ДАННЫХ ОБ ИНСАЙДЕРСКИХ АТАКАХ В ФОРМАТЕ NOSQL

И. В. Котенко[1], И. А. Ушаков[2]

[1]Санкт-Петербургский институт информатики и автоматизации Российской академии наук
[2]Санкт-Петербургский государственный университет телекоммуникаций им. проф. М. А. Бонч-Бруевича

В статье исследуется создание модели представления Big Data об инсайдерских атаках в формате NoSQL для обнаружения инсайдеров в КС. Суть задачи заключается в сборе максимального количества данных из системы, сформировании с их помощью

профилей поведения пользователей и определения по совокупности собранной информации, поведение каких пользователей отличается от нормального поведения. Далее с использованием этой информации выявляются возможные инсайдеры и способы реализации ими злонамеренных действий.

информационная безопасность, инсайдерские атаки, компьютерные сети, NoSQL, модель представления данных.

В современном мире инсайдеры являются хорошо подготовленными злоумышленниками, которые применяют все множество методов и средств для проведения атак на информационные ресурсы. При этом сами атаки могут идти не по одному каналу, а сразу по нескольким, усложняя тем самым их «точечное» детектирование. Также, источником атак – инсайдером – может быть сам сотрудник организации, к которому изначально обеспечивается большее доверие, чем к внешнему. Как результат, реализуются угрозы нарушения конфиденциальности, целостности и доступности информации непосредственно из периметра самой информационной системы – что усложняет их обнаружение. Возможным решением является так называемое «профилирование поведения пользователей» [1, 2]. В этом случае все действия пользователей записывают и анализируются с целью выявления в них тех, которые потенциально можно отнести к злонамеренным.

В интересах сбора информации о поведении пользователей в виде, подходящем для дальнейшего анализа, предложим следующую модель представления данных, которая исходя из специфики задачи должна отвечать критериям Big Data. Поскольку вся информация для модели должна собираться из некоторых источников, то сначала необходимо их описать [3]. Исходя из большого авторского опыта такими источниками являются все устройства клиентов, которые подключаются к компонентам корпоративной сети как по проводным, так и по беспроводным каналам. Также, модель должна отслеживать и отражать все множество оборудования локальной сети, а также всех подключаемых пользовательских устройств – ноутбуков, мобильный телефонов, планшетов и др. [4]

Все множество источников, по которым возможен сбор информации, применимой для обнаружения злонамеренных действий инсайдеров, представлено на рис. (см. ниже).

Предложенная модель является аналитической и может быть записана в следующим виде:

$$M = \langle A, I \rangle ,$$

где A – множество атрибутов, описывающих поведение пользователей; I – отдельная «подмодель» инсайдера и критерии, по которым возможно разделение пользователей на инсайдеров и легальных.

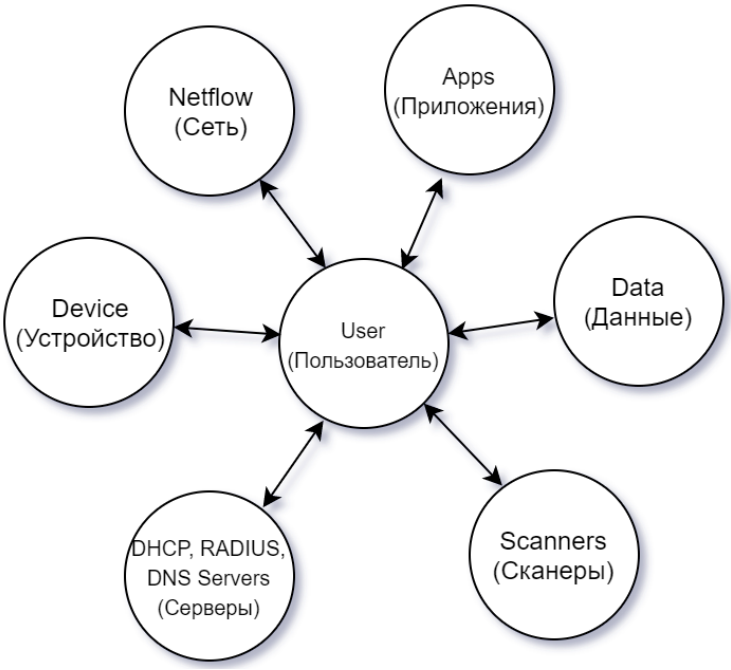


Рис. Источники для сбора информации,
применимой для обнаруженные инсайдеров

Атрибуты поведения пользователей можно записать в виде следующего кортежа:

$$A = \langle DataSources, Users, Data, Parser \rangle.$$

Опишем более детально элементы данного кортежа:

– $DataSources = \langle Netflow, Application, Scanner, Server, Device \rangle$ – источники информации, состоящие из набора сетевых пакетов, компьютерных программ, элементов ОС, сканера, серверного обеспечения, других устройств;

– $Users = \bigcup_{i=1}^{P} User_i$ – множество всех пользователей, где отдельный пользователь $User_i = \langle UserID_i, Attr_i, Sessions_i \rangle$ представим в виде триплета, который является отдельным кортежем из некоторого уникального идентификатора пользователя, его атрибутов и относящейся к нему сессии.

– $Data = \{0,1\}^+ = \{0,1,00,01,10,11,000, \dots\}$ – информация, которая содержит в себе все множество цепочек бит, расположенных на источниках информации.

– $Parser: Data \times DataSources \times Time \rightarrow Sessions$ – математическое отображение, которое создает сессию из информации с учетом типа источника информации и времени.

Используя предложенную нотацию модель самого инсайдера имеет следующую форму:

$$I =< R, L, Q, G >,$$

где R – критерии атрибутов, которые содержат в себе множество признаков, используемых для определении того, является ли пользователь легальным или же он инсайдер (например, типовой распорядок рабочего дня рядового пользователя определенной должности); L – доступа пользователя, задающий его права в корпоративной сети, превышение уровня которого сигнализирует о возможных действиях инсайдера в организации (например, принадлежность пользователя к определенному отделу организации, работающему со своим набором документов); Q – уровень подготовки инсайдера, задающий те навыки, опыт и знания, которые ему необходимы для успешности атаки (например, программный хакер – умеющий находить и использовать не декларированные возможности и backdoor-ы в программно-аппаратном обеспечении корпоративной сети; физический хакер – знающий способы взлома физических защит; случайный нарушитель – пользователь, который не ставит своей целью реализацию угроз в корпоративной сети, но может это осуществить по случайному стечению обстоятельств или из-за не знания основ информационной безопасности); G – главная цель инсайдера, задающая направление его действий (например, передачу конфиденциальной информации с заданного сервера третьим лицам).

Опишем более детально атрибуты, определяющие то, как ведет себя пользователь в корпоративной сети. Источники информации предоставляют данные о пользователях сети в необработанном (сыром) виде. Затем эти атрибуты необходимо обработать и преобразовать к подходящему виду – для этого используется упомянутое ранее отображение Parser. Для примера, из потока сетевых пакетов будут выделены соответствующие сессии (TCP, HTTP). Для программного обеспечения Parser выделит детали его установки в операционную систему, а для отдельных файлов – их создание, удаление или модификация.

Для объяснения работы приведем следующий пример. Пусть у нас есть источник информации *datasrc,* который создал на выходе данные *data* для заданного времени *time*. В этом случае уникальный идентификатор пользователя для некоторой сессии может быть записан, как:

$$uid \in \{userid | \langle userid, attr, sessions \rangle \in Users \wedge$$

$$Parser(data, datasrc, time) \in sessions\}$$

В этих данных заданы главные атрибуты, определяющие действия пользователя в корпоративной сети и которые подходят для анализа на предмет отнесения пользователя к легальному или инсайдеру [5, 6].

Представим их в виде множества пар Key и Document (табл., см. ниже), которые составляют поля базы данных.

Необходимо отметить, что заполнение значений в таблице произведено лишь частично и лишь для того, чтобы показать основной принцип хранения данных в базе.

ТАБЛИЦА. Пример главных атрибутов, используемых для выявления инсайдеров

Key	Document
1	{**"Session"**: "1001”, **"ID"**: "1", **"User-Agent"**: "Chrome", **"Login"**: "Ivan", **"Pass"**:"Ivan 123", **"T"**:"3", **"Income Traffic"**: [5,5,5, … 6,5,5], **"Outcome Traffic"**: [1,1,1, … 2,1,1], **"Traffic time"**: "01-01-2020 18:00:00", **"Rights"**:"Read|Write", "TotalAuth":"", "Active Directory-пробы":"", "AD-host":"", "AD-domain":"", "AD-operation-system":"", "AD-version OS":"", "AD-service pack":"", "Radius-пробы":"", "Calling-Station-ID":"", "NAS-IP-Address":"", "NAS-Port":"", "Framed-IP-Address":"", "Acct-Session-ID":"", "Acct-Session-Time":"", "Acct-Terminate-Cause":"", "On-For-Login-Auth":"", "DHCP-проба":"", "Dhcp-class-identifier":"", "Dhcp-client-identifer":"", "Dhcp-user-class-id":"", "Dhcp-requsted-address":"", "Dhcp-server-identifier":"", "Dhcp-parameters-request-list":"", "Dhcp-message-type":"", "DNS-пробы":"", "DNS-FQDN":"", "NMAP-пробы":"", "SessionData":"", "Session-ID":"", "Changes":"", "Auth":"", "LogPass":"", "Sites": [], "Periph":"", "Time":"", "Progs ":"", "NoAV":"", "LogType":"", "Geo":"", "Device-ID":"", "App-ID":"", "DeviceFields":"", "Name":"", "OS":"", "Vendor":"", "AppFields":"", "AppName":"", "Version":"", "Developer":"", "Ports":"", "Netflow":"", "Src IP address":"", "Dst IP address":"", "Nxt-Hop IP address":"", "In ifIndex":"", "Out ifIndex":"", "Packets":"", "Bytes":"", "Start time of flow":"", "End time of flow":"", "Src port":"", "Dst port":"", "TCP Flags":"", "IP protocol":"", "ToS":"", "Src AS":"", "Dst AS":"", "Src Mask":"", "Dst Mask":"", "Padding ":"", "Src VLAN":"", "Dst VLAN":"", "Src MAC":"", "Dst MAC - ":"", "UserFields":""}
2	{"Session":"1002”, "ID":"2", "User-Agent": "Firefox", "Login": "Petr", "Pass":"Pet_456", "T":"3", "Income Traffic": [0,0,0, … 0,0,10], "Outcome Traffic ": [10,0,0, … 0,0,0], ... }
…	…

В статье приведена модель хранения данных об пользователях, отражающая информацию, по которой можно их разделять на легальных и инсайдеров, и построенная на принципах Big Data. Модель имеет формат NoSQL. В дальнейших исследованиях планируется использовать данную модель для разработки методики обнаружения инсайдеров в компьютерной сети.

Работа выполнена в соответствии с Соглашением Минобрнауки России № 05.607.21.0322 (идентификатор RFMEFI60719X0322).

Список используемых источников

1. Котенко И. В., Ушаков И. А., Пелёвин Д. В., Преображенский А. И., Овраменко А. Ю. Выявление инсайдеров в корпоративной сети: подход на базе UBA и UEBA // Защита информации. Инсайд. 2019. № 5 (89). С. 26–35.

2. Ушаков И. А. Обнаружение инсайдеров в корпоративной компьютерной сети на основе технологий анализа больших данных // Вестник Санкт-Петербургского государственного университета технологии и дизайна. Серия 1: Естественные и технические науки. 2019. № 4. С. 38–43.

3. Котенко И. В., Ушаков И. А., Пелёвин Д. В., Овраменко А. Ю. Гибридная модель базы данных NoSQL для анализа сетевого трафика // Защита информации. Инсайд. 2019. № 1 (85). С. 46–54.

4. Komashinskiy D., Kotenko I. Malware Detection by Data Mining Techniques Based on Positionally Dependent Features // Proceedings of the 18th Euromicro International Conference on Parallel, Distributed and network-based Processing (PDP 2010). Pisa, Italy, 17–19 February, 2010. Los Alamitos, California. IEEE Computer Society. 2010. PP. 617–623.

5. Shashanka M., Shen M., Wang J. User and entity behavior analytics for enterprise security // 2016 IEEE International Conference on Big Data (Big Data). – Washington, DC, 2016. – PP. 1867–1874.

6. Shu X., Smiy J., Yao D., Lin H. Massive Distributed and Parallel Log Analysis for Organizational Security // IEEE Globecom Workshops (December). 2013. PP. 194–199.

УДК 004.043
ГРНТИ 81.93.29

ОБНАРУЖЕНИЕ ИНСАЙДЕРОВ В КОМПЬЮТЕРНОЙ СЕТИ НА ОСНОВЕ ЭКСПЕРТНЫХ ПРАВИЛ И МЕТОДОВ МАШИННОГО ОБУЧЕНИЯ

И. В. Котенко[1], И. А. Ушаков[2]

[1]Санкт-Петербургский институт информатики и автоматизации Российской академии наук
[2]Санкт-Петербургский государственный университет телекоммуникаций им. проф. М. А. Бонч-Бруевича

В статье рассматриваются подходы к обнаружению инсайдеров в компьютерной сети на основе экспертных правил и методов машинного обучения.

информационная безопасность, инсайдерские атаки, компьютерные сети, экспертные правила, методы машинного обучения.

После появления информационных технологий современный мир претерпел и продолжает претерпевать качественные изменения в своем функционировании, что влияет на жизнь практически всех его социальных и других групп. Основной причиной этого можно считать все проникающую информатизацию, связывающую невидимыми линиями его различных участников – людей, домашние устройства, автотранспорт, интеллектуальные системы (такие, как Умный Дом) и др. Тем не менее, как практически любой прогресс, у него есть и обратная сторона. Так, информационные технологии повышая такую сторону жизни людей, как комфорт, неизменно ведут к понижению другой ее стороны – безопасности. Особую актуальность последнее приобретает для передачи информации в рамках корпоративной

сети [1, 2, 3], которая, как правило, защищается в основном от внешних атак на информационные ресурсы. При этом считается, что внутренние атаки не настолько опасны или вообще отсутствуют, поскольку среда корпоративной сети считается доверенной.

Особенностью корпоративных сетей, помимо распределённой на достаточно большую территорию, является то, что основную работу с ее информационными ресурсами выполняют внутренние сотрудники. Последние, очевидно, априори изначально считаются легальными, поскольку работа с ресурсами прописана для них в должностных инструкциях. Это в ряде случаев и несет основную угрозу. Так, по ряду причин (финансовая прибыль, вандальные побуждения, спортивный интерес и пр.) пользователь из разряда легальных может перейти в группу инсайдеров путем реализации соответствующих угроз к информации, с которой он непосредственно работает или к которой случайно получил доступ. Борьба с инсайдерством является на данный момент крайне актуальной задачей информационной безопасности.

Противодействовать атаке инсайдера можно в различные точки ее осуществления – как еще до осуществления атаки, так и во время самого проведения атаки, а также уже впоследствии, стремясь снизить нанесенный ущерб и обнаружить источника атаки – инсайдера. Выбор точного момента для противодействия не имеет однозначного ответа, хотя очевидно, что любые превентивные меры всегда будут предпочтительнее. Также, слишком позднее реагирование в принципе может оказаться бесполезным, поскольку ценность украденных ресурсов уже уменьшиться (например, в случае их перепродажи или клонирования) и затраты на их возврат или восстановление попросту могут оказаться нецелесообразными.

Задаче обнаружения инсайдеров посвящено большое количество исследовательских работ [1, 2, 3, 4, 5, 6, 7, 8]. Существуют различные подходы к решению задачи обнаружения инсайдеров, наиболее востребованными среди которых являются следующие: на основе экспертных правил, а также с использованием интеллектуального анализа (на базе методов машинного обучения). Наиболее интересным с практической точки зрения может быть подход комбинирования представленных подходов.

Однако, если имеются 2 качественно разных алгоритма обнаружения инсайдеров (таких, как на базе экспертных правил и методов машинного обучения), то возникает задача объединения результатов их работы.

Опишем 4 наиболее распространенные комбинации результатов с точки зрения того, каким образом получается итоговое множество результирующих данных из исходных множеств инсайдеров, полученных каждым из алгоритмов:

1) объединение – итоговое множество содержит информацию об инсайдерах, которые были детектированы хотя бы одним из алгоритмов (оператор – ∨);

2) пересечение – итоговое множество содержит информацию об инсайдерах, которые были детектированы как первым, так и вторым алгоритмом (оператор – ∧);

3) только 1-й – итоговое множество содержит информацию об инсайдерах, которые были детектированы первым алгоритмом, но были пропущены вторым алгоритмом (оператор – *I*);

4) только 2-й – итоговое множество содержит информацию об инсайдерах, которые были детектированы вторым алгоритмом, но были пропущены первым алгоритмом (оператор – *II*).

Результаты работы приведенных выше комбинаций могут быть представлены в интуитивно-понятном виде на рис. 1 (итоговое множество ограничено прерывистой линией красного цвета).

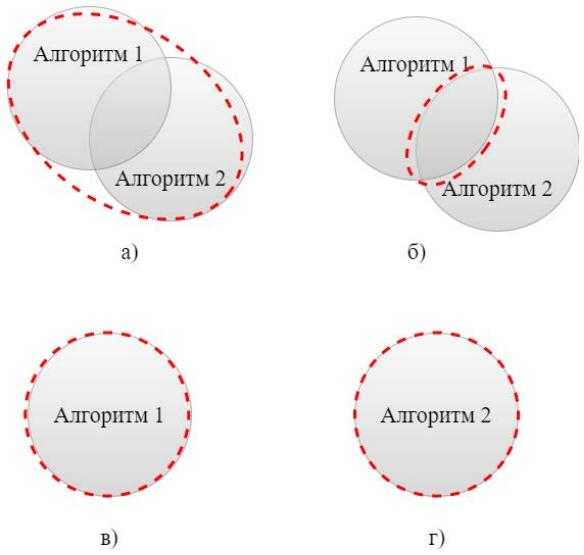


Рис. 1. Интуитивное-понятное представление результатов работы комбинаций алгоритмов: а) объединение, б) пересечение, в) только первый, г) только второй

В аналитическом виде описанное выше комбинирование результатов работы комплекса (K_A) двух алгоритмов (A_1 и A_2) по обнаружению инсайдеров в корпоративной сети может быть записано как:

$$\begin{cases} K_A = \{A_1 \otimes A_2\} \\ \otimes \in \{I, II, \vee, \wedge\} \end{cases},$$

где $\otimes$ – оператор составления комбинации, *I* – итоговое множество результатов работы 1-го алгоритма, *II* – итоговое множество результатов работы 2-го алгоритма, ∨ – итоговое множество объединения результатов работы алгоритмов, ∧ – итоговое множество пересечения результатов работы алгоритмов.

В зависимости от способа вычисления итогового множества инсайдеров, очевидно, будет зависеть и результативность работы всей системы обнаружения, которая классически оценивается, используя приведенное на рис. 1 представление результатов работы комбинации алгоритмов можно отразить в графическом виде меры качества (TP – истинно-положительный, TN – истинно-отрицательный, FP – ложно-положительный, TN – ложно-отрицательный) так, как показано на рис. 2 с помощью мер качества.

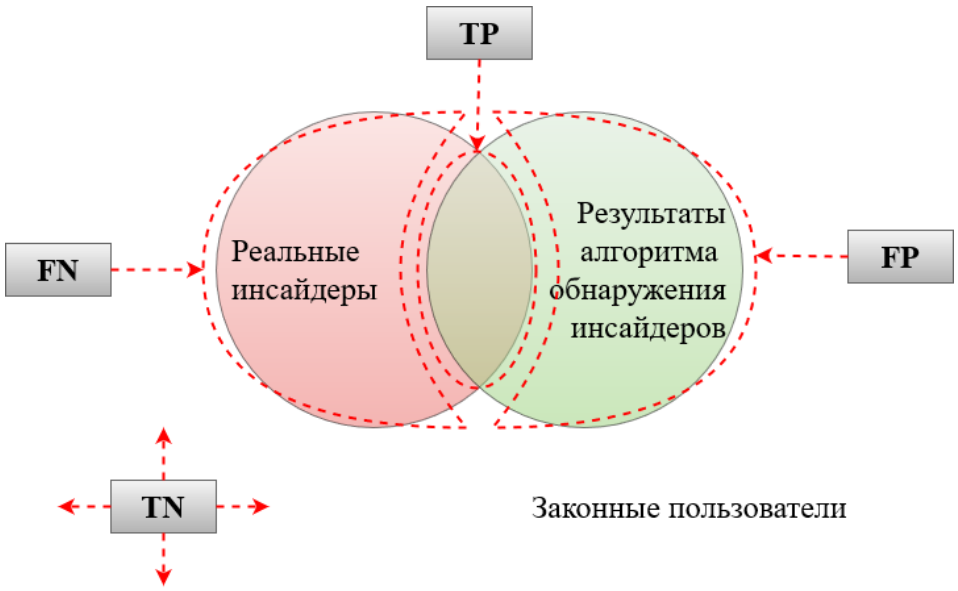


Рис. 2. Представление в графическом виде мер качества работы алгоритма по выявлению инсайдеров

Дадим пояснения к рисунку 2. Рисунок содержит множества в виде двух кругов – зеленого и красного. Первый круг интерпретируется, как множество пользователей, которые алгоритм отнес к инсайдерам. А второй круг – как множество реальных инсайдеров, действующих в корпоративной сети. При этом каждый алгоритм мог как пропустить некоторых инсайдеров, так и ошибочно отнести к ним легальных пользователей – именно это и снижает результативность работы системы обнаружения. Используя тот факт, что эти два множества могут пересекаться, как раз и возможно ввести интерпретацию мер качества. Необходимо пояснить, что границы двух непрерывных множеств как раз и делят все пространство на 4 части – пересечение множеств, область без множеств, не пересекаемая часть первого множества и не пересекаемая часть второго множества.

Исходя из выше сказанного и определений мер качеств дадим им следующее графическое отображение:

а) TP – пересечение зеленого и красного кругов, означающее корректную работу алгоритма по обнаружению инсайдеров;

б) TN – область вне зеленого и красного кругов, означающая корректную работу алгоритма по обнаружению легальных пользователей (т. е. не отнесению пользователей к инсайдерам);

в) FP – область зеленого круга, не пересекаемая с красным кругом, означающая ошибочное отнесение алгоритмом легальных пользователей к инсайдерам (ошибка первого рода);

г) FP – область красного круга, не пересекаемая с зеленым кругом, означающая ошибочное отнесение алгоритмом инсайдеров к легальным пользователям инсайдерам (ошибка первого рода).

В статье предложен подход к обнаружению инсайдеров на основе комбинированного использования алгоритмов, основанных на экспертных правилах и методах машинного обучения. Направление будущих исследований заключается в проведении развернутых экспериментов по использованию различных комбинаций алгоритмов и поиска наилучшей комбинации для решения задачи обнаружения инсайдеров.

Работа выполнена в соответствии с соглашением Минобрнауки России № 05.607.21.0322 (идентификатор RFMEFI60719X0322).

Список используемых источников

1. Савинов Н. В., Токарева К. А., Ушаков И. А., Красов А. В., Сахаров Д. В. Исследование модели сети ЦОД на основе политик Cisco ACI // Защита информации. Инсайд. 2019. № 4 (88). С. 32–43.

2. Котенко И. В., Ушаков И. А. Использование технологий больших данных для мониторинга инцидентов информационной безопасности // Региональная информатика «РИ-2016» : материалы конференции. 2016. С. 168–169.

3. Дубровин Н. Д., Ушаков И. А., Чечулин А. А. Применение технологии больших данных в системах управления информацией и событиями безопасности // Актуальные проблемы инфотелекоммуникаций в науке и образовании сборник научных статей (АПИНО 2016). V Международная научно-техническая и научно-методическая конференция. 2016. С. 348–353.

4. K. Nance, R. Marty. Identifying and Visualizing the Malicious Insider Threat Using Bipartite Graphs // 44th Hawaii Int. Conf. on System Sciences. 2011. PP. 1–9.

5. J. Ignacio, M. Martinez, R. Eliot, C. Stephen, D. Andersen, T. Stewart. A Behavioral Theory of Insider-Threat Risks: A System Dynamics Approach // ACM Transactions on Modeling and Computer Simulation (TOMACS). Vol. 18. Iss. 2. – PP. 1–27.

6. Y. Chen, S. Nyemba, W. Zhang, B. Malin. Specializing network analysis to detect anomalous insider actions // Security Informatics. 2012. Vol. 1. Art. 5. – PP. 1–24.

7. T. Chen et al. A probabilistic analysis framework for malicious insider threats // International Conference on Human Aspects of Information Security, Privacy, and Trust. Springer, Cham, 2015. PP. 178–189.

8. Котенко И. В., Ушаков И. А., Пелевин Д. В., Преображенский А. И., Овраменко А. Ю. Выявление инсайдеров в корпоративной сети: подход на базе UBA и UEBA // Защита информации. Инсайд. 2019. № 5 (89). С. 2–11.

УДК 004.056.53
ГРНТИ 81.93.29

АНАЛИЗ АЛГОРИТМОВ ОБНАРУЖЕНИЯ АНОМАЛЬНОГО ПОВЕДЕНИЯ В СОЦИАЛЬНЫХ СЕТЯХ

И. В. Котенко[1,2], А. В. Хинензон[1]

[1]Санкт-Петербургский государственный университет телекоммуникаций им. проф. М. А. Бонч-Бруевича
[2]Санкт-Петербургский институт информатики и автоматизации Российской академии наук

Задача обеспечения информационной безопасности в пространстве социальных сетей, занимает ключевые позиции в современном мире. Возможными путями решения такой задачи при стремительном развитии информационных технологий могут быть алгоритмы машинного обучения и глубокого анализа данных. Авторы исследуют модели, методы и алгоритмы машинного обучения, а также статистический анализ данных, применимые для обнаружения аномального поведения в социальных сетях. В работе рассматриваются существующие подходы, формируются наборы признаков аномального поведения и предлагается классификация аккаунтов по ним.

машинное обучение, социальные сети, аномальное поведение, информационная безопасность.

За последнее десятилетие спрос на социальное взаимодействие посредством такого инструмента, как социальные сети, возрос. Это говорит об увеличении количества пользователей и зарегистрированных учетных записей в медиа пространстве. По данным статистики из отчета о состоянии цифровой сферы Digital 2020 наиболее популярными социальными платформами являются Facebook (2,449 млн), Youtube (2,000 млн), Whatsapp (1,600 млн) [1]. В России, конечно же, лидирует социальная сеть ВКонтакте.

Одновременно со среднестатистическими пользовательскими аккаунтами, для достижения различных целей, например, рекламы, распространения новостей или общения, появляются аккаунты вредоносного характера и назначения. Тем самым подвергается опасности сохранение принципов информационной безопасности. Количество дублированных и ложных учетных записей Facebook по всему миру на 4 квартал 2018 года составило 255,2 млн и 116 миллионов. Данное число показывает, что злоумышленники и мошенники не только находят новые пути для нежелательных действий, но и используют ряд устоявшихся атак.

Условно категорирование аккаунтов в социальных сетях по их поведению, можно провести таким образом, как представлено в таблице.

ТАБЛИЦА. Классификация аккаунтов по признакам аномального поведения

Класс	Признаки аномального поведения	Примеры действий злоумышленника
Поддельный аккаунт (ПА), Sybil	Копирование личных изображений, личных данных	Перехват управления коммуникационной среды законного пользователя, подрыв репутации, разрушение доверительных отношений, сбор личной информации, травля, спам, создание новостных лент, создание подпольного рынка для покупки подписчиков
Спам-аккаунт (СА)	Наличие множества рекламных сюжетов, на личной странице	Распространение нежелательной информации, ложной распространение вредоносных ссылок
Скомпрометированный аккаунт (СкА)	Аккаунт реального пользователя, похищенный у жертвы	Разрушение доверительных отношений, социальный инжиниринг, вымогательство, мошенничество, фрауд, влияние на результаты голосования

Моделирование процесса обнаружения программных ботов стало одной из задач проведения экспериментов авторами [2, 3] по предложенной архитектуре интегрированной системы мониторинга и противодействия злонамеренному влиянию, а также определения источников и путей распространения информации.

Организация атак возможна при использовании знаний социальной психологии, компьютерных технологий в совокупности с уязвимостью пользователя т. е. социальной инженерии (СИ). Под термином СИ понимают набор прикладных и аналитический приемов, которые применяются нелегитимными пользователями для скрытого побуждения людей в сети к нарушениям политик и правил в области информационной безопасности [4].

Социальная инженерия направлена на такие действия, выполняемыми злонамеренными аккаунтами, как: фишинг – вид мошенничества, при котором происходит захват логинов и паролей, путем рассылок спама и перехода на сторонние сайты; фарминг – вид мошенничества с использованием переадресации пользователя на ложный IP адрес; претекстинг – атака с целью выуживания конфиденциальной информации, при этом уже владея некоторыми данными о жертве, представляясь другим человеком; фрауд – перехват смс при использовании электронных платежей в кошельках; сбор информации из открытых источников с последующим профилированием – индивидуально ориентированный механизм. Все данные механизмы приводят к последствиям разной степени тяжести, исходя из модели коммуникации пользователя в [5] и наблюдения, что социальные сети являются менее

контролируемыми со стороны закона, чем такие информационные каналы как СМИ, ТВ, или радио.

При этом, социальный инжиниринг почти всегда связан с перехватом управления аккаунтом и последующим его аномальным поведением (АП). Аномальное поведение с точки зрения аналитики данных и теории статистики представляет собой некий выброс, который выделяется из общей выборки. Как правило, аномальное поведение являет собой «проблемную активность». Следовательно, в контексте социальных сетей, за АП можно принять автоматизированную программу, управляющую аккаунтом – бота, ботнет или иного пользователя (злоумышленника).

Отдельно стоит отметить, что к методам обнаружения ботов и бот-сетей в социальном пространстве относят: изучение статичных признаков (изучение профиля: количества друзей, наличия данных о самом пользователе, наличие фотографий т. д.); методы автоматизированного обнаружения, при помощи прикладных программ; метод частотного анализа сообщений; метод анализа распространяемого контента, а также методы машинного обучения.

Опираясь на [6] выделим подходы, подразделяющиеся на три класса:

– системы обнаружения ботов на основе графического представления;

– системы, основанные на краудсорсинге и привлечении человеческого интеллекта;

– методы машинного обучения, основанные на выявлении показательных функций, различающих ботов и людей.

При этом есть несколько подходов обучения классификаторов: контролируемый, неконтролируемый, полууправляемый [7].

Контролируемый подход, основывается на маркированных данных с набором функций. Это требует экспертной оценки. В исследовании [8] при помощи ручной разметки, авторы выбрали отличительные черты злонамеренных пользователей, это – публикация нежелательных сообщений, публикация информации, не имеющей отношения к данному пользователю, а также стремление к следованию за более крупными аккаунтами с относительно небольшим количеством подписчиков. Через некоторое время, в микроблоге Twitter, проявился на практике автоматизированный подход с высокой точностью итога по маркировке данных, использующий параметры по оценке пользователя и оценке твита. Впоследствии авторы данного исследования обучили пять алгоритмов классификации с использованием функций контента и поведения. Производительность дерева решений и случайного леса (*random Forest* RF) показали высокий процент точности. Недочет данного подхода состоит в том, что существует возможность при реальных условиях получить ложную тревогу.

В сборнике [9] подробно описывается метод ансамблевого обучения на основе мета-классификатора (*Meta-based*) для классификации настроений. Суть данного метода состоит в совмещении нескольких алгоритмов машинного обучения в одну сильную прогнозирующую модель. Плюсом данной модели является улучшение качества прогнозирования классификаторов, а также успешного выявления спамеров, за счет обнаружения высокой доли спам-слов в совокупности с другими функциями контента. Проблематика состоит в нахождении независимых классификаторов и неопределенности достижения достаточной производительности на используемых данных [10].

Полууправляемые алгоритмы машинного обучения подбирают модель для классификации с использованием как маркированных, так и немаркированных данных. Такой подход может быть оптимален в пространстве с нехваткой маркированных данных для обнаружения аномального поведения.

Неконтролируемое обучение соответственно не использует маркированные данные. Следовательно, невозможно предопределить исход и проявление атаки. Сущность метода составляет объединение данных в кластеры исходя из их начальных характеристик. К приведенной категории относят метод попарного сходства (*Pairwise similarity*) – сравнение двух учетных записей, основанных на их деятельности для выяснения неожиданно проявившихся характеристик.

Данный метод крайне удобен для скомпрометированных аккаунтов. Наблюдение за поведением аккаунта, с последующим сравнением, как с легитимным, позволяет выявлять аномальное поведение злоумышленника. Однако важным замечанием при использовании такого метода будет строгая настойка модели, так как злоумышленник может сам скомпрометировать ход, подобный идеальной модели. Можно выделить работу авторов [11] по выявлению лидеров мнений, посредством собранных данных которого можно провести сравнительный анализ сообществ в сети.

Авторы исследования [12] разработали алгоритм для обнаружения поддельных аккаунтов, где сначала происходит идентификация и категорирование подозрительных пользователей с учетом их IP адресов. Следом применяется восходящая (агломеративная) кластеризация. Данный метод трудно осуществляется при работе с большими данными.

Подводя итоги отметим, что социальные сети становятся важной частью жизни людей и их жизнедеятельности. Публикация, обмен и распространение информации дает повод злоумышленникам совершать нежелательные и противоправные действия. Необходимость обнаружения аномального поведения актуальна и важна.

В статье рассматривались методы и алгоритмы машинного обучения. Были определены понятия и признаки аномального поведения в пространстве социальных сетей.

Работа выполнена при финансовой поддержке Гранта РНФ (проект РНФ № 18-71-10094) в СПИИРАН.

Список используемых источников

1. Most popular social networks worldwide as of January 2020, ranked by number of active users [Электронный ресурс] // Statista. URL: https://www.statista.com/statistics/272014/global-social-networks-ranked-by-number-of-users/ (дата обращения 01.03.2020).

2. Kotenko I., Saenko I., Chechulin A., Desnitsky V., Vitkova L., Pronoza A. Vjnitoring and counteraction to malicious influences in the information space of social networks // 10th International Conference on Social Informatics (SocInfo). 2018. PP. 159–167.

3. Виткова Л. А. Методика анализа аудитории канала распространения информации в социальных сетях // Известия высших учебных заведений. Технология легкой промышленности. 2018. Т. 42. № 4. С. 5–10.

4. Хлобыстова А. О., Абрамов М. В., Тулупьева Т. В., Тулупьев А. Л. Социальное влияние на пользователя в социальной сети: типы связей в оценке поведенческих рисков, связанных с социоинженерными атаками // Управленческое консультирование 2019. С. 104–117.

5. Виткова Л. А. Место и роль мониторинга и противодействия нежелательной информации в социальных сетях // Актуальные проблемы инфотелекоммуникаций в науке и образовании (АПИНО 2019). VIII Международная научно-техническая и научно-методическая конференция : сб. науч. ст. в 4-х т. 2019. Т. 1. С. 209–212.

6. Emilio Ferrara Measuring social spam and the effect of bots on information diffusion in social media // Computational Social Sciences 2014 – 2020 P. 1–26.

7. Kayode Sakariyah Adewole, Nor Badrul Anuar, Amirrudin Kamsin, Kasturi Dewi Varathan, Syed Abdul Razak Malicious accounts: Dark of the social networks // Journal of Network and Computer Applications. 2017. P. 41–67.

8. J. Martinez-Romo, L. Araujo Detecting malicious tweets in trending topics using a statistical analysis of language Expert Syst. Appl., 40 (2013), pp. 2992–3000.

9. Mohammad Shorif Uddin, Jagdish Chand Bansal Proceedings of International Joint Conference on Computational Intelligence // Algorithms for Intelligent Systems 2019 P. 84.

10. Шелухин О. И., Ванюшина А. В., Габисова М. Е. Фильтрация нежелательных приложений интернет-трафика с использованием алгоритма классификации RANDOM FOREST // Вопросы кибербезопасности. 2018. С. 44–50.

11. Виткова Л. А., Кураева А. М., Проноза А. А., Чечулин А. А. Анализ методов выявления и оценки страниц лидеров мнений в социальных сетях // Актуальные проблемы инфотелекоммуникаций в науке и образовании (АПИНО 2019). VIII Международная научно-техническая и научно-методическая конференция : сб. науч. ст. в 4-х т. 2019. Т. 1. С. 233–237.

12. Ahmed F., Abulaish M. An MCL-based approach for spam profile detection in online social networks // 2012 IEEE Proceedings of the 11th International Conference on Trust, Security and Privacy in Computing and Communications (TrustCom).

УДК 004.733
ГРНТИ 49.33.29

ПРОЕКТИРОВАНИЕ СЕГМЕНТА СЕТИ АПК «БЕЗОПАСНЫЙ ГОРОД» И ИССЛЕДОВАНИЕ МЕТОДОВ ОБЕСПЕЧЕНИЯ ЗАЩИТЫ ОТ АУТСАЙДЕРСКИХ УГРОЗ

А. В. Красов, А. В. Крылов, И. А. Ушаков

Санкт-Петербургский государственный университет телекоммуникаций им. проф. М. А. Бонч-Бруевича

Современные города должны соответствовать возрастающим информационным потребностям граждан и автономно обеспечивать их безопасность. Для этого сети, объединяющие АПК в единую структуру, совершенствуются и расширяются, появляются новые возможности и растет уровень безопасности таких сетей. Города, в ближайшем будущем, станут удобнее и безопаснее для каждого, благодаря внедрению АПК повсеместно.

обеспечение безопасности, АПК «Безопасный город», сегмент сети городского уровня, внедрение системы безопасности, методы защиты от аутсайдерских атак.

Аппаратно-программный комплекс «Безопасный город» (АПК «Безопасный город») – совокупность комплексов средств автоматизации, объединенных для решения задач в сфере обеспечения защиты населения и территорий от чрезвычайных ситуаций природного и техногенного характера, общественной безопасности, правопорядка и безопасности среды обитания.

Структура АПК состоит из 12 частей – автоматизированных систем. Перечень автоматизированных систем государственной информационной системы «Аппаратно-программный комплекс «Безопасный город» и порядок их взаимодействия описан в постановлении Правительства Санкт-Петербурга от 25.08.2016 № 759.

Все компоненты АПК «Безопасный город» объединены Единой мультисервисной телекоммуникационной сетью, которая обеспечивает функционирование системы в целом и создает единое информационное пространство для всех пользователей [1].

Целью построения и развития аппаратно-программного комплекса «Безопасный город» является повышение общего уровня общественной безопасности, правопорядка и безопасности окружающей среды за счет обеспечения координации деятельности сил и служб, путем внедрения на базе

муниципальных образований комплексной информационной системы, обеспечивающей прогнозирование, мониторинг, предупреждение и ликвидацию возможных угроз.

Основными задачами построения и развития комплекса «Безопасный город» являются:

– формирование коммуникационной платформы для органов местного самоуправления;

– разработка единых функциональных и технических требований к аппаратно-программным средствам;

– обеспечение информационного обмена между участниками всех действующих программ;

– обеспечение информационного обмена на федеральном, региональном и муниципальном уровнях;

– создание дополнительных инструментов для оптимизации работы;

– построение и развитие систем ситуационного анализа.

Единая информационно-коммуникационная инфраструктура комплекса «Безопасный город» строится по модульному принципу с возможностью включения в единый контур управления и информационного обмена элементов уже существующей инфраструктуры муниципальных образований.

Для проектной реализации был выбран сегмент сети Городской системы видеонаблюдения по адресу пл. Александра Невского. Данный сегмент обеспечивает: видеонаблюдения объектной площади, общественную сеть wi-fi для граждан, экстренную связь с полицией, интегрирование локальных сетей метрополитена и гостиницы.

На карте объекта (рис. 1) представлено расположение телекоммуникационного оборудования и средств видеонаблюдения.

Рис. 1. Карта объекта

Схемы построения сети представлены на рис. 2–4.

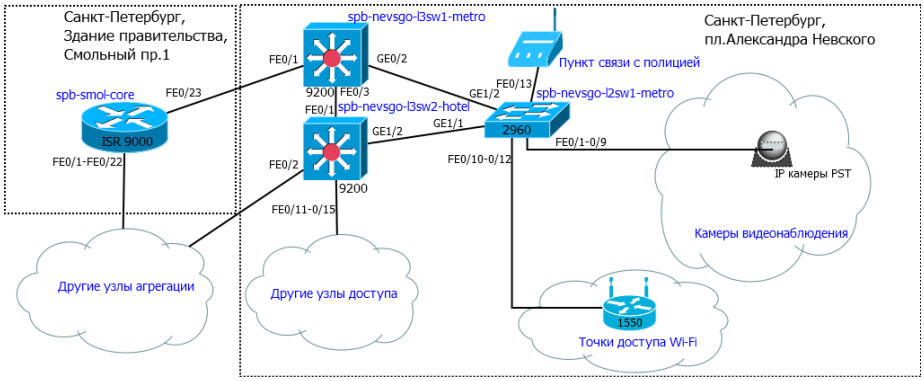


Рис. 2. Физический уровень

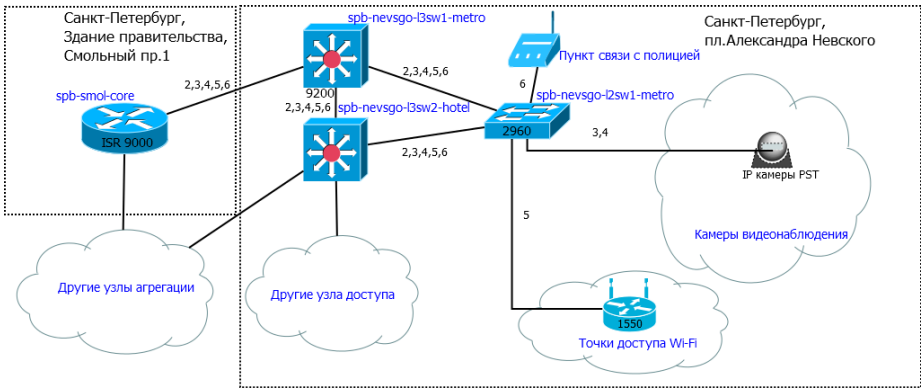


Рис. 3. Канальный уровень

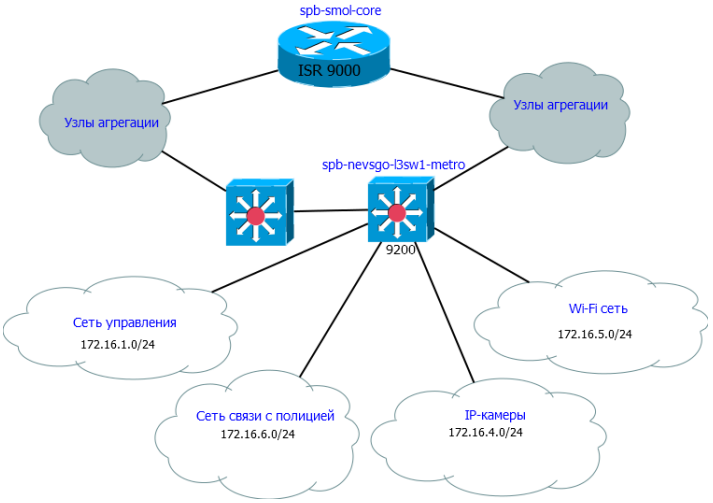


Рис. 4. Сетевой уровень

Для реализации проекта сегмента сети АПК «Безопасный город» было выбрано следующее оборудование:

1) Уровень Ядра – Роутер Cisco ASR 9000, они отличаются избыточностью и высокой доступностью за счет возможности агрегирования каналов, установки резервных аппаратных элементов и целых маршрутизаторов

и пр. Основная особенность Cisco ASR – физическое разделение аппаратных инструментов управления и коммутации, что позволяет значительно ускорить реализацию сетевых процессов.

2) Уровень распространения – L3 коммутаторы Cisco 9200.

3) Уровень доступа – L2 коммутаторы Cisco 2960, IP камеры PST.

Выбранное оборудование полностью соответствует потребностям и требованиями сети АПК. Уровень распространения строится по кольцевой топологии, обеспечивая отказоустойчивость сети.

Основным типом угроз для сети АПК являются аутсайдерские (снаружи).

Базовые методы защиты оборудования:

– Подключения только по протоколу SSH.

SSH – Secure SHell, сетевой протокол прикладного уровня, который дает возможность шифрования передаваемых данных и паролей [3]. Только данный протокол обеспечит шифрованное подключение к оборудованию.

– Использования шифрования в паролях доступа.

Каждый пароль, настраиваемый на оборудование, должен шифроваться в закрытом виде.

– Разделения уровня привилегий.

Функционал оперативной системы оборудования Cisco позволяет разделить права доступа по различным ролям (например, полный доступ или права только на просмотр настроек).

– Ограничения физической доступности устройств.

Каждое устройство должно быть хорошо защищено от физического воздействия, при помощи железных боксов и замков.

– Настройка сетевого времени (протокол NTP).

Протокол NTP обеспечивает механизмы синхронизации с точностью до наносекунд. Протокол предлагает средства для определения характеристик и оценки ошибок локальных часов и временного сервера, который осуществляет синхронизацию. Предусмотрены возможности работы с иерархически распределенными первичными эталонами, такими как синхронизуемые радио-часы [4].

– Логирование Syslog.

Syslog – протокол передачи текстовых сообщений, прежде всего логов – сообщений о происходящих событиях [5]. Протокол позволяет отслеживать все действия, произошедшие в сети.

– Отключение протоколов обнаружения (CDP, LLDP).

CDP (англ. *Cisco Discovery Protocol*) – проприетарный протокол второго уровня, разработанный компанией Cisco Systems, позволяющий обнаруживать подключённое (напрямую или через устройства первого уровня) сетевое оборудование Cisco, его название, версию IOS и IP-адреса. Если

не отключить данный протокол, злоумышленник, сумев подключиться к одному из устройств, сможет получить информацию о всей сети.

– Использование протоколов AAA.

AAA (*Authentication Authorization and Accounting*) – система аутентификации авторизации и учета событий, встроенная в операционную систему Cisco IOS, служит для предоставления пользователям безопасного удаленного доступа к сетевому оборудованию Cisco. Она предлагает различные методы идентификации пользователя, авторизации, а также сбора и отправки информации на сервер [6].

Список используемых источников

1. Федеральный закон от 26 июля 2017 г. № 187-ФЗ «О безопасности критической информационной инфраструктуры Российской Федерации».

2. Официальный сайт Правительства Санкт-Петербурга [Электронный ресурс]. – Режим доступа: https://kis.gov.spb.ru/proekty/bezopasnyj-gorod/ (дата обращения 11.03.2020).

3. Холодницкая М. Как подключиться к серверу по протоколу SSH [Электронный ресурс]. – Режим доступа: https://hyperhost.ua/info (дата обращения 19.03.2020).

4. Семенов Ю. А. Сетевой протокол времени NTP [Электронный ресурс]. – Режим доступа: http://book.itep.ru/4/44/ntp_4415.htm (дата обращения 10.03.2020).

5. SysLog-протокол журналирования сообщений [Электронный ресурс]. – Режим доступа: https://catethysis.ru/syslog/ (дата обращения 19.03.2020).

6. Аутентификация в Cisco IOS [Электронный ресурс]. – Режим доступа: https://habr.com/ru/company/pt/blog/192668/ (дата обращения 16.03.2020).

УДК 004.72
ГРНТИ 49.33.29

АЛГОРИТМ ПРЕДВАРИТЕЛЬНОЙ ИДЕНТИФИКАЦИИ ПАРАМЕТРОВ МОДЕЛИ ЛОГИЧЕСКОГО КАНАЛА МУЛЬТИСЕРВИСНОЙ СЕТИ СВЯЗИ

А. Р. Краюшкин, О. В. Крюков, Д. В. Романов, И. В. Ульянов

Академия Федеральной службы охраны Российской Федерации

Рассмотрена проблема предварительной идентификации параметров модели логического канала мультисервисной сети связи, использующей ресурс оператора связи в условиях нестационарности измеренных значений показателей качества обслуживания.

мультисервисная сеть связи, логический канал, качество обслуживания (QoS), скрытая марковская модель.

Введение

Современный этап развития инфокоммуникационных систем, в том числе систем специального назначения, использующих технологию коммутации пакетов, характеризуется постоянно расширяющимся спектром предоставляемых услуг и повышением предъявляемых требований. В таких условиях развитие ведомственных мультисервисных сетей связи (МСС) затруднено без аренды ресурса операторов связи (ОС), например, MPLS VPN L2, VPN L3 и т. п. МСС строятся по принципу совместного использования, как собственных ресурсов, так и ресурсов, арендуемых у операторов связи. Наличие в структуре МСС арендованных сегментов приводит к снижению возможностей по наблюдению и управлению параметрами функционирования отдельных логических каналов (ЛК).

Модель ЛК МСС

Условие недостаточной наблюдаемости процесса функционирования ЛК МСС определяет необходимость использования математического аппарата теории скрытых Марковских моделей (СММ) при моделировании ЛК МСС.

В рамках модели ЛК МСС, использующей ресурс ОС [1], процесс функционирования ЛК МСС предлагается рассматривать как совокупность двух взаимосвязанных стохастических процессов: скрытый – процесс изменения состояний функционирования («норма», «деградация» или «отказ») и наблюдаемый – процесс генерации значений показателей качества обслуживания (QoS). Таким образом, ЛК МСС может быть описан как стохастическая динамическая система:

$$X_{t+1} = A_t X_t + V_{t+1}, \quad (1)$$

$$Y_{t+1} = C_t X_t + W_{t+1}, \quad (2)$$

где $X_t \in \mathbb{X} = \{x_1, \ldots, x_N\}$, $t \in \mathbb{T}$ – скрытый процесс; $A_t = (a_{ji}^t)$ – матрица вероятностей переходов между состояниями; $a_{ji}^t = P(X_{t+1} = x_j \mid X_t = x_i)$, $i, j = 1..N$ – вероятность перехода из состояния x_i в момент времени t в состояние x_j в момент $t+1$ в предположении, что процесс X_t можно описать цепью Маркова; N – количество состояний функционирования ЛК МСС; V_t – последовательность приращений мартингала (шум возбуждения);

$Y_t \in \mathbb{Y} = \{y_1,\dots,y_N\}$, $t \in \mathbb{T}$ – наблюдаемый процесс; $C_t = (c_{ji}^t)$ – матрица вероятностей генерации наблюдений; $c_{ji}^t = P(Y_{t+1} = y_j \mid X_t = x_i)$, $i = 1..N$, $j = 1..M$ – вероятность появления наблюдения y_j в момент времени $t+1$, если в момент времени t скрытый процесс находился в состоянии x_i; M – количество генерируемых наблюдений; W_t – независимая от V_t последовательность приращений мартингала (шум наблюдения).

Выражения (1) и (2) обуславливают принципиальную возможность получения общепринятых критериев наблюдаемости и управляемости [2, 3]. Однако такой подход требует создания алгоритма предварительной идентификации параметров модели ЛК МСС $\lambda_0 = \{A_0, C_0\}$, а именно определения матриц вероятностей перехода и наблюдения в начальный момент времени при условии знания $\{Y_{-T},\dots,Y_0\}$ – заранее измеренной последовательности показателей качества обслуживания длинны T и X_{-T} – состояния функционирования ЛК МСС в начальный момент времени $(t = -T)$.

Стоит отметить, что использование математического аппарата теории СММ для определения матриц A и C целесообразно в том случае, если выражения (1) и (2) предполагают, что скрытый и наблюдаемый процессы представлены в индикаторном виде. Например, для процесса X_t множество возможных состояний $\mathbb{X}$ определяется следующим образом:

$$x_n = (\theta_1(\dot{x}_n),\dots,\theta_N(\dot{x}_n))^T,\ n = 1..N,$$

где $\dot{x}_n$ – возможное состояние исходного процесса $\dot{X}_t \in \dot{\mathbb{X}} = \{\dot{x}_1 = \text{"норма"}, \dot{x}_2 = \text{"деградация"}, \dot{x}_3 = \text{"отказ"}\}$, $(\cdot)^T$ – оператор транспонирования; $\theta_i(\dot{x}_n)$ – индикаторная функция такая, что:

$$\theta_i(\dot{x}_n) = \begin{cases} 1, \text{если } n = i, \\ 0, \text{если } n \neq i; \end{cases} \quad i = 1..N.$$

Таким образом, состояниям $\dot{x}_1 = \text{"норма"}$, $\dot{x}_2 = \text{"деградация"}$, $\dot{x}_3 = \text{"отказ"}$ соответствуют состояния $x_1 = (1,0,0)^T$, $x_2 = (0,1,0)^T$, $x_3 = (0,0,1)^T$.

Идентификация параметров модели ЛК МСС

Задачу определения матриц вероятностей перехода и наблюдения в рамках СММ принято решать в два этапа [4, 5]: первый – оценка вспомогательных параметров J_t^{ij} – количество переходов из состояния x_i в состояние x_j (за время t), $\mathcal{T}_t^{ij}$ – количество переходов из состояния x_i при условии появлений наблюдения y_j, O_t^i – количество переходов в (из) состояния x_i; второй – решение оптимизационной задачи: поиск таких матриц A и C, для которых максимизируется $L(\lambda)$ – правдоподобие появления исследуемой последовательности наблюдений.

Оценка вспомогательных параметров модели может быть выполнена как с использованием общеизвестного алгоритма прямого-обратного хода Баума-Уэлча [4, 6], так и другими способами, например, с помощью рекурентных выражений [5]. Для решения оптимизационной задачи можно использовать: EM-алгоритм [7] или его разновидности, метод множителей Лагранжа, различные градиентные методы [4] и т. п.

Алгоритм Баума-Уэлча предполагает вычисление вспомогательных параметров с помощью переменных прямого и обратного хода, что предусматривает представление скрытого процесса в виде однородной цепи Маркова. Такой подход удобен в рамках предварительной идентификации параметров модели ЛК МСС, как самостоятельной задачи. Однако, если после предварительной идентификации параметры модели ЛК МСС предполагается уточнять, это влечет повторную идентификацию параметров модели, что требует значительных вычислительных и временных затрат (при больших T). Кроме того, анализ последовательностей измеренных значений показателей качества обслуживания различных ЛК МСС показывает, что они обладают стационарностью в рамках небольших временных интервалов [8]. Это существенно ограничивает использование предположения об однородности цепи Маркова, которой описывается процесс изменения состояния функционирования ЛК МСС.

В таком случае в рамках задачи идентификации параметров модели ЛК МСС целесообразно применять рекуррентные выражения для получения оценок вспомогательных параметров [5]:

$$p_t = \frac{q_t}{\langle q_t, 1_N \rangle},\ q_{t+1} = \sum\nolimits_{i=1}^{N} c_i(Y_{t+1}) \langle q_t, x_i \rangle a_i^t; \qquad (3)$$

$$J_t^{rs} = \frac{\langle \dot{J}_t^{rs}, 1_N \rangle}{\langle q_t, 1_N \rangle},\ \dot{J}_{t+1}^{rs} = \sum\nolimits_{i=1}^{N} c_i(Y_{t+1}) \langle \dot{J}_t^{rs}, x_i \rangle a_i^t + c_r(Y_{t+1}) \langle q_t, x_r \rangle a_{sr}^t x_s; \qquad (4)$$

$$\mathcal{T}_t^{rs} = \frac{\left\langle \dot{\mathcal{T}}_t^{rs}, 1_N \right\rangle}{\left\langle q_t, 1_N \right\rangle},\ \dot{\mathcal{T}}_{t+1}^{rs} = \sum\nolimits_{i=1}^{N} c_i(Y_{t+1}) \left\langle \dot{\mathcal{T}}_t^{rs}, x_i \right\rangle a_i^t + M \left\langle q_t, x_r \right\rangle \left\langle Y_{t+1}, y_s \right\rangle c_{sr}^t\, a_r^t; \quad (5)$$

$$O_t^r = \frac{\left\langle \dot{O}_t^r, 1_N \right\rangle}{\left\langle q_t, 1_N \right\rangle},\ \dot{O}_{t+1}^r = \sum\nolimits_{i=1}^{N} c_i(Y_{t+1}) \left\langle \dot{O}_t^r, x_i \right\rangle a_i^t + c_r(Y_{t+1}) \left\langle q_t, x_r \right\rangle a_r^t; \quad (6)$$

где: $p_t = (p_1^t, ..., p_N^t)^T$ – вектор оценки состояния процесса X_t, такой что $\sum\limits_{i=1}^{N} p_i^t = 1$; $q_t = (q_1^t, ..., q_N^t)^T$ – вектор ненормированной оценки состояния; $\left\langle q_t, x_i \right\rangle = q_t^T x_i$ – функционал [5], равный 1, если $q_t = x_i$, и 0 в противном случае; $c_i(Y_t) = M \prod_{j=1}^{M} (c_{ji}^t)^{Y_t^j}$; Y_t^j – элемент вектора наблюдений $Y_t = (Y_t^1, ..., Y_t^j, ..., Y_t^M)^T$; $1_N = (1, .., 1)^T$ – единичный вектор длины N; $a_i^t = A_t x_i = (a_{1i}^t, ... a_{Ni}^t)^T$ – вектор столбец из матрицы переходов; $\dot{J}_t^{ij}$, $\dot{\mathcal{T}}_t^{ij}$, $\dot{O}_t^i$ – ненормированные оценки вспомогательных параметров.

Ненормированные оценки в выражениях (3)–(6) получены в преобразованном вероятностном пространстве, переход к которому осуществим в предположении, что вероятностная мера P пространства $(\Omega, \mathcal{F}_t^{XY}, P)$ не имеет тождественных нулю значений [5]. Таким образом, можно обосновать существование производной Радона-Никодима:

$$\Lambda_t = \prod\nolimits_{l=1}^{t} \lambda_l = \overline{P} \Big/ P \Big|_{\mathcal{F}_t^{XY}}, \quad (7)$$

где $\bar{P}$ – новая вероятностная мера, построенная на $(\Omega, \mathcal{F}_t^{XY})$, для наблюдаемого процесса (2), таким образом, что наблюдения в вероятностном пространстве $(\Omega, \mathcal{F}_t^{XY}, \overline{P})$ становятся независимыми одинаково распределенными случайными величинами; $\mathcal{F}_t^{XY}$ – полная σ-алгебра подмножеств, порожденная последовательностями состояний $\{X_0, ..., X_t\}$ и наблюдений $\{Y_0, ..., Y_t\}$. Существование меры $\overline{P}$ следует из теоремы Колмогорова о продолжении меры.

Возвращение к исходной вероятностной мере осуществляется с помощью обратной к (7) функции:

$$\overline{\Lambda}_t = \prod\nolimits_{l=1}^{t} \overline{\lambda}_l = P \Big/ \overline{P} \Big|_{\mathcal{F}_t^{XY}}.$$

В левых частях выражений (3)–(6) такой переход осуществлен в рамках процедуры нормирования.

Таким образом, алгоритм предварительной идентификации параметров модели ЛК МСС можно записать с помощью следующей последовательности действий:

1. Получение последовательности наблюдений $\{Y_0,...,Y_T\}$.
2. Выбор X_0 – начального значения скрытого процесса.
3. Выбор $\lambda_0 = \{A_0, C_0\}$ – начальных значений параметров модели.
4. Вычисление $L(\lambda_0)$ [5].
5. Вычисление вспомогательных параметров J_t^{ij}, $\mathcal{T}_t^{ij}$, O_t^i.
6. Переоценка параметров модели $\bar{\lambda} = \{\bar{A}, \bar{C}\}$:

$$\bar{A} = (\bar{a}_{ji}),\ \bar{a}_{ji}(t) = \frac{\bar{\mathcal{T}}_t^{ij}}{\bar{O}_t^i} = \frac{\gamma_t(\mathcal{T}_t^{ij})}{\gamma_t(O_t^i)},\ i, j = 1..N;$$

$$\bar{C} = (\bar{c}_{ji}),\ \bar{c}_{ji}(t) = \frac{\bar{J}_t^{ij}}{\bar{O}_t^i} = \frac{\gamma_t(J_t^{ij})}{\gamma_t(O_t^i)},\ i = 1..N,\ j = 1..M.$$

7. Вычисление $L(\bar{\lambda})$. Сравнение с предыдущим значением функции правдоподобия. В случае равенства значений остановка алгоритма, иначе – переход к действию 5.

Заключение

Предложенный алгоритм идентификации параметров модели ЛК МСС позволяет выполнить предварительное обучение модели и применим для построения на его основе алгоритма идентификации, работающего в режиме реального времени в условиях нестационарности процесса генерации значений показателей QoS и неоднородности цепи Маркова, описывающей процесс изменения состояний функционирования ЛК.

Список используемых источников

1. Крюков О. В., Ульянов И. В. Модель логического канала мультисервисной сети связи, использующей ресурс оператора связи в условиях недостаточных наблюдаемости и управляемости // Информационные системы и технологии. 2019. № 3 (113). С. 97–104.

2. Терентьев В. М., Паращук И. Б. Теоретические основы управления сетями многоканальной радиосвязи. СПб. : Типография ВАС, 1995. 195 с.

3. Бударгин О. М., Мисриханов М. Ш., Рябченко В. Н. Новые эффективные критерии управляемости и наблюдаемости для систем большой размерности // Проблемы управления. 2012. № 1. С. 21–25.

4. Рабинер Л. Р. Скрытые марковские модели и их применение в избранных приложениях при распознавании речи: Обзор // ТИИЭР. 1989. Т. 77. № 2. С. 86–120.

5. Elliott, R. J. Aggoun, L. Moore, J. B. Hidden Markov Models : Estimation and Control. New York : Springer-Verlag, 1995. 382 p. ISBN 0-387-94364-1.

6. Baum, L. E. and Petrie, T. Statistical inference for probabilistic functions of finite state Markov chains // Annals of the Institute of Statistical Mathematics. 1966. N 37. PP. 1554–1563.

7. Dempster, A. P., Laird, N. M., Rubin, D. B. Maximum likelihood from incomplete data via the EM algorithm // Journal of the Royal Statistical Society of London. 1977. Series B 39. PP. 1–38.

8. Крюков О. В., Царев М. С. Модель логического канала транспортной сети с коммутацией пакетов // Телекоммуникации. 2018. № 5. С. 39–48.

УДК 621.39
ГРАНТИ 49.44.33

ИССЛЕДОВАНИЕ ВЛИЯНИЯ МНОГОВОЛНОВОЙ НАКАЧКИ НА СПЕКТР УСИЛЕНИЯ ОПТИЧЕСКИХ УСИЛИТЕЛЕЙ EDFA

В. С. Кузнецов, Д. С. Микутавичайте

Санкт-Петербургский государственный университет телекоммуникаций им. проф. М. А. Бонч-Бруевича

Одной из важнейших задач в области инфокоммуникаций является достижение достаточного для приема уровня выходного сигнала во всем спектральном диапазоне усиления оптических усилителей EDFA. Использование многоволновой накачки позволяет существенно снизить требования к источнику накачки оптического сигнала. В данной работе рассматривается использование нескольких источников излучения сигнала накачки с длинами волн, отличных от эффективной – 980 нм. В моделирующей программе рассмотрено влияние параметров усилителя с многоволновой накачкой на усиление входного оптического сигнала различной мощности. Полученные результаты могут быть использованы в качестве рекомендаций для разработчиков оптических усилителей и проектировщиков волоконно-оптической линии связи.

эрбиевые оптические усилители, спектральный диапазон, смещение, уплотнение каналов.

Оптические усилители EDFA (*Erbium Doped Fiber Amplifier*) работают в стандартном С-диапазоне, включающий длины волн от 1530 до 1560 нм, что позволяет использовать такие усилители на магистральных волоконно-оптических линиях связи с системами плотного спектрального мультиплексирования DWDM (*Dense Wavelenght Division Multiplexing*). Дальность передачи сигнала определяется прежде всего ослаблением сигнала за счет потери части энергии передаваемого сигнала при распространении его по волокну. Усилители с удаленной накачкой ROPA (*Remote Optically Pumped Amplifier*) широко применяются с использованием многоволновой накачки сигнала. Такие усилители позволяют подавать в усилительный

пункт более мощный суммарный сигнал накачки на длине волны близкой к 1480 нм. Однако для возможности использования оптических усилителей в обслуживаемых усилительных пунктах необходимо определить эффективность использования многоволновой накачки на длине волны 980 нм [1, 2].

Исследование проводилось для различных конфигураций оптического усилителя: с различным количеством источников сигнала накачки – 1, 2, 4, 8, 16, с различными уровнями мощности усиливаемого сигнала и сигнала накачки. Для всех моделируемых схем использовалось эрбиевое волокно I-4 длиной 10 м.

В структурную схему усилительного пункта входят источник сигнала с диапазоном длин волн 1500–1600 нм с частотным интервалом 200 ГГц, мультиплексор, позволяющий объединить усиливаемый сигнал и сигнал накачки. Сигнал накачки формируется путем мультиплексирования массива источников накачки (рис. 1).

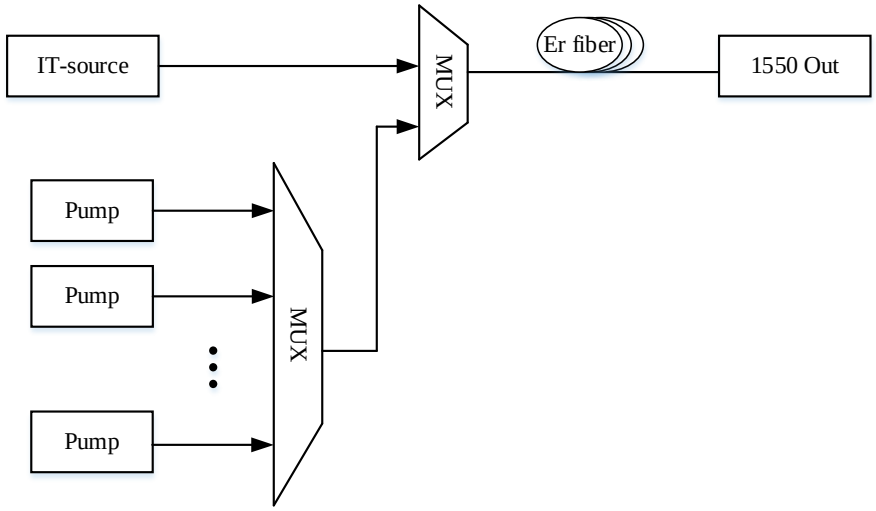


Рис. 1. Структурная схема исследуемого усилительного пункта с многоволновой накачкой

Прежде чем моделировать схему с большим количеством источников накачки, необходимо было определить эффективный интервал между длинами волн накачки. Для этого в моделирующей программе была исследована схема с 4-мя источниками накачки с различными наборами длин волн (табл., см. ниже).

В моделирующей схеме учитываются следующие параметры:

– способ включения накачки: попутный;
– мощность накачки: 11 (рис. 2, см. ниже), 17 дБм (рис. 3, см. ниже);
– уровень мощности входного сигнала: −20 дБм.

Как видно из результатов моделирования (рис. 2, рис. 3) набор длин волн источников накачки с различными уровнями мощности не влияет

на усиленный сигнал. В связи с этим дальнейшие исследования проводились с набором длин волн № 1.

ТАБЛИЦА. Наборы длин волн источников накачки (нм)

Набор 1	Набор 2	Набор 3	Набор 4	Набор 5	Набор 6
970	975	974	977	984	979
975	980	977	980	982	980
980	985	980	983	980	981
985	990	983	986	978	982

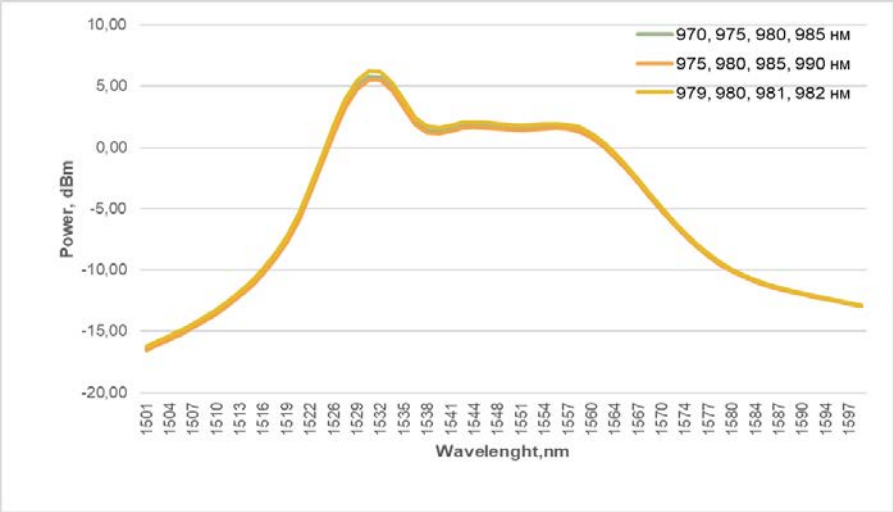


Рис. 2. Моделирование диапазона 1500–1600 нм с различными длинами волн накачки с уровнем мощности сигнала накачки 11 дБм

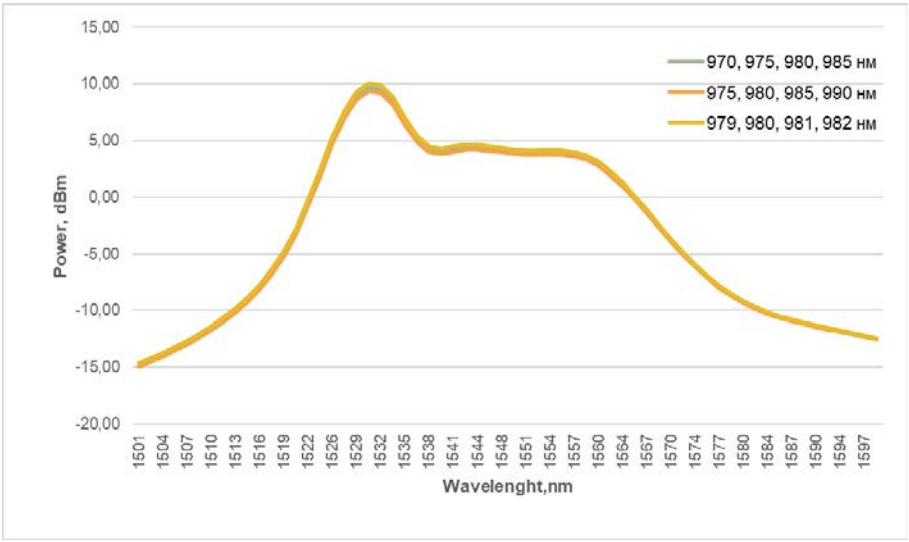


Рис. 3. Моделирование диапазона 1500–1600 нм с различными длинами волн накачки с уровнем мощности сигнала накачки 17 дБм

Прежде чем исследовать схему с большим количеством источников накачки, необходимо определить эффективность многоволновой накачки относительно схем моделирования с одним источником накачки сигнала. Для этой задачи в схеме моделирования с одним источником накачки зафиксирован уровень мощности накачки 14 дБм и поделен поровну для схемы с двумя источниками. Использование многоволновой накачки позволяет получить меньший уровень выходной мощности (рис. 4).

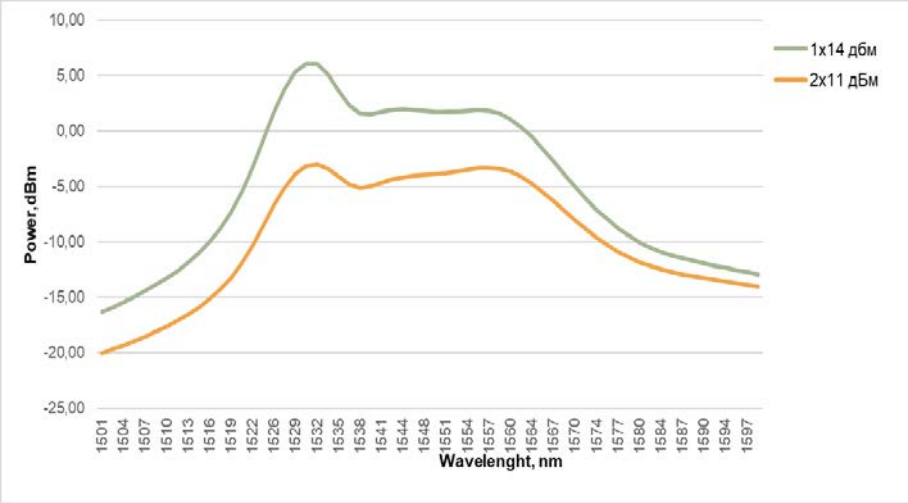


Рис. 4. Моделирование диапазона длин волн 1500–1600 нм с попутным включением сигнала накачки для 1-го источника накачки, мощностью 14 дБм и для 2-х источников накачки, мощность 11 дБм, с уровнем усиливаемого сигнала −20 дБм

Многоволновая накачка позволяет уменьшить мощность каждого источника накачки. При этом ширина спектра усиленного сигнала не изменяется (рис. 5).

Рис. 5. Моделирование диапазона длин волн 1500–1600 нм с попутным включением накачки для 1, 2, 4, 8, 16 источников с различной мощностью накачки и мощностью входного сигнала −20 дБм

Включение многоволновой накачки встречным образом также не оказывает существенного влияния по сравнению с попутным включением накачки на мощность и спектр усиленного сигнала.

Изменение уровня мощности усиливаемого сигнала (−10 и −30 дБм) также не дает преимуществ в использовании многоволновой накачки источников (рис. 6, рис. 7).

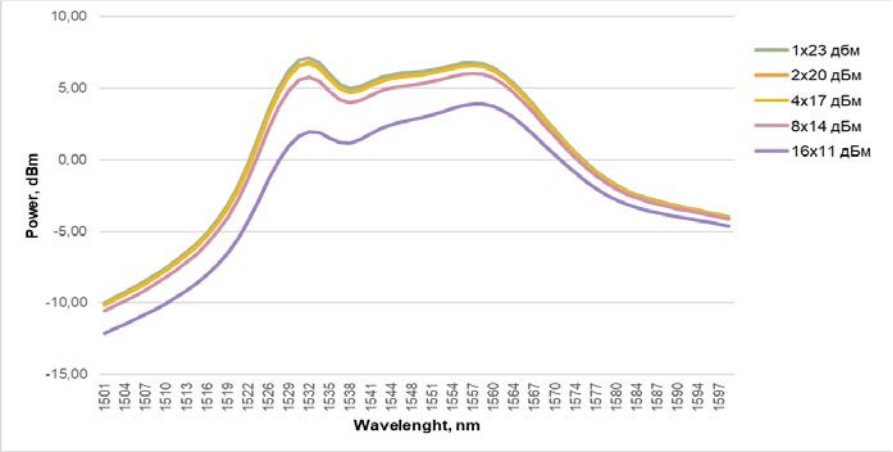


Рис. 6. Моделирование диапазона длин волн 1500–1600 нм с попутным включением сигнала накачки для 1, 2, 4, 8, 16 источников с различной мощностью накачки и уровнем мощности входного сигнала −10 дБм

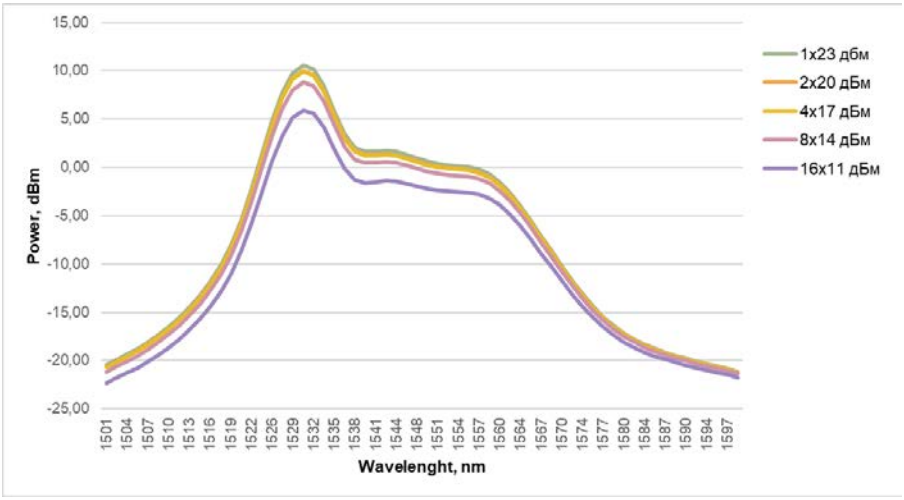


Рис. 7. Моделирование диапазона длин волн 1500–1600 нм с попутным включением сигнала накачки для 1, 2, 4, 8, 16 источников с различной мощностью накачки и уровнем мощности входного сигнала −30 дБм

Таким образом, многоволновая накачка в оптических усилителях EDFA на длине волны 980 нм не оказывает непосредственного влияния на спектр усиленного сигнала, позволяет уменьшить уровень мощности каждого из источников накачки, что приведет к повышению стабильности усилителя в обслуживаемых пунктах.

Список используемых источников

1. Листвин В. Н., Трещиков В. Н. DWDM системы: научное издание. М. : Издательский Дом «Наука», 2013. 300 с.

2. Гайнов В. В., Гуркин Н. В, Лукиных С. Н., Наний О. Е, Трещиков В. Н. Сверхдлинные однопролетные линии связи с удаленной накачкой оптических усилителей // Журнал технической физики. 2015. Т. 85. Вып. 4. С. 83–89.

Статья предоставлена заведующим кафедрой ФиЛС СПбГУТ, кандидатом технических наук, доцентом М. С. Былиной.

УДК 681.324
ГРНТИ 49.33.29

ОСОБЕННОСТИ ПОДХОДА К СОЗДАНИЮ ИНФОРМАЦИОННЫХ СИСТЕМ В ИНТЕРЕСАХ УПРАВЛЕНИЯ ТЕХНИЧЕСКИМ ОБЕСПЕЧЕНИЕМ СПЕЦИАЛЬНОГО НАЗНАЧЕНИЯ

Е. М. Кузнецов, О. И. Пантюхин, Г. А. Рябов, Б. В. Солодухин

Военная академия связи им. Маршала Советского Союза С. М. Будённого

Значительный прогресс в области программного обеспечения и средств вычислительной техники в настоящее время вызывает значительный рост размеров и сложности информационных систем, разрабатываемых, внедряемых и применяемых в различных областях деятельности организаций.

Особенностью разработки информационных систем специального назначения является не только необходимость строгого соблюдения государственных стандартов в области качества программного обеспечения и разработки систем специального назначения, но и зависимость структуры информационной системы от действующей структуры органов управления и их взаимодействия.

информационные системы, управление техническим обеспечением.

Одним из важных условий эффективного использования информационных технологий является внедрение определенных стандартов, которые собой определяют единые правила организации технологии или управления. При этом за основу таких ведомственных стандартов могут приниматься отраслевые, национальные и даже международные стандарты.

Динамика развития информационных технологий приводит к быстрому устареванию существующих стандартов и методик разработки инфор-

мационных систем. Так, в связи со значительным прогрессом в области программного обеспечения и средств вычислительной техники наблюдается рост размеров и сложности информационных систем. При этом существенно меняются требования как к основным функциям и сервисным возможностям систем, так и к динамике изменения этих функций. В этих условиях применение классических способов разработки и обеспечения качества информационных систем становится малоэффективным и не приводит к уровню качества, адекватному реальным требованиям.

Создание информационных систем в интересах управления техническим обеспечением специального назначения (ТО СН) в организациях и подразделениях силовых ведомств является вопросом, актуальность которого растет с каждым годом. Обусловлено это, в первую очередь, увеличением объемов обрабатываемой информации и сокращением времени цикла управления. Главной целью ТО СН является поддержание максимально возможной обеспеченности организаций работоспособными (исправными), готовыми к применению по назначению средствами техники специального назначения [1]. В свою очередь, внедрение информационных систем позволит повысить оперативность управления ТО и степень обоснованности принимаемых решений.

С целью достижения наибольшей эффективности информационная система должна быть реализована, в части касающейся, на всех уровнях управления с предоставлением соответствующим должностным лицам возможности реализации основных функций управления [2]:

прогнозирование (формирование цели);

принятие решения;

планирование;

оперативное управление (регулирование);

контроль;

учет.

Все функции управления ТО СН находятся в тесном взаимодействии и базируются на сведениях, основные источники которых можно условно разделить на следующие группы [2, 3]:

руководящие документы (ГОСТ, ОСТ, ведомственные приказы и руководства);

нормативно-справочных документация (техническая, справочная и иная);

показатели системы ТО СН (состав, наличие и производственные возможности органов технического обеспечения и др.);

сведения о материальных средствах (изделиях);

финансовые документы (первичные учётные документы и реестры учета);

документы по учету эксплуатации техники (формуляр, аппаратный журнал);

планирующие документы по техническому обеспечению (планы эксплуатации, восстановления и списания).

Поскольку данные составляют основу деятельности любой организации и являются наиболее стабильной её составляющей (функции и структура организации меняются гораздо чаще), то при построении ведомственных информационных систем наиболее адекватным решаемым задачам является подход к проектированию, основанный на данных [2, 4]. Такой подход обеспечивает наилучшее архитектурное решение при разбиении системы на приложения, а также простоту и согласованность при интеграции приложений. Таким образом, при создании информационной системы технического обеспечения специального назначения необходимо добиться:

выделения элементарных (неделимых) параметров (атрибутов), однозначно определяющих характеристики и свойства, как конкретного изделия, так и системы в целом;

реализации различных запросов с возможностью совершать среднесрочные и долгосрочные прогнозы;

обеспечение устойчивого функционирования и развития информационной системы.

Модульная структура функционирования информационной системы ТО СН (рис.), как вариант, может состоять из подсистем, объединённых в функциональные группы:

группа формирования данных об изделиях;

подсистема предоставления элементарных сведений;

группа формирования запросов и отчётов.

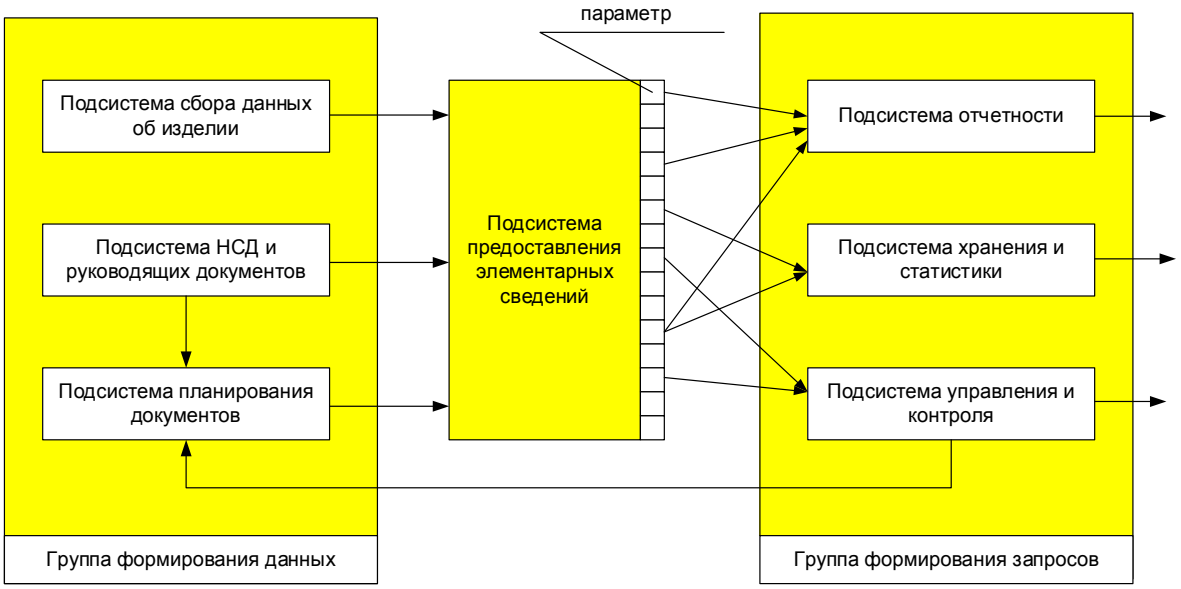


Рис. Формирование обобщённых сведений в системе ТО СН

Данное построение сможет обеспечить изменение практически любых разделов при сохранении целостности информационной системы ТО СН.

В настоящее время в организациях и подразделениях силовых ведомств назрела необходимость в создании таких, устойчивых и способных к дальнейшему развитию информационных систем, основанных на единых принципах и подходах для формирования объективной и актуальной информации о системе ТО СН, выполнении мероприятий технического обеспечения, техническом состоянии, как видов (групп) техники, так и каждой отдельно взятой единицы в отдельности.

Список используемых источников

1. Чихачев А. В., Третьяков С. М., Бурлаков А. А. и др. Техническое обеспечение связи и автоматизации. СПб. : ВАС, 2017. 302 с.

2. Анфилатов В. С., Авраменко В. С., Пантюхин О. И. Теоретические основы автоматизации управления войсками и связью. Часть 2. Основы построения и функционирования систем автоматизации управления войсками и связью: учебное пособие. СПб. : ВАС, 2015. 304 с.

3. Пантюхин О. И., Солодухин Б. В., Григорян В. М., Куликов В. А. Вопросы планирования мероприятий оперативно-технической службы на объектах автоматизации специального назначения. // Информационная безопасность регионов России (ИБРР-2017). Материалы юбилейной X СПб межрегиональной конференции. 1–3 нояб. 2017 г. СПОИСУ. СПб., 2017. С. 75–76.

4. Гвоздева Т. В., Баллод Б. А. Проектирование информационных систем: учеб. пособие. – Ростов н/Д : Феникс, 2009. – 508 с.

УДК 004.7
ГРНТИ 49.37.29

ТАКТИЛЬНЫЙ ИНТЕРНЕТ В СФЕРЕ ПРОМЫШЛЕННОСТИ

К. А. Кузнецов, А. С. А. Мутханна

Санкт-Петербургский государственный университет телекоммуникаций им. проф. М. А. Бонч-Бруевича

Тактильный Интернет в своем широком понимании представляет коммуникационные сети, позволяющие обеспечить управление в режиме реального времени, передавать касания, информацию с датчиков и актуаторов. Такие сети должны быть достаточно надежны, интеллектуальны и отзывчивы. В статье исследуется роль Тактильного Интернета в современных и будущих промышленных системах, которые позволят пересмотреть взгляды на существующие реализации и дадут возможность обезопасить человеческий труд, ускорить производство с ростом качества, сделать

обучение продуктивным, увлекательным и т. д. Огромное количество датчиков, информация с которых может собираться в реальном времени обеспечивают беспрецедентную точность принимаемых решений. Также дается представление о разработках 3GPP в области создания сверх надежных сетей и малым задержками – 5G/IMT2020.

тактильный Интернет, 5G, IIoT.

Введение

Беспроводные технологии стали неотъемлемой частью нашей жизни. Они позволяют стать свободным, в перемещениях, в количестве подключений, в образе мышление. Еще несколько лет назад, люди спускались в метро с длинными проводами, идущими от телефона до самых ушей, чтобы музыка сгладила ожидание своей станции. Сегодня этого кажется вовсе неудобно. Изменения касаются не только очевидных вещей, но и почти всех современных отраслей промышленности. Пятое поколение мобильных сетей, готово предоставить широкополосный доступ в интернет с сопоставимыми показателями с проводным доступом. В последние несколько лет беспроводные технологии сфокусировались на предоставление повсеместного доступа для машин и устройств, тем самым создавая Интернет вещей.

Раньше, беспроводные технологи использовали для передачи контента (голосовые звонки, короткие текстовые сообщения, передача файлов и т. д.), для мониторинга активностей приложений и сервисов. Появление Тактильного Интернета меняет это представление, теперь можно отправлять не только состояния объекта, но и его пространственные перемещения, изменения, преобразования в режиме реального времени. Рабочая группа IEEE P1918.1 определяет Тактильный Интернет как сеть или сеть, состоящую из множества других сетей, для удаленного доступа, манипулирования, управления или контролирования физических, виртуальных объектов или процессов в реальном времени.

Тактильный Интернет

В отличии от других понятий в этой области Тактильный Интернет нуждается в самых современных сетях передачи данных. Опираясь на их технологии, он позволит управлять, трогать, чувствовать актуальную информацию находясь на большом расстоянии от эпицентра генерации событий. Это позволит людям и машинам взаимодействовать между собой и окружающей их средой в реальном времени. В качества примера можно представить: такая система позволит вам обнять родного человека находясь на большом удалении от него.

Архитектуру Тактильного Интернета, как правило, разделяют на три основных домена – управляющий, сетевой и исполнительный. Схема взаимодействия изображена на рис. 1.

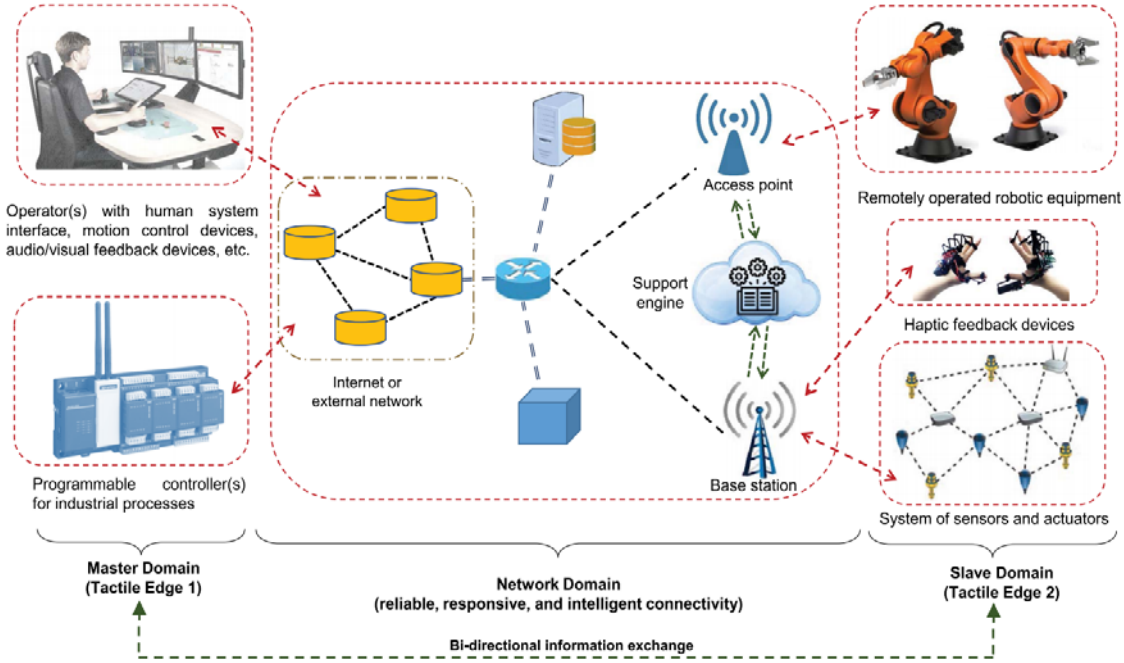


Рис. 1. Архитектура Тактильного Интернета

Основной принадлежностью домена управления является human system interface (HSI), что подразумевает взаимодействие человека и машины посредствам устройства управления визуальных, слуховых устройств обратной связи. Сетевой домен предоставляет возможности для двухстороннего обмена информаций, передачи тактильных ощущений и поддержки обратной связи. Домен исполнения характеризуется датчиками, актуаторами, роботами и т. д., что позволять собирать данные об окружающем пространстве и взаимодействовать с ним всеми возможными способами.

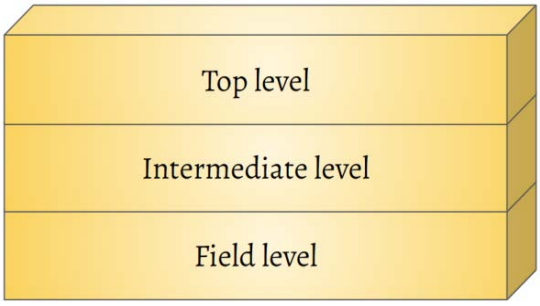


Рис. 2. Уровни промышленной сети

Промышленность стремительно развивается уже более 50 лет. Такому продолжительному росту несомненно способствует автоматизация, которая начиналась с простых, порой даже банальных задач и на сегодняшний день может достигает уровня принятий ответственных решений по управлению производственными линиями. Одним из ключей успеха в данной области стали промышленные сети, которые позволили улучшить взаимодействия интегрированность устройств, вывести на новый уровень ремонтопригодность, значительно эффективнее стал процесс поиска и устранения неисправностей. В отличии от корпоративных или частных сетей промышленные имеют иерархическую структуру, обычно разделяемую на три основных уровня (рис. 2). Основной уровень (*field level*) – включает в себя все конечные устройства такие как: датчики, сенсоры, актуаторы и прочее.

Промежуточный уровень (*intermediate level*) обеспечивает взаимодействие с контроллерами и управляющими устройствами. На контроллерах исполняются логические алгоритмы для принятия решений. Верхний уровень (*top level*) – это ЛВС, позволяющая контролировать и координировать, обладая оперативной информацией поступающих с основного уровня.

Эволюция промышленных систем может быть разделена на несколько основных этапов. Первый этап – это применение технологии fieldbus основанной на применении общей шины для поочередного, двухстороннего обмена информацией. Вторая технология базируется на индустриальном Ethernet, который позволил существенно увеличивать масштаб таких сетей, значительно возросли скорости передачи данных и, конечно, появились full-duplex взаимодействия. В последнем этапе появляются беспроводные технологии передачи данных для промышленности, увеличивая свободу перемещения устройств и упрощая процесс внедрения.

Появления технологии мобильной передачи данных пятого поколения должно заполнить потребность в передаче информации по беспроводным каналам в соответствии с концепцией IMT-2020. Такие сети поддерживают не только традиционные мобильные сервисы и услуги, но предоставляют совершенно новые возможности. 5G разделятся на три главных сегмента: улучшенная мобильная широкополосная связь (eMBB), массовые машинные взаимодействия (mMTC) и сверхнадежные сети с малыми задержками (URLLC). Основные требования фокусируются на обеспечении уровня круговой задержки, не превышающего 1 мс и степени надежности, достигающей 99,999 %.

New Radio – новая технология радиодоступа (NR), работающая в новых полосах спектра. 5G-NR обеспечивает унифицированный радиоинтерфейс, который будет гибко, масштабируемо и эффективно поддерживать различные требования различных вариантов использования. 5G-NR разработан с нативной поддержкой uRLLC. Далее будут рассмотрены некоторые из ключевых элементов дизайна, с точки зрения стека протоколов, 5G-NR, которые имеют решающее значение для uRLLC.

I. Масштабируемая нумерология физического уровня: ортогональное мультиплексирование с частотным разделением (OFDM) широко используется в большинстве современных широкополосных систем связи, включая современные сети LTE четвертого поколения (4G). 3GPP недавно согласился с тем, что семейство OFDM является правильным выбором для формирования сигнала 5G-NR. В частности, был принят OFDM с циклическим префиксом в нисходящей линии связи и OFDM с расширением DFT в восходящей линии связи. Это делает 5G первым поколением сотовой связи, которое не будет основано на совершенно новой форме сигнала и конструкции множественного доступа.

Для достижения низкой задержки порядка 1–2 мс бюджет передачи на физическом уровне ограничен 100–200 мкс, что означает, что каждый пакет должен быть меньше этой длительности. Однако, в LTE каждый символ OFDM имеет порядок 70 мкс, который основан на фиксированном разнесении поднесущих в 15 кГц. LTE поддерживает ширину полосы, несущей до 20 МГц [1]. С другой стороны, 5G-NR потенциально может работать в диапазоне частот с различной шириной полосы канала. Руководствуясь этими требованиями, 5G-NR принимает масштабируемую нумерологию OFDM (параметризацию формы сигнала) с масштабированием 2M разнесения поднесущих.

II. Гибкая структура кадра: фиксированная передача интервала времени (TTI) длительностью 1 мс, и время ожидания 8 мс при каждой повторной передаче в LTE приводят к сквозным задержкам, которые не подходят для uRLLC. Для достижения низкой задержки при поддержке сосуществования с приложениями eMBB и mMTC, 5G-NR принимает гибкую структуру кадра с динамической настройкой TTI на основе требований к обслуживанию. Концепция гибкой структуры кадра показывает мультиплексирование пользователя с различными TTI [2]. Наименьшая единица выделения – это «ресурсный фрагмент», который состоит из целого числа поднесущих и символов OFDM. В дополнение к динамически масштабируемому TTI, 5G-NR позволяет передачам с различными TTI начинаться на границах целочисленных символов вместо границы подкадра. Это дополнительно уменьшает задержку за счет исключения периода ожидания.

III. Сигнализация управления ресурсами: в стандарте LTE существует строгое временное разделение физического уровня управления и данных. Например, канал управления нисходящей линии связи передается по всей ширине полосы в первых символах OFDM TTI. Структура кадра 5G-NR предотвращает отображение каналов управления по всей полосе пропускания системы посредством управляющей сигнализации физического уровня в ресурсах, которая следует за соответствующей передачей данных для каждого отдельного пользователя. Канал управления в ресурсе отображается в начале распределения ресурсов для пользователя в первых символах времени по подмножеству частотных ресурсов. Такой канал управления позволяет использовать методы формирования луча и многоантенные системы для управления и передачи данных, что приводит к повышению надежности и производительности.

Заключение

Тактильный Интернет обеспечивает сдвиг парадигмы в сторону беспроводных технологий для обеспечений удаленного управления в реальном

времени. Такие возможности наиболее востребованы в области промышленности. Они позволяют создавать более гибкие и адаптивные производства в короткие сроки.

Список используемых источников

1. Zaidi A. A. et al. Waveform and numerology to support 5G services and requirements // IEEE Commun. Mag., vol. 54, no. 11, pp. 90–98, Nov. 2016.

2. Pedersen K. I., Berardinelli G., Frederiksen F., Mogensen P., and Szufarska A. A flexible 5G frame structure design // IEEE Commun. Mag., vol. 54 pp. 53–59, Mar. 2016.

УДК 550.34.013.2
ГРНТИ 50.41.25

АНАЛИЗ ПРИМЕНЕНИЯ ТРАССИРОВКИ ЛУЧЕЙ ДЛЯ ПРЕОБРАЗОВАНИЯ 3D ОБЪЕКТОВ В РАСТРОВОЕ ИЗОБРАЖЕНИЕ

Н. Ю. Ларионов, А. И. Ходанович

Санкт-Петербургский государственный университет телекоммуникаций им. проф. М. А. Бонч-Бруевича

Обоснована актуальность технологии трассировки лучей для преобразования 3D объектов в растровое изображение. Проанализированы перспективные направления развития технологий 3д визуализации объектов в форме растрового изображения, математическое обеспечение технологий 3д визуализации объектов в форме растрового изображения, определены недостатки и преимущества существующих методов, проведен анализ направления развития технологий 3д визуализации объектов в форме растрового изображения, проанализированы известные формализации для исследования технологий 3д визуализации объектов в форме растрового изображения.

трассировка лучей, визуализация, рендеринг.

3D-рендеринг – это процесс создания двухмерных изображений (например, для экрана компьютера) из 3D-модели. Изображения генерируются на основе наборов данных, определяющих цвет, текстуру и материал определенного объекта на изображении [1].

Рендеринг впервые появился в 1960 году, когда Уильям Феттер создал изображение пилота, чтобы смоделировать пространство, необходимое в кабине. Затем, в 1963 году, Иван Сазерленд создал Sketchpad, первую программу 3D-моделирования, в то время как в MIT. За свою новаторскую работу он известен как «Отец компьютерной графики».

В 1975 году исследователь Мартин Ньюэлл создал «Чайник Юты», трехмерную тестовую модель, которая стала стандартным тестовым рендером. Этот чайник, также называемый Newell Teapot, стал настолько знаковым, что его считают эквивалентом «Hello World» в области компьютерного программирования [2].

Как это работает

3D-рендеринг похож на фотографию. Например, программа рендеринга эффективно направляет камеру на объект для создания фотографии. Таким образом, цифровое освещение важно для создания детального и реалистичного рендера [3].

Со временем был разработан ряд различных методов рендеринга. Тем не менее, цель каждого рендера состоит в том, чтобы захватить изображение, основанное на том, как свет попадает на объекты, как в реальной жизни.

Техники рендеринга:

1) Растеризация – это один из самых ранних методов рендеринга, растеризация работает, рассматривая модель как сетку многоугольников. Эти полигоны имеют вершины, в которые встроена такая информация, как положение, текстура и цвет. Эти вершины затем проецируются на плоскость, перпендикулярную к перспективе (то есть камеру).

С вершинами, действующими как границы, оставшиеся пиксели заполнены правильными цветами. Представьте себе, что сначала нужно нарисовать контур для каждого цвета, который вы рисуете – это рендеринг с помощью растеризации.

Растеризация – это быстрая форма рендеринга. Она до сих пор широко используется, особенно для рендеринга в реальном времени (например, компьютерные игры, симуляторы и интерактивный графический интерфейс). Совсем недавно этот процесс был еще более усовершенствован благодаря более высокому разрешению и сглаживанию, который использовался для сглаживания краев объектов и смешивания их с окружающими пикселями.

2) Ray casting (метод бросания лучей). Несмотря на свою полезность, растеризация сталкивается с проблемами при наличии перекрывающихся объектов: если поверхности перекрываются, последняя нарисованная часть будет отражена при рендеринге, что приведет к отображению неправильного объекта. Чтобы решить эту проблему, была разработана концепция Z-буфера для растеризации. Это включает в себя датчик глубины, чтобы указать, какая поверхность находится под или над в конкретной точке зрения [4].

Это стало ненужным, однако, когда было разработано литье лучей. В отличие от растеризации, потенциальная проблема перекрывающихся поверхностей не возникает при литье лучей.

Приведение лучей, как следует из названия, направляет лучи на модель с точки зрения камеры. Лучи выводятся на каждый пиксель на плоскости изображения. Поверхность, на которую она попадает первой, будет показана при рендеринге, и любое другое пересечение после первой поверхности не будет отрисовано.

3) Трассировка лучей. Несмотря на преимущества, которые дает отливка лучей, в методике по-прежнему отсутствовала способность правильно моделировать тени, отражения и преломления. Таким образом, трассировка лучей была разработана [5].

Трассировка лучей работает аналогично приведению лучей, за исключением того, что она лучше отображает свет. По сути, первичные лучи с точки зрения камеры направляются на модели для получения вторичных лучей. После удара по модели будут испускаться теневые лучи, отраженные лучи или преломляющие лучи, в зависимости от свойств поверхности.

Тень генерируется на другой поверхности, если путь луча тени к источнику света затруднен этой поверхностью. Если поверхность является отражающей, результирующий отраженный луч будет излучаться под углом и освещать любую другую поверхность, на которую он попадает, что будет дополнительно излучать другой набор лучей. По этой причине этот метод также известен как рекурсивная трассировка лучей. Для прозрачной поверхности преломляющий луч испускается, когда на поверхность ударяет вторичный луч.

4) Техника уравнения. Дальнейшее развитие рендеринга в конечном итоге привело к уравнению рендеринга, которое пытается смоделировать, как свет излучается более точно в реальности. Техника считает, что свет испускается всем, а не только одним источником света. Это уравнение пытается рассмотреть все источники света в рендере, по сравнению с трассировкой лучей, которая использует только прямое освещение. Алгоритм, созданный с использованием этого уравнения, известен как глобальное освещение или косвенное освещение [6].

Аппаратные средства

Качество рендеринга улучшается, но процесс все еще медленный – поэтому крупные компании вкладывают значительные средства в рендерные фермы. В то же время отдельные дизайнеры и художники должны использовать современное оборудование.

Программное обеспечение рендеринга использует GPU, CPU или оба для создания рендеров. Кроме того, приложения рендеринга являются ресурсоемкими программами. Для более быстрого рендеринга часто требуются дополнительные обновления. Скорость процессора, интеграция и совместимость видеокарт, совместимость с драйверами и оперативной

памятью – вот некоторые из аспектов, обеспечивающих быстрое и качественное отображение.

Говоря о программном обеспечении рендеринга, если у вас мало вариантов, посмотрите этот огромный список приложений рендеринга, доступных сегодня.

Программное обеспечение

Как бы грустно это не звучало, идеального рендера не бывает. Это связано с тем, что постоянно находятся в равновесии несколько переменных, в том числе фотореализм, качество, скорость, размер данных и разрешение.

Несмотря на сложность, можно работать с этими основными факторами для получения фотореалистичных рендеров. Во-первых, модель должна быть скорректирована в правильной пропорции. Модель, масштабированная в реальной жизни, помогает. Измерения не обязательно должны быть точными, так как детали могут быть перенастроены, если они отображаются на визуализации.

Модельные материалы должны быть как подходящими, так и высокодетализированными для достижения реалистичных результатов. Случайные элементы в текстурах также помогают рендерам выглядеть более реалистично.

Интенсивность освещения, температура и расположение - это, конечно, огромный фактор. Правильное количество и расположение света облегчит детали, чтобы быть достаточно видимым. Также обратите внимание, что цветовая температура, если она не установлена правильно, может испортить ваш рендер.

Наконец, постобработка дает последние штрихи к вашему рендеру. Простые ретуши вашего необработанного рендера могут превратить ваши рендеры в захватывающее фотореалистичное изображение.

Трассировка лучей описывает метод получения визуальных изображений, созданных в трехмерных компьютерных графических средах, с большим количеством фотореализма, чем при использовании методов выпускания лучей или отрисовки линий сканирования. Отслеживается путь от камеры до каждого пикселя на экране и вычисляется цвет объекта, видимого через него.

Сцены с использованием метода трассировкой лучей, обычно описываются программистом, художником по. Сцены могут включать в себя различные источники освещения, карты, текстуры, сканы существующих объектов.

Каждый луч проверяется на пересечение с некоторыми объектами в созданной сцене. Ближайший объект идентифицируется и алгоритм оценивает отразившийся свет в точке пересечения, затем изучает свойства материала ближайшего объекта и объединит информацию для просчёта финального

цвета пикселя. Определенные материалы, отражающие поверхности или источники освещения, требуют больше лучей для просчёта в сцене.

Поскольку большая часть световых лучей от источника освещения не попадает прямо в камеру, «прямое» моделирование может потратить огромное времени на вычисления пути света, которые не регистрируются.

Следовательно, трассировка лучей предполагает, что данный луч пересекает рамку обзора. После максимального количества отражений или луча, проходящего определенное расстояние без пересечения, луч перестает перемещаться, и значение пикселя обновляется.

В наши дни, большинство программ, например, Blender, Maya используют трассировку лучей вместе с другими алгоритмами для генерации фотореалистичных изображений [5].

К сожалению, невозможно использовать метод трассировки лучей во всех случаях рендеринга по следующим причинам:

Самая простая трассировка лучей может создавать несколько миллионов лучей, которые нужно многократно вычислять. Даже для самых простых сцен с маленьким разрешение рендеринга будет выброшено несколько сотен тысяч лучей, что превращает этот процесс в сложный и ресурсоёмкий.

Вторая проблема состоит в том, что обычная трассировка лучей не является фотореалистичной, в ней не присутствует большое количество физических уравнений для просчёта математики эффектов, например, каустика. На данный момент, даже самый мощные настольные ПК не в состоянии потянуть честную трассировку лучей в реальном времени.

В результате, на сегодняшний момент, существует следующие технологии:

− CUDA, к ним относятся Octane Render, Mental Ray, Arion Render, Cycles и другие;

− FireStream;

− OpenCL, к ним относятся Cycles, Indigo Render, SmallLuxGPU;

− DirectCompute;

− шейдеры, к ним относится WebGL, это реализация алгоритма трассировки пути на шейдерах [8].

Octane Render

Это графический движок для рендеринга в реальном времени, созданный компанией Refractive Software, который использует CUDA и работает на всех видеокартах компании Nvidia. Этот движок использует метод трассировки лучей.

Проект был основан в Новой Зеландии. Компания OTOY занималась развитием проекта, программа была представлена публике в 2018 году. Octane Render является первым коммерчески доступным визуализатором

для работы только на видеокартах, который ещё и позволяет работать в реальном времени.

Плюсы:

− скорость при прямом освещении с помощью источников света;

− картинка в разрешении HD очищается за 5-10 секунд.

Минусы:

− отсутствует SSS;

− не работает каустика;

− неудобный встроенный редактор материалов, простые шейдеры.

Mental Ray

Профессиональная система фотореалистичного рендеринга, которая разработана компанией Mental Images. Это дочерняя компания Nvidia.

Mental Ray интегрирован с Softimage XSI, Houdini, Autodesk Maya, Autodesk 3ds Max, SolidWorks. Есть отдельное приложение с данным движком. Это довольно мощный инструмент визуализации, поддерживающий визуализацию по тайлам, рендеринг слоёв, окклюзию, тени.

Есть поддержка шейдеров на языке C++. Это отличает его от других рендер движков. В отличии от Octane, Mental Ray может рендерить каустику.

Минусы:

− отсутствии интерактивной визуализации при использовании одной GPU, при использовании нескольких GPU, Mental Ray может рендерить интерактивно;

− слишком примитивные шейдеры, подобные Octane Render.

Arion

Arion – это физически корректный движок рендеринга, разработанный RandomControl.

Версия: RandomControl – v2019.08.11

Существую разные ошибки, например, присутствует функция перемещения объекта, но точка, относительно которой этот объект вращается и перемещается, находится за пределами экрана, поэтому нет возможности посмотреть объект со всех сторон, камера постоянно пролетает мимо

При отсутствии освещения неба, не работают остальные источники освещения. Кроме того, Arion рендерит только CPU, что по современным меркам устарело.

Минусы:

− автофокус не работает;

− sss присутствует, но не работает;

− большое количество шума от каустики и других физических эффектов;

− множество ошибок и проблем в работе.

Cycles

Cycles – это движок рендеринга с отслеживанием путей, разработанный для того, чтобы быть интерактивным и простым в использовании, при этом поддерживая многие функции. Он был включен в Blender с 2011 года, с выпуском Blender 2.61.

Полностью бесплатный рендер, который встроен в Blender. Поддерживает технологии CUDA, OpenCL, также может рендерить и на GPU. Есть возможность просматривать результат прямо в окне сцены Блендера.

Есть поддержка нескольких графических процессоров. Их можно использовать для создания рендер фермы. К сожалению, на данный момент наличие нескольких графических процессоров не позволяет увеличить доступную память. Каждый графический процессор имеет возможность получить доступ только к своей памяти.

Минусы:

− сложный пользовательский интерфейс;
− примитивные шейдер;
− отсутствует физически корректное процедурное небо.

В результате анализа можно сделать вывод, что GPU рендеры еще не стали массово производиться и они имеют множество недостатков, но их успешность определена. Технология вычисления на GPU сильно увеличивает скорость рендеринга по сравнению с CPU рендерингом, позволяя получить физически корректное изображение в реальном времени.

Список используемых источников

1. Аксюхин А. А., Вицен А. А., Мекшенева Ж. В. Информационные технологии в образовании и науке // Современные наукоемкие технологии. 2009. № 11. С. 50–52.

2. Марчевский С. Распределённый рендеринг. Распределенный рендеринг и его особенности, 15.03.2013// Хабр. URL: https://habr.com/ru/post/172473/

3. Кормишин С. Что такое рендеринг? И что такое рендер, 25.04.2019 // CoreMission. URL: https://coremission.net/gamedev/chto-takoe-rendering/

4. How 3D Game Rendering Works, A Deeper Dive: Rasterization and Ray Tracing, Nikiforov Valentin, 2019, P. 2.

5. Wellner, P., Mackay, W. & Gold, R. Eds. Special issue on computer-augmented environments: back to the real world // Communications of the ACM, Vol. 36, Iss. 7 (Июль 1993), P. 34.

6. Гаврилов Н. И. Высокопроизводительная визуализация и морфологический анализ трехмерных данных в медицине и биологии : дисс. … канд. техн. наук, 05.13.17 / Гаврилов Николай Игоревич. Нижний Новгород, 2013. 168 с.

7. Афанасьев В. О. Системы 3D-визуализации индуцированной виртуальной среды : автореф. дисс. … докт. физ.-мат. наук, 05.13.11 / Афанасьев Валерий Олегович. М., 2007. 35 с.

8. Романовский А. М. Визуализация сцены при помощи систем рендеринга V-Ray и Corona Renderer // Творчество молодых: дизайн, реклама, информационные технологии: сб. тр. XIV Межд. науч.-практ. конф. студ. и асп. 2015. С. 117–120.

УДК 004.056
ГРНТИ 81.93.29

ПОСТРОЕНИЕ МОДЕЛИ АТАКУЮЩЕГО ДЛЯ СОВРЕМЕННОЙ КИБЕРФИЗИЧЕСКОЙ СИСТЕМЫ

Д. С. Левшун

Санкт-Петербургский институт информатики и автоматизации Российской академии наук

Стандартная модель атакующего предполагает классификацию злоумышленника по уровню его знаний, доступных ему ресурсов и типу доступа, который он имеет к атакуемой системе. Так, например, если оценить знания и доступные злоумышленнику ресурсы от 1 до 3, то 1 будет соответствовать минимальным ресурсам и поверхностным знаниям, в то время как 3 – почти неограниченным ресурсам и знаниям, достаточным для обнаружения и эксплуатации ранее неизвестных уязвимостей. Тип доступа от 1 до 5 показывает интерфейсы системы, доступные злоумышленнику: от (1) доступа к веб-сервисам через сеть интернет до (5) внутренних интерфейсов отдельных устройств. В рамках данной работы представлен подход к построению модели атакующего для современной киберфизической системы. Сформированная таким образом модель учитывает возможные намерения атакующего, в том числе нарушение конфиденциальности и целостности информации, а также нарушение доступности устройств и перехват управления ими. Таким образом, представленное решение позволит ответить не только на вопрос «кто атакует?», но и «зачем атакует?».

модель атакующего, киберфизическая система, атакующее действие, анализ намерений.

Модель атакующего позволяет выявлять перечень атакующих действий на инфраструктуру киберфизической системы и ее сервисы. Подобная модель позволяет описать атакующие действия, а также предполагать намерения злоумышленника. Более того, модель атакующего способствует оценке конкретных атакующих действий с точки зрения их выполнимости, в том числе на основе необходимы ресурсов. Модель нарушителя применима для проектирования механизмов защиты от различных классов атак, а также тестирования системы на предмет подверженности тем или иным угрозам информационной безопасности.

Основными нормативными документами, определяющими модель атакующего на территории Российской Федерации, являются:

1) Базовая модель угроз безопасности персональных данных при их обработке в информационных системах персональных данных (ФСТЭК России) [1].

2) Методика определения угроз безопасности информации в информационных системах (ФСТЭК России) [2].

3) Методические рекомендации по разработке нормативных правовых актов, определяющих угрозы безопасности персональных данных, актуальные при обработке персональных данных в информационных системах персональных данных, эксплуатируемых при осуществлении соответствующих видов деятельности (ФСБ России) [3].

В нормативном документе ФСТЭК России [1] атакующие подразделяются на внешних и внутренних. При этом внутренние атакующие подразделяются на восемь категорий в зависимости от способа доступа к персональным данных и имеющихся полномочий: от пользователей системы до её разработчиков и обслуживающего персонала.

В нормативном документе ФСТЭК России [2] вводится понятие потенциала атакующего, который может быть низким, средним и высоким. Нарушитель с низким потенциалом имеет возможность получить информацию об уязвимостях отдельных компонент информационной системы, опубликованную в общедоступных источниках. Нарушитель со средним потенциалом обладает всеми возможностями нарушителей с базовым потенциалом, а также имеет осведомленность о мерах защиты информации, применяемых в информационной системе данного типа. Нарушитель с высоким потенциалом обладает всеми возможностями нарушителей с низким и средним потенциалами, а также имеет возможность осуществлять несанкционированный доступ из выделенных сетей связи, к которым возможен физический доступ.

В нормативном документе ФСБ России [3] приводятся обобщенные возможности атакующих, при этом основное внимание уделяется атакам на криптографические средства и среду их функционирования. Возможности атакующего разграничены относительно доступа к контролируемой зоне: от возможности проведение атак только за пределами данной зоны до физического доступа к системе. А также по возможности привлечения специалистов различного уровня: анализ сигналов и побочного электромагнитного излучения, использование недокументированных возможностей программного обеспечения и т. д.

Помимо основных нормативных документов, существует ряд научно-исследовательских работ в области анализа угроз информационной безопасности и построения моделей атакующих. Так, в работах [4, 5] обосновывается необходимость и важность построения модели атакующего как элемента процесса проектирования и разработки защищенных

устройств на базе микроконтроллеров. В работе [6] рассматривается классификация атакующего на основе уровня его компетенции и знаний о его возможностях. В работе [7] предлагается разделить нарушителей на несколько групп в зависимости от уровня взаимодействия нарушителя с устройствами системы.

В работе [8] предложена модель атакующего, состоящая из следующих параметров: знаний атакующего, доступных ему технических ресурсов и его намерений. При этом выделяется несколько типов атакующих: от скрипт-кидди до кибератвиста. Скрипт-кидди – неопытный и неквалифицированный атакующий, использующий общеизвестные инструменты и уязвимости. Его намерения в основном связаны с получением репутации. Кибератвист же имеет самый высокий уровень знаний и ресурсов, в то время как его намерения связаны с политикой.

В работе [9] предлагается оценивать намерения атакующего на основе времени и ресурсов, необходимых ему для успешной реализации атакующего действия. В работе [10] предлагается характеризовать намерения атакующего на основе атакующих действий: получение root или пользовательских привилегий; вызов отказа в обслуживании; нарушение целостности, конфиденциальности или доступности данных.

Таким образом, процесс построения модели атакующего для современной киберфизической системы можно условно разделить на следующие этапы:

1) Формирование классификации атакующего по уровню его компетентности.

2) Формирование классификации атакующего по уровню его знаний об объекте атаки и его инфраструктуре.

3) Формирование классификации атакующего по уровню его доступа к объекту атаки и его инфраструктуре.

5) Формирование списка атакующих действий и взаимосвязи отдельных атак с возможностью их выполнения атакующим в соответствии с классификациями из п. 1, 2 и 3.

6) Формирование механизма учета ресурсов, которые необходимо затратить на выполнение различных атакующих действий из п. 4, а также механизма оценки ресурсов, доступных атакующему в соответствии с классификациями из п. 1, 2 и 3.

7) Формирование классификации намерений атакующего в зависимости от выполняемых атакующих действий, уровня его компетентности, знаний и доступа, а также затрачиваемых ресурсов.

Сформированная таким образом модель атакующего позволит учесть его намерения, в том числе связанные с различными атакующими действиями, финансовой выгодой, желанием получить репутацию в преступном мире, политическими событиями.

Исследование выполнено при финансовой поддержке РФФИ в рамках научного проекта № 19-17-50205.

Список используемых источников

1. Базовая модель угроз безопасности персональных данных при их обработке в информационных системах персональных данных (выписка) // Федеральная служба по техническому и экспортному контролю (ФСТЭК России), утв. 15 февраля 2008 года. 69 с. URL: https://fstec.ru/tekhnicheskaya-zashchita-informatsii/dokumenty/114-spetsialnye-normativnye-dokumenty/379-bazovaya-model-ugroz-bezopasnosti-personalnykh-dannykh-pri-ikh-obrabotke-v-informatsionnykh-sistemakh-personalnykh-dannykh-vypiska-fstek-rossii-2008-god

2. Методика определения угроз безопасности информации в информационных системах (проект) // Федеральная служба по техническому и экспортному контролю (ФСТЭК России). 2015 г. 43 с. URL: https://fstec.ru/component/attachments/download/812

3. Методические рекомендации по разработке нормативных правовых актов, определяющих угрозы безопасности персональных данных, актуальные при обработке персональных данных в информационных системах персональных данных, эксплуатируемых при осуществлении соответствующих видов деятельности // Федеральная служба безопасности (ФСБ России), утв. 31.03.2015 № 149/7/2/6-432. 22 с. URL: http://www.fsb.ru/files/PDF/Metodicheskie_recomendacii.pdf

4. Howard M. Secure systems begin with knowing your threats [Электронный ресурс] // 2004. – URL: https://bit.ly/39vSxAs. 2000 (дата обращения 31.03.2020).

5. Kocher P., Lee R., Mcgraw G., Ravi S. Security as a new dimension in embedded system design // Proceedings of the 41st Design Automation Conference (DAC ’04). – PP. 753–760. – 2004.

6. Abraham D. G., Dolan G. M., Double G. P., Stevens J. V. Transaction security system // IBM Systems Journal. 1991. No 30 (2). PP. 206–228.

7. Rae A. J., Wildman L. P. A Taxonomy of Attacks on Secure Devices // Department of Information Technology and Electrical Engineering. Australia : University of Queensland, 2003. – PP. 251–264.

8. Orojloo, H.; Abdollahi Azgomi, M. Predicting the behavior of attackers and the consequences of attacks against cyber-physical systems // Secur. Commun. Netw. 2016, 9, 6111–6136.

9. Fraunholz, D.; Krohmer, D.; Duque Antón, S.; Schotten, H. D. YAAS – On the Attribution of Honeypot Data // Int. J. Cyber Situat. Aware. 2017, 2, 31–48.

10. Aliyev V. Using honeypots to study skill level of attackers based on the exploited vulnerabilities in the network. – 2010. Master of Science Thesis in the Master Degree Programme, Secure and Dependable Computer Systems.

Статья представлена заведующим кафедрой ЗСС СПбГУТ, кандидатом технических наук, доцентом А. В. Красовым.

УДК 004.7
ГРНТИ 50.41.23

АНАЛИЗ ВОЗМОЖНОСТЕЙ НАРУШИТЕЛЯ ПО КОНТРОЛЮ ТРАФИКА В ИНФОТЕЛЕКОММУНИКАЦИОННОЙ СЕТИ

О. М. Лепешкин, А. С. Пермяков, А. С. Шуравин

Военная академия связи им. Маршала Советского Союза С. М. Буденного

В статье представлена сравнительная характеристика программных средств, предназначенных для перехвата и анализа трафика в телекоммуникационной сети. Сделан акцент на архитектурных особенностях инструментов, проанализированы их основные достоинства и недостатки с точки зрения функциональности. Также выполнен анализ возможностей по извлечению маршрутной информации из трафика нарушителем. Сформулированы рекомендации по снижению доступности информации, позволяющей вскрыть структуру инфотелекоммуникационной сети.

анализ трафика, телекоммуникационная сеть, сниффер, перехват трафика.

В настоящее время во ФСТЭК России в стадии обсуждения находится проект нового методического документа, касающегося «Методики моделирования угроз безопасности информации». Новый алгоритм моделирования угроз разработан на основании лучших мировых практик. Согласно документа, угроза информационной безопасности не реализуется в одно действие, а представляет собой цепочку из нескольких этапов. При этом первым из них является сбор данных, необходимых для реализации угрозы, о системах и сетях [1, 2].

Данный этап также называется предварительной разведкой, являющейся составной частью компьютерной разведки (КР). Ее задачей является получение сведений об автоматизированной системе обработки данных противника, то есть об информационно-телекоммуникационной сети (ИТКС). Целью предварительной разведки является сбор данных, необходимых для последующего проникновения в сеть.

Такими данными являются [3]:

- сетевая топология внутренней сети и ИТКС в целом;
- сведения об активности абонентов сети;
- тип и версия операционной системы атакуемых узлов;
- сведения о доступных сетевых и иных сервисах;
- сведения об установленном антивирусном обеспечении;
- личная информация пользователя, его адресная книга, сообщения;

– история посещения ресурсов в глобальной сети.

Перехват данных для последующего анализа осуществляется с помощью программ-шпионов или при помощи сетевых анализаторов трафика. Шпионские программы способны записывать всю передаваемую по сети информацию с конкретной рабочей станции или устройства.

Схема реализации воздействия «контроль сетевого трафика» представлена на рис. 1.

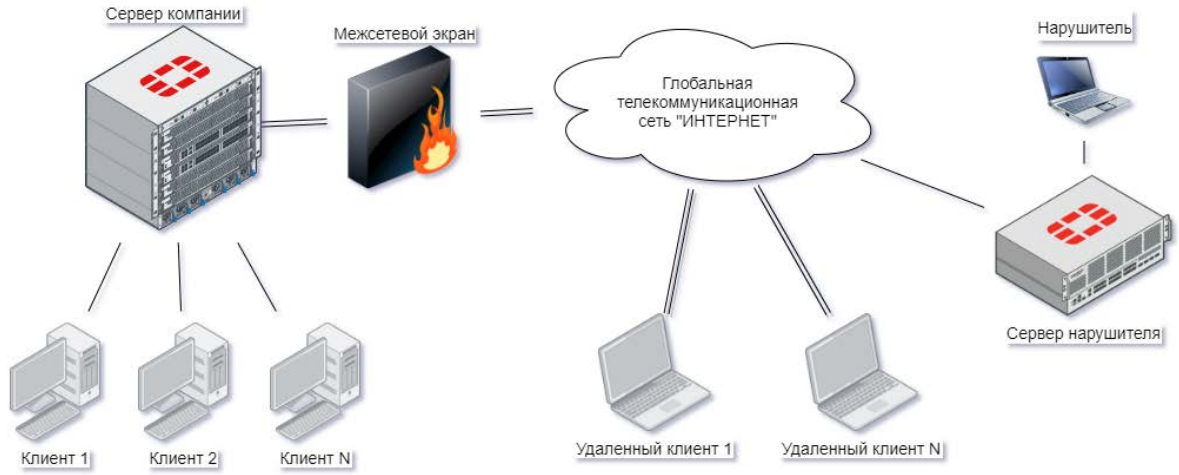


Рис. 1. Схема реализации воздействия «Контроль сетевого трафика»

Анализаторы трафика (снифферы) – это программные средства, предназначенные для перехвата и анализа сетевого трафика. Они могут быть установлены на маршрутизаторе или на конечном узле. Сниффер в сети, работающей по протоколу TCP/IP, подразумевает захват, декодирование, исследование и интерпретацию данных, передающихся в пакетах.

Пакет TCP/IP содержит данные, необходимые для соединения двух сетевых интерфейсов. Это поля с информацией об IP-адресах отправителя и получателя, номерах портов, номере пакета и типе протокола. Каждое из этих полей является необходимым для функционирования различных уровней сетевого стека и особенно приложений, работающих на верхнем уровне модели OSI и занимающихся обработкой данных.

Назначением протокола TCP/IP является проверка формирования пакета, добавления его в Ethernet-фрейм и доставки от отправителя к получателю по сети. Данный протокол не имеет механизмов для контроля безопасности данных. Данные, которые может получить нарушитель путем перехвата и анализа трафика, представлены на рис. 2 (см. ниже).

Технологии перехвата трафика с помощью снифферов различны. Наиболее распространенными способами являются [4]:

– прослушивание сетевого интерфейса в обычном режиме;

– подключение устройства перехвата в разрыв канала связи (атака «человек посередине» или «man-in-the-middle»);

– выполнение перенаправления трафика на сниффер путем проведения атаки (например, путем подмены IP адреса пользователя злоумышленником);

– анализ побочных электромагнитных излучений и наводок;

– создание ложных запросов ARP;

– выполнение атаки на уровень канала и сети, приводящей к изменению сетевых маршрутов.

Анализаторы трафика имеют следующие функциональные возможности:

– поддержка протоколов канального уровня, а также физических интерфейсов;

– определение, разбор и декодирование протоколов;

– командный или графический пользовательский интерфейс;

– анализ и просмотр трафика в реальном масштабе времени, а также накопление данных и доступ к статистике.

Рис. 2. Перехват данных по уровням модели OSI

По данным портала Hack Tools существует более ста анализаторов сетевого трафика, предназначенных для различных целей. Среди них можно выделить следующие: HTTP снифферы, антиснифферы, принт-снифферы, анализаторы протоколов, снифферы IM систем (ICQ и др), парольные снифферы, снифферы беспроводных сетей, пакетные снифферы.

В общем, существует два основных направления развития программного обеспечения для анализа сетевого трафика [4]:

1) рост «глубины» анализа для отдельного сетевого пакета, то есть увеличение уровня модели OSI, данные которого подвергаются анализу;

2) полнота учёта состояния потока, к которому относится пакет, а также других потоков, связанных с данным.

С точки зрения глубины, выделяют программные продукты поверхностного анализа пакетов, среднего анализа и глубокого анализа.

Поверхностный анализ основывающаяся исключительно на заголовках пакета первых трех уровней L1–L3 по модели OSI (см. рис. 2).

Средний анализ пакетов основывается на инспектировании сессий и сеансов связи, инициированных приложением, но устанавливаемых шлюзом

посредником. В рамках данной технологии содержимое пакетов анализируется частично и по предопределенным правилам. Не используются сложные методы анализа типа сигнатурного. Устройства, реализующие данный функционал размещаются между провайдером интернета и конечным пользователем. При среднем анализе заголовки разбираются вплоть до транспортного уровня.

Глубокий анализ трафика подразумевает такие действия над пакетами, как модификация, фильтрация или перенаправление. В рамках данного подхода анализатор трафика просматривает содержимое каждого пакета полностью.

При этом отметим, что в зависимости от целей применения глубокого анализа трафика, классификация может выполняться с различной точностью:

– тип протокола или приложения (например, Web, P2P, VoIP);

– конкретный протокол уровня приложения (HTTP, *BitTorrent*, SIP);

– приложение, использующее протокол (*Google Chrome, µTorrent, Skype*).

Вторым направлением развития технологии анализа можно назвать учет состояния протокола (потока) в процессе анализа (*stateless/statefu*l анализ). Данное направление актуально только для протоколов, использующих транспортный протокол с установлением соединения (*connection-oriented*).

Среди конкретных программных продуктов, используемых для анализа трафика, выделим несколько наиболее популярных:

1. Malcolm – программа с открытым исходным кодом для анализа сетевого трафика и визуализации. Принимает данные о сетевом трафике в форме дампов (файлов PCAP) и логов Zeek. Объединяет возможности других распространенных инструментов, таких как: Zeek, Moloch, Elasticsearch, Logstash, Filebeat, Kibana, ClamAV, Docker и т.д. Также имеет встроенную поддержку промышленных протоколов за счет парсеров Zeek.

2. ThreatEye – открытая, масштабируемая AIOps-платформа (*artificial intelligence for IT operations* – искусственный интеллект для IT-операций). Данная программа объединяет машинное обучение, полный захват сетевых пакетов и визуализацию.

3. Gurucul Network Behavior Analytics – программный продукт для анализа сетевого трафика, обладающий возможностями технологии машинного обучения. Данная программа способна обеспечить гибкое моделирование сущностей для мониторинга и выявления аномальной или опасной активности каждой из них. Среди сущностей могут быть: рабочие станции, сервера и межсетевые экраны, устройства интернета вещей и другие.

4. NetworkMiner – пассивный сетевой анализатор, позволяющий исследовать перехваченные данные. Программа выполняет анализ дампа с трафи-

ком, при этом способна безошибочно определить участников обмена сетевыми данными, распознать установленные на рабочих местах и серверах операционные системы по размеру окна, времени жизни пакета и уникальному набору флагов. Также она позволяет выдавать структурированную информацию об открытых сессиях, активных портах и прочей инфраструктуре сети, снимает баннеры различных демонов. Среди ключевых особенностей данного сниффера необходимо выделить возможность извлечения файлов и сертификатов, передаваемых по сети, а также пользовательских «логинов и паролей» (поддерживает протоколы FTP, HTTP и SMB).

5. Wireshark – анализатор сетевых протоколов, позволяющий сохранять и в интерактивном режиме просматривать содержание сетевых фреймов. Поддерживает большое количество протоколов (DNS, FDDI, FTP, HTTP, ICQ, IPV6, IPX, IRC, MAPI, MOUNT, NETBIOS, NFS, NNTP, POP, PPP, TCP, TELNET, X25 и т. д.), а также форматов файлов для записи дампа (*tcpdump, Sniffer Pro, NetXray, MS Network Monitor, Novell's LanAlyzer* и т. п).

6. Tcpdump – основной инструмент сбора сетевого трафика, Имеет интерфейс командной строки, а также очень сложный и богатый язык фильтрации.

Среди большого разнообразия анализаторов трафика практически всегда можно подобрать тот, который справится с поставленной задачей наилучшим образом. Это будет либо узкоспециализированное решение, либо универсальное с тонко настроенным фильтром [5]. Перехват всей совокупности циркулирующих в сети пакетов целесообразен при наличии мощных программных средств, позволяющих анализировать большие объемы данных, в том числе использующие технологии машинного обучения.

Для защиты пакетов, передаваемых по сети, от нарушителя, может быть использована технология создания виртуальных частных сетей. Одним из наиболее популярных и надежных решений в данной области является набор протоколов IPSec. Он позволяет производить инкапсуляцию и шифрование данных при передаче по сети, и при этом поддерживается современными маршрутизаторами, межсетевыми экранами и другими компонентами сетей. Практически все операционные системы поддерживают IPSec. Данная технология была создана для IPv6, но в настоящее время также портирована и для IPv4.

Список используемых источников

1. Пермяков А. С., Сташко Я. С. Вопросы повышения защищенности информационно-телекоммуникационной сети на основе интеллектуализации // Нейрокомпьютеры и их применение. XVIII Всероссийская научная конференция : тезисы докладов. 2020. С. 226–227.

2. Худайназаров Ю. К., Пермяков А. С., Лепешкин Е. О. Задачи системы интеллектуального мониторинга информационной безопасности инфотелекоммуникационной

сети // Нейрокомпьютеры и их применение. XVIII Всероссийская научная конференция : тезисы докладов. 2020. С. 198–200.

3. Карпов А. В., Лепешкин О. М., Новиков П. А., Шостак Р. К. Способ сетевого мониторинга объектов и систем связи // Актуальные проблемы инфотелекоммуникаций в науке и образовании (АПИНО 2018). VII Международная научно-техническая и научно-методическая конференция : сб. науч. ст. в 4-х т. 2018. С. 442–445.

4. Шостак Р. К., Лепешкин О. М., Новиков П. А., Худайназаров Ю. К. Концептуальное описание модели системы сетевого мониторинга систем связи специального назначения, реализованной в среде радикалов // Вопросы оборонной техники. Серия 16: Технические средства противодействия терроризму. 2018. № 5–6 (119–120). С. 66–73.

5. Лепешкин О. М., Лепешкин М. О., Бурлов В. Г. Синтез модели процесса управления техническими системами на основе теории радикалов // Нейрокомпьютеры и их применение : тезисы докладов / Под ред. А. И. Галушкина, А. В. Чечкина, Л. С. Куравского, С. Л. Артеменкова, Г. А. Юрьева, П. А. Мармалюка, А. В. Горбатова, С. Д. Кулика. 2016. С. 18-В.

УДК 004.421
ГРНТИ 49.33.29

МОДЕЛЬ ДЛЯ ОЦЕНКИ НАДЕЖНОСТИ ФУНКЦИОНИРОВАНИЯ СЕТИ ТАКТОВОЙ СЕТЕВОЙ СИНХРОНИЗАЦИИ

М. В. Лобастова, А. Ю. Матюхин

Санкт-Петербургский государственный университет телекоммуникаций им. проф. М. А. Бонч-Бруевича

Развитие современных цифровых систем передачи невозможно представить без грамотно организованной сети тактовой сетевой синхронизации, основной задачей которой является согласованная работа элементов сети. Одним из показателей работы данной сети является ее надежность. Для оценки надежности сети рассматривается ее модель, которая отражает основные режимы работы сети тактовой синхронизации, и может быть применена к источнику сигнала синхронизации любого уровня. Кроме того, рассматривается оценка показателей надежности сети. Рассматриваемые методы основаны на теории матриц, теории графов, теории вероятности, теории надежности.

тактовая сетевая синхронизация, надежность сети, режимы работы сети синхронизации, теория матриц, теория графов.

Сегодня проблема надежности телекоммуникационной сети является крайне актуальной. Так предполагается, что сети 5G будут работать с очень высоким коэффициентом готовности, в перспективе возможен рост требований к надежности сети. Однако, надежность сети связи во многом зависит

от работы тактовой сетевой синхронизации, как одной из важнейших ее компонент. Возникновение отказов в сети тактовой сетевой синхронизации может привести к существенному ухудшению качества предоставления услуг связи вплоть до отказа сети.

Согласно классификации, телекоммуникационные системы по уровню надежности можно разделить на:

– обычную (*Conventional*) с коэффициентом надежности 0,99;

– высокой надежности (*Highavailability*) с коэффициентом надежности 0,999;

– отказоустойчивую (*FaultResilient*) с коэффициентом надежности 0,9999;

– безотказную (*Faulttolerant*) с коэффициентом надежности 0,99999 [1].

Разработка математической модели направлена на количественную оценку надежности сети и оценку эффективности ее функционирования.

Математические модели надежности сети – это вероятностные характеристики. Так коэффициент аппаратной готовности сети синхронизации можно вычислить по формуле:

$$K_{\text{гот}} = \prod_{i=1}^{H} P_{Ti},$$

где H – количество узлов в сети синхронизации, P_{Ti} – вероятность того, что i-й узел сети находится в рабочем состоянии.

Сеть тактовой сетевой синхронизации имеет сложную иерархическую структуру. Главным источником сигнала синхронизации является первичный задающий генератор, формирующий сигнал синхронизации с высокой точностью. От него сигнал передается вторичным генераторам, а от них – генераторам узлов или, как их еще называют, генераторам сетевых элементов. Согласно требованиям, предъявляемым к сети синхронизации, она должна иметь древовидную структуру без петель и с числом переприемов сигнала синхронизации между вторичными задающими генераторами не более двадцати (рис. 1, см. ниже). Дополнительным требованием является наличие резервного источника сигнала синхронизации для каждого узла. Поддержание иерархии необходимо для получения наилучших рабочих характеристик сети.

При такой сложной структуре сети важно, чтобы каждый из ее элементов работал надежно. Основными элементами сети тактовой сетевой синхронизации являются генераторы. Поэтому необходимо знать, в каких состояниях может находится генератор узла, а также знать вероятности перехода из одного состояния в другое.

Математическим аппаратом, позволяющим оценить возможные переходы из одного состояния в другое, зная вероятности наступления того или иного события является полумарковский процесс [2].

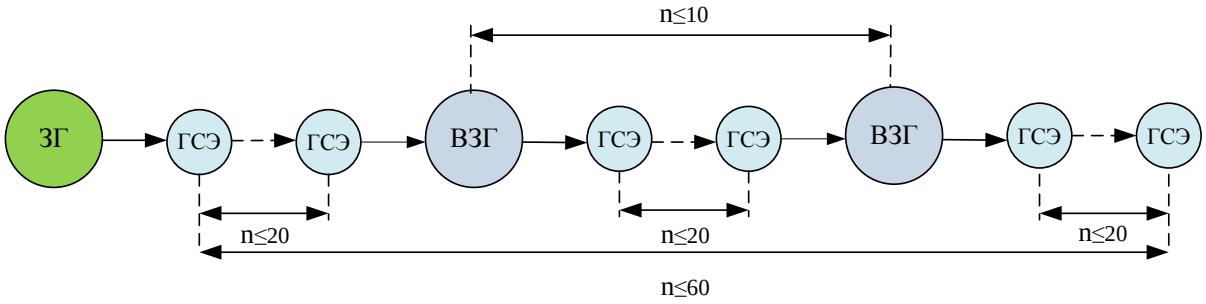


Рис. 1. Структура сети тактовой сетевой синхронизации

Важно, что полумарковский процесс – это процесс, который переходит из одного состояния в другое в соответствии с заданными распределениями вероятностей, а время пребывания процесса в каком-либо состоянии является случайной величиной, распределение которой зависит как от этого состояния, так и от состояния, в которое будет осуществлен следующий переход процесса. Будем использовать полумарковские процессы для описания состояния одного из узлов сети.

Модель полумарковского процесса для элемента сети тактовой сетевой синхронизации описывают ориентированным графом, вершинами которого являются возможные состояния s_k, в которых может находиться элемент, а ребрами – вероятности перехода из одного состояния в другое p_{ij} (рис. 2) [3].

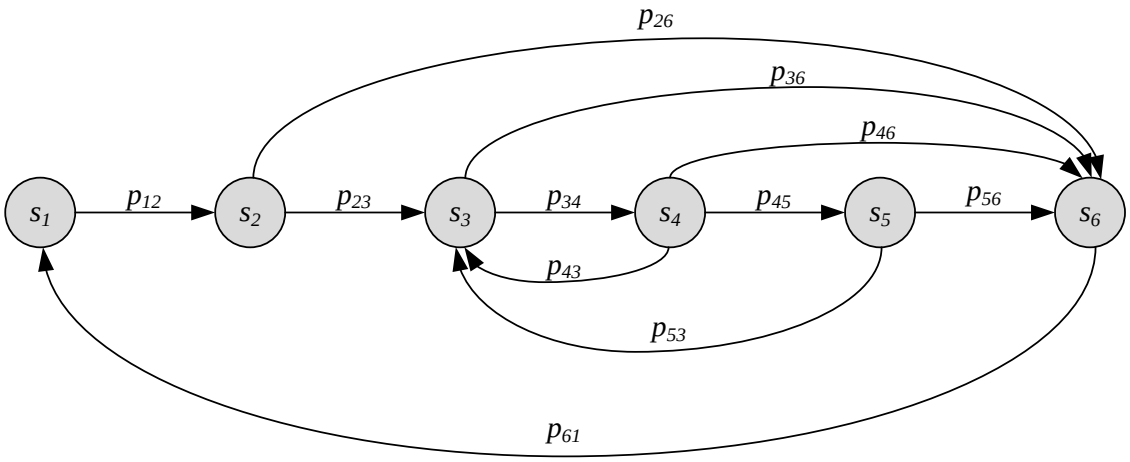


Рис. 2. Модель работы элемента сети тактовой сетевой синхронизации

Основными режимами, в которых может находиться каждый из генераторов, являются следующие:

s_1 – включение электропитания;

s_2 – самотестирование;

s_1 – выбор внешнего источника сигнала синхронизации и установка режима свободных колебаний;

s_3 – синхронный режим работы;

s_4 – режим удержания;

s_5 – отказ и восстановление [3].

Основным показателем надежности работы сетевого элемента сети тактовой сетевой синхронизации являются стационарные вероятности пребывания элемента сети в каждом из описанных выше состояний s.

Стационарную вероятность пребывания в каждом из состояний можно вычислить следующим образом [3]:

$$\pi_i = \frac{P_i T_i}{\sum_{j=1}^{S} P_j T_j}, (i, j \in s),$$

где P_i, P_j – стационарные вероятности пребывания вложенной марковской цепи в состояниях s_i и s_j, T_i, T_j – математические ожидания безусловного времени пребывания сетевого элемента в каждом из возможных состояний.

Сумма вероятностей нахождения элемента в одном из возможных состояний равна единице

$$\sum_{i \in s} \pi_i = 1.$$

Математические ожидания времени пребывания в каждом из состояний можно вычислить, используя следующее выражение:

$$T_i = \sum_{j=1}^{s} p_{ij} T_{ij},$$

где T_{ij} – математическое ожидание условного времени пребывания элемента сети синхронизации в каждом состоянии.

Если разделить все возможные состояния на работоспособные ($s_1 - s_5$) и неработоспособные (s_6), то можно определить коэффициенты готовности и простоя каждого элемента сети по следующим двум выражениям [2]:

$$K_{\text{гот}} = \sum_{i=1}^{s_5} \pi_i,$$

$$K_{\text{пр}} = 1 - K_{\text{гот}} = \pi_6.$$

Однако, рассмотренная модель описывает возможные состояния каждого отдельного элемента, а не сети в целом. Рассматривая сеть синхронизации, важно понимать, что узлы сети имеют различную важность для функционирования сети.

Так работоспособность задающего и вторичных генераторов гораздо важнее работоспособности генераторов сетевых элементов. Кроме того, вторичные генераторы можно разделить между собой по числу исходящих связей.

В теории графов число ребер, связанных с рассматриваемой вершиной определяется степенью этой вершины. Так как сеть синхронизации описывается ориентированным графом, то значимость узлов одного уровня иерархии можно определить исходящими степенями соответствующих вершин.

Таким образом, можно ввести коэффициенты значимости каждой вершины. Коэффициент может определяться отношением исходящей степени рассматриваемой вершины к общему числу исходящих связей генераторов одного уровня:

$$\alpha_i(\lambda_i) = \frac{\lambda_i}{\sum_{i=1}^{N} \lambda_i},$$

где λ_i – исходящая степень рассматриваемого узла, N – количество узлов синхронизации одного уровня.

Введение понятия о коэффициентах важности элементов сети может быть применено не только для оценки надежности сети синхронизации: при устранении петель синхронизации удалением ребер встает вопрос о том, как выбрать ребро, удаление которого минимально повлияет на работу сети. Очевидно, что удалять стоит ребро, инцидентное вершине с наименьшим коэффициентом важности.

Такой подход позволяет принять решение о важности узлов одного уровня, однако, он не учитывает общее число узлов, входящих в цепь, началом которой является рассматриваемый узел. Данной проблеме будут посвящены дальнейшие исследования.

Таким образом, рассмотренная математическая модель оценки надежности работы сети тактовой сетевой синхронизации позволяет оценить коэффициенты готовности и простоя каждого элемента сети синхронизации. А предложенный подход к определению коэффициентов важности узлов сети синхронизации может быть применен при устранении петель в сети. Знание этих параметров позволяет предотвращать отказы, вызванные неисправностями в сети тактовой сетевой синхронизации, а также планировать необходимый ремонт или замену элемента сети.

Список используемых источников

1. Поляков К. А., Сафонова И. Е., Иванов В. В. Графовая модель расчета аппаратурной надежности корпоративной телекоммуникационной сети // Телекоммуникации. 2012. № 12. С. 7–9.

2. Саати Т. Л. Элементы теории массового обслуживания и ее приложения. 3-е изд. М. : Книжный дом «ЛИБРОКОМ», 2010. 520 с.

3. Канаев А. К., Опарин Е. В. Математическая модель процесса функционирования элемента сети тактовой сетевой синхронизации для определения стационарных характеристик его надежности // Бюллетень результатов научных исследований. 2015. № 3–4 (16–17). С. 82–91.

УДК 004.932.1
ГРНТИ 50.41.25

ИСПОЛЬЗОВАНИЕ МЕТОДА ОЦУ ДЛЯ ВЫЧИСЛЕНИЯ АДАПТИВНОГО ПОРОГА СЕГМЕНТАЦИИ

М. А. Маколкина, М. В. Шарлаева

Санкт-Петербургский государственный университет телекоммуникаций им. проф. М. А. Бонч-Бруевича

В рамках данной статьи рассмотрена работа метода Оцу, приведены результаты применения глобального и адаптивного порога для сегментации изображений. Представлен метод оконной фильтрации исходного изображения. Выполнено сравнение использования метода вычисления значения порога Оцу в случаях исходного изображения с шумом и после применения оконного фильтра.

компьютерное зрение, обработка изображения, метод Оцу, глобальный порог, адаптивный порог, сегментация изображения.

На сегодняшний день одним из наиболее активно развивающихся направлений технологического прогресса являются системы искусственного интеллекта. Искусственный интеллект захватывает как давно существующие области человеческой деятельности, так и в корне новые, далекие от массового применения, направления. Технологии создания искусственных систем, получающих информацию из изображений, порождают такие научные направления, как компьютерное (техническое) и машинное зрение.

Компьютерное зрение – теория и технология создания машин, которые могут обнаруживать, отслеживать, классифицировать и идентифицировать объекты, извлекая данные из изображений для дальнейшего анализа без привязки к конкретной области. Машинное зрение является применением компьютерного зрения для промышленности и производства.

Любое изображение в компьютерной графике можно представить в виде набора пикселей [1]. Каждый пиксель характеризуется числовыми показателями цветовой модели, на основе которых можно произвести сегментацию. В компьютерном зрении под сегментацией понимается процесс разделения цифрового изображения на области с целью изменения его представления для дальнейшей обработки и анализа. Понятие области применяется для определения связности элементов изображения на основе общего признака.

В качестве промежуточного этапа обработки изображений часто используется пороговая сегментация. Пороговая обработка позволяет преобразовать исходное изображение, содержащее некоторое количество уровней

яркости, в бинарное или состоящее из сегментов различной яркости, отличных от первоначальных данных. Главной целью бинаризации является радикальное уменьшение количества информации [2], с которой требуется работать в дальнейшем.

Рассмотрим бимодальное изображение, где гистограмма уровней яркости состоит только из двух пиков. Метод Оцу автоматически вычисляет порог, минимизирующий среднюю ошибку сегментации [3]. Значения яркостей пикселей можно рассматривать как случайную величину, а их гистограмму как оценку плотностей распределения вероятностей, а значит можно определить и оптимальное пороговое значение. При помощи гистограммы все пиксели разделяются на фоновые и объектные. Каждому виду соответствуют относительные частоты w_0 (1), w_1 (2) и средние уровни μ_0 (3), μ_1 (4).

$$w_0 = \sum_{i=1}^{k} p_i, \tag{1}$$

$$w_1 = \sum_{i=k+1}^{L} p_i = 1 - w_0, \tag{2}$$

$$\mu_0 = \sum_{i=1}^{k} \frac{ip_i}{w_0}, \tag{3}$$

$$\mu_1 = \sum_{i=k+1}^{L} \frac{ip_i}{w_1}, \tag{4}$$

где $p_i -$ частота попадания пикселей в интервал уровня яркости, $k -$ порог яркости, $L -$ максимально допустимое значение порога яркости.

Далее вычисляется максимальное значение оценки качества разделения изображения на две части (5):

$$\eta(k) = \max_{1 \le k \le (L-1)} \frac{\sigma(k)^2}{\sigma^2_{\text{общ}}}, \tag{5}$$

где $\sigma(k)^2$ −межклассовая дисперсия, а $\sigma^2_{\text{общ}}$ −общая дисперсия всего изображения.

Процесс бинаризации полутоновых изображений является примером квантования изображения на два уровня, однако в результате могут возникать потери информации с последующей потерей качества изображения. Преимуществами метода Оцу являются простота реализации, высокая скорость выполнения и адаптация к искажениям входного изображения [2].

Для демонстрации работы описанного метода в качестве исходного полутонового изображения принят снимок гематологического исследования печени (рис. 1). Гематологическое исследование – это изучение образца крови с целью качественного и количественного анализа клеточных элементов [4].

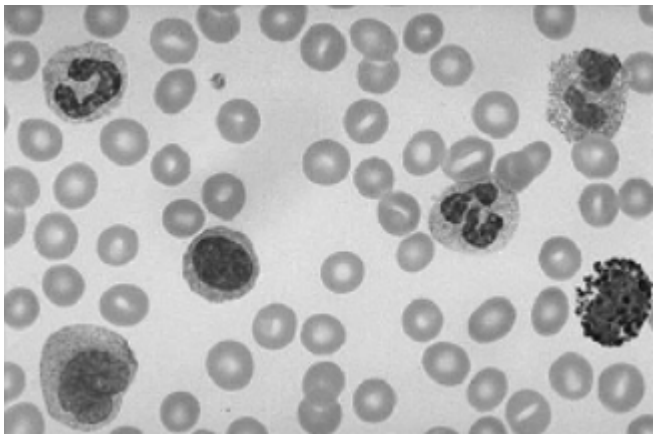


Рис. 1. Гематологическое исследование образца крови

В связи с особенностями аппаратуры на конечном изображении может присутствовать шумовая составляющая. Рассмотрим результат работы метода Оцу, примененный к изображению без шумов (рис. 2). Для получения такого изображения используется процедура оконной фильтрации. Данная процедура предполагает, что окно фильтрации последовательно перемещается по входному изображению согласно заданному маршруту, в каждом положении окна происходит анализ всех пикселей, принадлежащих данной области, и на основе анализа центральному пикселю окна на выходном изображении присваивается финальное значение [5, 6].

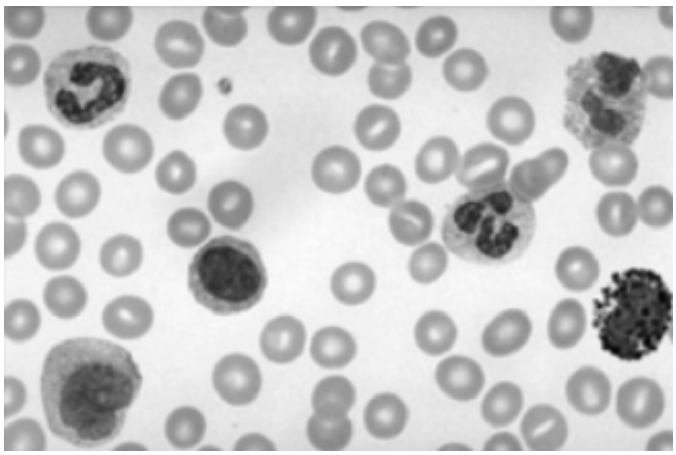


Рис. 2. Изображение после применения оконного фильтра

Сравнив результаты применения пороговой сегментации с использованием глобального порога (рис. 3) и метода Оцу (рис. 4), можно сделать вывод, что использование метода Оцу повышает точность сегментации [7].

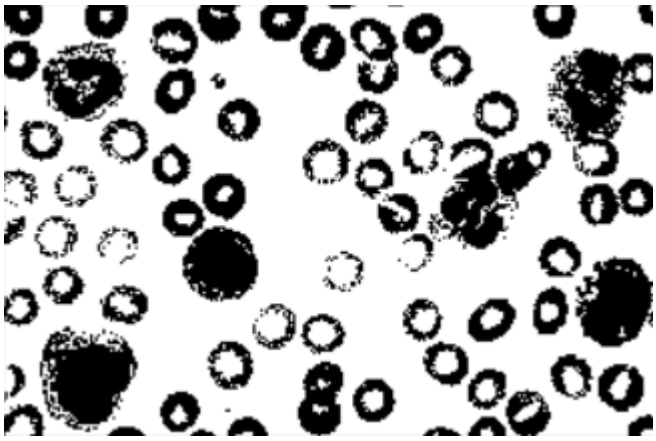
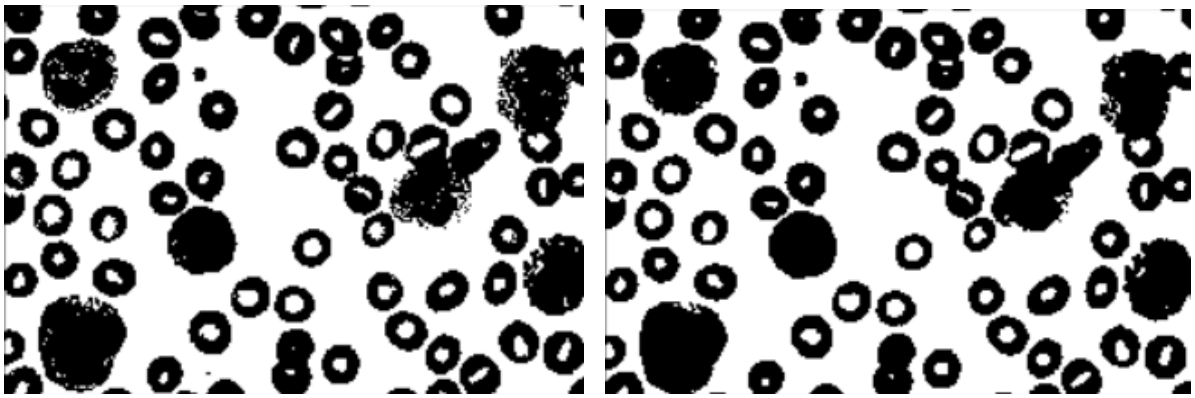


Рис. 3. Результат сегментации с применением глобального порога



а) б)

Рис. 4. Выходное изображение после применения: а) метода Оцу к зашумленному изображению; б) метода Оцу к изображению без шумов

Заключение

Реализованы и рассмотрены примеры порогового преобразования с использованием языка Python 3.4 и библиотеки для машинного обучения OpenCV 4.2. Выбирать подход бинаризации следует, исходя из изображений, которые необходимо распознавать. Адаптивную бинаризацию рекомендуется использовать для обработки полутоновых изображений невысокого качества, так как обычная бинаризация в таких случаях может повлечь за собой искажения [8]. Несмотря на то, что адаптивные методы позволяют более точно определить границы объектов, они работают медленнее пороговых, что также влияет на выбор метода.

Список используемых источников

1. Верхлютов В. М., Гапиенко Г. В. Обзор методов сегментации и триангуляции данных МРТ. – М. : Институт высшей нервной деятельности и нейрофизиологии РАН, 2005. С. 2–3.
2. Исрафилов Х. С. Исследование методов бинаризации изображений. – М. : Вестник науки и образования. Т. 2. 2017. С. 1.
3. Обнаружение объектов методом Оцу [Электронный ресурс]. URL: https://habr.com/ru/post/112079 (дата обращения: 04.01.2020).
4. Гематологические исследования [Электронный ресурс]. URL: https://www.niioncologii.ru/patients/screening-and-diagnosis/research-types/hematologic (дата обращения: 04.01.2020).
5. Фильтрация изображения на FPGA [Электронный ресурс]. URL: https://habr.com/ru/post/324070 (дата обращения: 04.01.2020).
6. Задача фильтрации изображений [Электронный ресурс]. URL: http://wiki.technicalvision.ru/index.php/Задача_фильтрации_изображений (дата обращения: 04.01.2020).
7. Otsu N. A threshold selection method from gray-level histograms. IEEE Trans. On System, Man and Cybernetics, 1979, Vol. SMC-9, № 1.
8. Яковлева Е.С., Макаров А.А. О свойствах блочного алгоритма бинаризации цифровых изображений // Компьютерные инструменты в образовании. 2015. № 4. С. 26–36.

УДК 004.932.1
ГРНТИ 50.41.25

ПРИМЕНЕНИЕ ПОРОГОВОГО ПРЕОБРАЗОВАНИЯ ДЛЯ СЕГМЕНТАЦИИ ИЗОБРАЖЕНИЙ

М. А. Маколкина, М. В. Шарлаева

Санкт-Петербургский государственный университет телекоммуникаций им. проф. М. А. Бонч-Бруевича

В данной статье представлено развитие концепции «Internet of Things» в области здравоохранения как появление новой идеи – «Internet of Medical Things». Приведены существующие анализаторы медицинских изображений и программные решения в области искусственного интеллекта для диагностики заболеваний. Описана классификация медицинских изображений, методы и фазы их обработки. Представлен сравнительный результат работы методов сегментации, основанных на пороговом преобразовании, реализованных с использованием библиотек машинного обучения. Рассмотрены примеры применения порогового преобразования в медицинских исследованиях.

медицинские изображения, искусственный интеллект, сегментация, пороговые методы, бинаризация, порог бинарного преобразования.

Введение

Высокий интерес к реализации концепции «Internet of Things» в области здравоохранения привел к быстрому появлению новой идеи – «Internet of Medical Things» («IoMT»).

«IoMT» – это концепция сети, объединяющей «подключенные устройства» и приборы, которые отслеживают состояние организма человека и окружающей его среды, включая медицинские изделия, способные интерактивно влиять на профилактический, лечебный и реабилитационный процессы [1].

Основная цель развития концепции заключается в получении максимально полной информации об организме человека, на основании которой можно производить диагностику, назначать лечение, а также предотвращать возникновение заболеваний.

Разработки в области искусственного интеллекта для диагностики заболеваний

Разработки в данной области ведутся ведущими странами и учеными. Корпорация IBM представила мировому рынку программных решений платформу Watson Health, в состав которой входит несколько модулей, в том числе и диагностический, направленный на выявление возможных онкологических заболеваний [2].

Подразделение британской компании DeepMind, занимающееся искусственным интеллектом, DeepMind Health выпустило решение, позволяющие диагностировать острую почечную недостаточность, а также предоставляющее специалистам расшифровку снимков оптической когерентной томографии с возможностью диагностики глазных заболеваний [3].

Разработка BioMind была создана компанией Hanalytics в сотрудничестве с крупнейшей в мире больницей неврологических заболеваний Tiantan. BioMind – это система поддержки диагностики заболеваний головного мозга, объединяющая новейшие технологии глубокого обучения с обширными клиническими знаниями, чтобы имитировать процесс диагностики изображений МРТ и КТ пациентов [4].

Израильская компания Zebra-Med выпустила продукт Zebra AI1, который совмещает аналитику и визуализацию в сфере пульмонологии. Работа основана на базе библиотеки примитивов для сверточных нейронных сетей cuDNN, в которой содержатся результаты КТ, МРТ, УЗИ, рентгенографии и других медицинских изображений [2, 5]. Благодаря чему платформа способна выявлять заболевания сердечно-сосудистой системы, печени, лёгких, костей, а также оценить риски пациентов.

Система Arterys является уникальной, поскольку объединяет в себе технологии облачного хранения данных, машинного обучения и медицинскую интроскопию [6]. На основе результатов МРТ и рентгенографии

можно визуализировать строение исследуемых областей организма в многомерных моделях.

Обработка медицинских изображений

Медицинские изображения принято классифицировать по способу получения и области исследования. Выделяют следующие виды изображений:

– анатомические: плоскостные или объемные снимки МРТ, рентгеновские снимки, снимки ультразвукового исследования;

– гистологические: изображения оптической микроскопии, изображения электронной микроскопии;

За создание и внедрение в медицинскую практику современных измерительно-вычислительных средств, методов и методик, позволяющих комплексно автоматизировать процесс исследования отвечает активно развивающееся научное направление – компьютерная электрофизиология.

Обработка любого медицинского изображения включает в себя фазы по улучшению качества изображения и выделению элементов, что в конечном итоге увеличивает точность диагностики.

Основные стадии цифровой обработки медицинских изображений:

– предварительная обработка;
– сегментация;
– улучшение и фильтрация;
– распознавание;
– диагностика.

Пороговые методы сегментации изображений

Пороговая обработка изображений является одним из методов сегментации изображений, который уменьшает формат изображения до двоичного, то есть вся информация на изображении сводится к двум категориям: переднего плана и фона [7]. Пороговая обработка является как самостоятельным методом сегментации изображений, так и может являться составляющей более сложных алгоритмов. Например, в основе метода водоразделов лежат три базовых концепции:

– обнаружение и устранение разрывов;
– пороговая обработка;
– обработка областей.

Центральным вопросом пороговой сегментации является определение порогов, которое должно выполняться автоматически [8]. Низкий порог приводит к трудностям сегментации, так как объекты сливаются и отчасти становятся трудноразличимы от помех (рис. 1).

Рис. 1. Результат использования низкого порога

Высокий порог способен привести к разрушению важных объектов путем разделения на мелкие фрагменты (рис. 2).

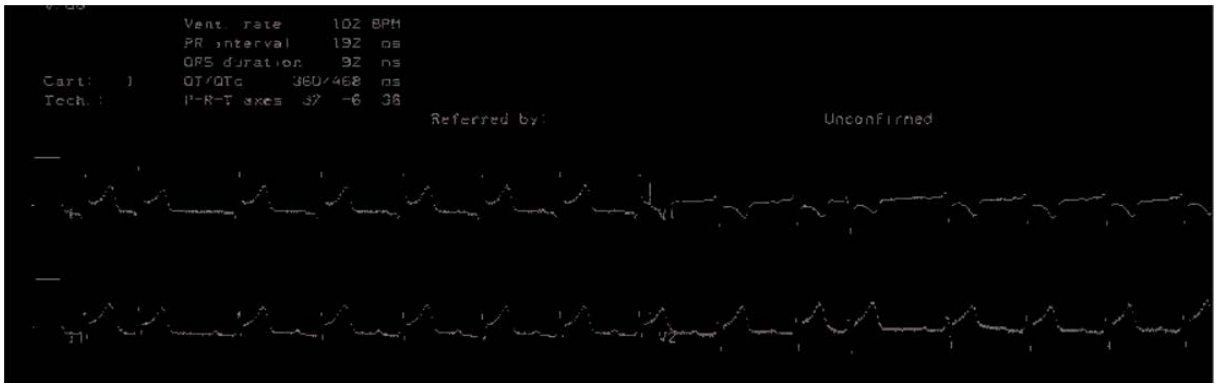


Рис. 2. Результат применения высокого порога

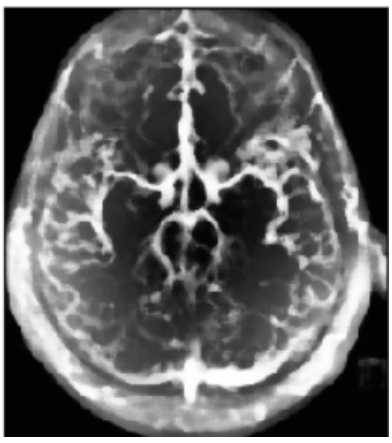
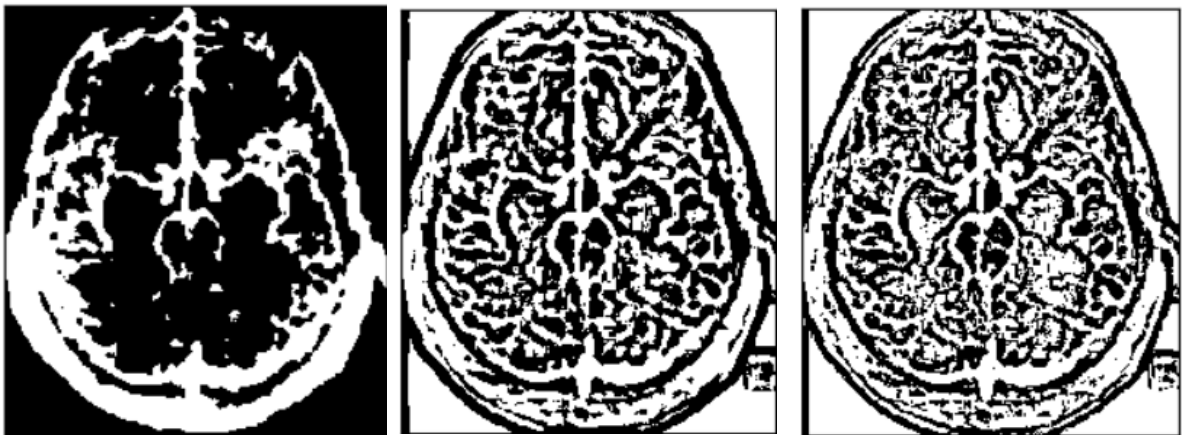


Рис. 3. Снимок МРТ сосудов головного мозга

Порог может быть постоянным или адаптивным, основой его выбора может служить гистограмма значений яркостей или энтропия [9]. Способы применения постоянного (глобального) порога рассмотрены выше и их главным недостатком является некорректная работа в условиях разной освещенности объектов. Адаптивный порог определяет порог для пикселя на основе области вокруг него, таким образом получаются разные пороги для разных областей исходного изображения. Результаты применения глобального и адаптивного порога представлены на рис. 4, в качестве входного изображения применялся рис. 3. Из чего можно сделать вывод, что адаптивный порог позволяет более точно определить границы объектов.



а) б) в)

Рис. 4. Выходное изображение после применения: а) глобального порога; б) адаптивного порога методом нахождения среднего значения окрестности; в) адаптивного порога методом взвешенной суммы значений окрестности

Заключение

Рассмотрены разработки в области искусственного интеллекта для диагностики заболеваний. Описана классификация медицинских изображений и фазы их обработки. Реализованы методы пороговой сегментации с использованием библиотек машинного обучения. Проведено сравнение методов вычисления порогового значения при сегментации медицинских изображений.

Адаптивную бинаризацию можно рекомендовать в случае обработки полутоновых изображений невысокого качества, поскольку из-за неравномерности фона применение фиксированного порога даст плохие результаты.

Неудачи в процессе бинаризации могут привести к искажениям, таким, как разрывы в линиях, потеря значащих деталей, нарушение целостности объектов, появление шума и непредсказуемое искажение символов из-за неоднородностей фона [10].

Список используемых источников

1. Лебедев Г. С., Шадеркин И. А., Фомина И. В., Лисненко А. А., Рябков И. В., Качковский С. В., Мелаев Д. В. Интернет медицинских вещей: первые шаги по систематизации // Журнал телемедицины и электронного здравоохранения. 2017. № 3 (5). С. 128–136.

2. Искусственный интеллект ставит диагнозы [Электронный ресурс]. URL: https://aiconference.ru/ru/article/iskusstvenniy-intellekt-stavit-diagnozi-95945 (дата обращения: 04.01.2020).

3. DeepMind’s health team joins Google Health [Электронный ресурс]. URL: https://deepmind.com/blog/announcements/deepmind-health-joins-google-health (дата обращения: 26.01.2020).

4. Product BioMind [Электронный ресурс]. URL: https://biomind.ai/product-biomind-2 (дата обращения: 26.01.2020).

5. Стрижов В. В. Использование технологий NVIDIA для решения задач глубокого обучения [Электронный ресурс]. URL: http://www.machinelearning.ru/wiki/index.php?title=Использование_технологий_NVIDIA_для_решения_задач_глубокого_обучения (дата обращения: 28.01.2020).

6. Asterys. Applications [Электронный ресурс]. URL: https://www.arterys.com/platform (дата обращения: 26.01.2020).

7. Мехатронные системы QNET. Методическое пособие для студентов [Электронный ресурс]. URL: http://nitec.nstu.ru (дата обращения: 04.01.2020).

8. Грузман И. С., Киричук В. С., Косых В. П., Перетягин Г. И., Спектор А. А. Цифровая обработка изображений в информационных системах: учебное пособие. – Новосибирск : Изд-во НГТУ, 2002. – 352 с.

9. Яковлева Е.С., Макаров А.А. О свойствах блочного алгоритма бинаризации цифровых изображений // Компьютерные инструменты в образовании. 2015. № 4. С. 26–36.

10. Федоров А. Бинаризация черно-белых изображений: состояние и перспективы развития [Электронный ресурс]. Режим доступа: http://itclaim.ru/Library/Books/ITS/wwwbook/ist4b/its4/fyodorov.htm/ (дата обращения: 21.02.2020).

УДК 004.725.4
ГРНТИ 50.41.23

ИССЛЕДОВАНИЕ МЕТОДОВ РАСПОЗНАВАНИЯ ОБЪЕКТОВ ДЛЯ ОРГАНИЗАЦИИ ДВИЖЕНИЯ БЕСПИЛОТНЫХ АВТОМОБИЛЕЙ

З. Б. Мамашев, А. С. А. Мутханна

Санкт-Петербургский Государственный Университет телекоммуникаций им. проф. М. А. Бонч-Бруевича

Сегодня происходит революция в автомобилестроении. Автомобили становятся беспилотными, оснащаясь продвинутыми датчиками, сенсорами, камерами и алгоритмами распознавания. Алгоритмы и сценарии каждый день развиваются и совершенствуются, однако беспилотным автомобилям рано выходить на дороги общего пользования. Работа алгоритмов детекции далека от идеала. Для правильной и синхронизированной работы всех элементов беспилотного автомобиля человеку необходимо передать весь свой интеллектуальный опыт алгоритмам искусственного интеллекта. В этой статье рассматриваются методы распознавания различных объектов системой компьютерного зрения и проблемы в данной области, а также анализируются различные варианты реализации сложных систем беспилотных автомобилей.

беспилотные автомобили, компьютерное зрение, нейронные сети, искусственный интеллект, распознавание объектов.

В последние годы, сфера беспилотных автомобилей привлекает всё больше внимания. На разработку умных транспортных средств идет большое количество инвестиций. У общества растет интерес к данному направлению. Разработчики работают над тем, чтобы автомобиль мог видеть и понимать, что происходит вокруг него. Такие автомобили уже ездят по дорогам, получают огромное количество информации и учатся. Крупными производителями беспилотных автомобилей являются такие компании как Waymo, Uber, Tesla, Яндекс и другие.

Автомобили с автономным управлением являются автономными системами принятия решений, которые обрабатывают потоки наблюдений, поступающих от различных бортовых источников. Эти наблюдения используются системой автономного вождения автомобиля для принятия решения на дороге [1]. На сегодняшний день, производители Waymo, Tesla, Nvidia/Audi, достигли третьего уровня автоматизации автономного транспорта [2].

На рис. 1 представлена классификация автоматизации беспилотных автомобилей сообществом автомобильных инженеров (SAE), содержащая 6 уровней [2].

Рис. 1. Уровни автоматизации беспилотных автомобилей

Программное обеспечение автономного автомобиля управляет работой всех систем, приводящих его в движение. Различные датчики и сенсоры собирают информацию об окружающей обстановке, которая ложится в основу действий автомобиля. Датчики и сенсоры устанавливаются, такие как:

– лидары составляющие часть чувствительных устройств, которые являются устройством дистанционного зондирования, используемым для проверки окружение транспортного средства с высокой точностью, посылая световые лучи [2];

– радары, используемые для обнаружения окружающих автомобиль объектов, и определения их размеров, скорости и дальности нахождения с помощью импульсов радиоволн;

– камеры;

– система глобального позиционирования (GPS, ГЛОНАСС);

– датчики одометрии используемые как средство оценки перемещения при движении приводов.

Программное обеспечение беспилотного автомобиля может включать машинное зрение и глубинные нейронные сети.

Машинное зрение использует компьютерное зрение для того, чтобы решать промышленные задачи. Компьютерное зрение представляет собой набор методов, с помощью которых машины могут отслеживать, классифицировать и идентифицировать объекты, анализируя данные из изображений.

До появления глубокого обучения, системы компьютерного зрения использовались на основе таких функций, как признаки Хаара, локальные бинарные шаблоны или гистограммы ориентированных градиентов. По сравнению с этими традиционными функциями ручной работы, свёрточные нейронные сети способны автоматически изучать представление пространства признаков, закодированного в обучающем наборе [1].

Свёрточные нейронные сети в основном используются для обработки пространственной информации, такой как изображения, и могут рассматриваться как экстракторы признаков изображения и универсальные аппроксиматоры нелинейных функций [1].

Рассматривая нейронные сети, можно сделать упор на свёрточную нейросеть YOLO построенную на базе фреймворка Darknet. Она является очень популярной, благодаря быстроте и точности [3].

Модель YOLO накладывает на изображение сетку, разделяя его на ячейки. Каждая ячейка пытается предсказать координаты зоны обнаружения с оценкой уверенности для этих полей и вероятностью классов. Затем оценка уверенности для каждой зоны обнаружения умножается на вероятность класса, чтобы получить окончательную оценку.

Был проведен эксперимент, на основе которого можно было понять, что данная нейросеть действительно быстро обнаруживает объекты и делает это довольно точно. На автомобиль Chevrolet Lacetti, была закреплена экшн-камера Digma DiCam-380. Данная камера снимала с разрешением FullHD и частотой 60 кадров/с. Отснятый материал был пропущен через нейросеть YOLO. Тесты проводились на среднем мультимедийном компьютере. В компьютере был установлен процессор AMD FX-8320 и видеокарта

Nvidia GTX 1050. Стоит отметить, что максимальной производительности можно достигнуть, имея видеокарты Nvidia с программно-аппаратной архитектурой параллельных вычислений CUDA, которая позволяет существенно увеличить вычислительную производительность. Для функционирования распознавания фреймворк Darknet требует предустановленную библиотеку алгоритмов компьютерного зрения, обработки изображений и численных алгоритмов общего назначения с открытым кодом – OpenCV (*Open Source Computer Vision Library*) [4]. Также необходимо установить библиотеку cuDNN представляющую собой ускоренную на GPU библиотеку примитивов для глубоких нейронных сетей. cuDNN предоставляет хорошо настроенные реализации для стандартных подпрограмм, таких как прямая и обратная свертка, пул, нормализация и уровни активации [5].

На рис. 2 можно видеть изображение из обработанного видео с прямоугольниками, окаймляющими объект, классификацией и вероятностью обнаружения объекта. Были распознаны автомобили, светофоры, люди.

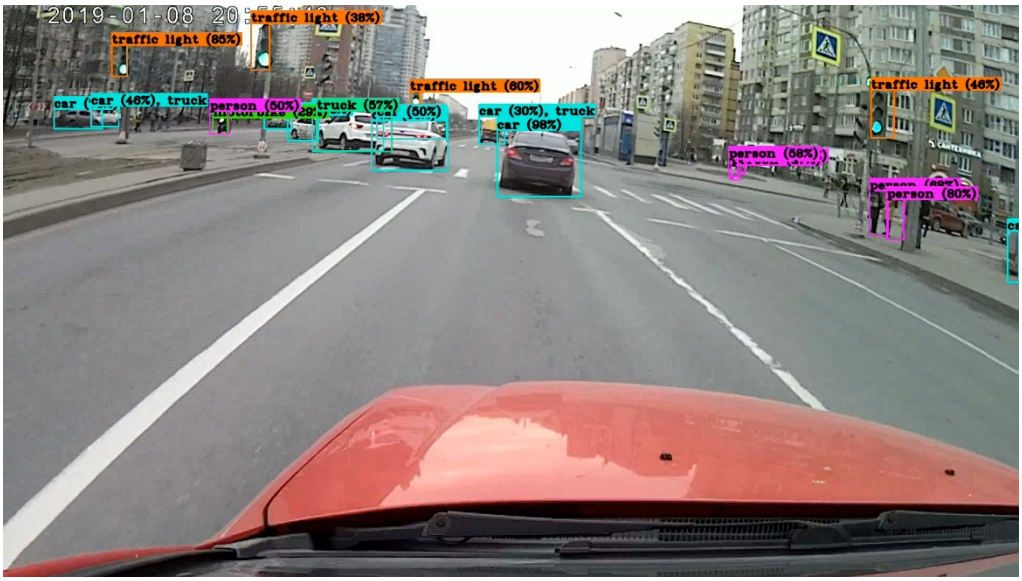


Рис. 2. Распознавание объектов на проезжей части моделью YOLOv3-608

В данном тесте использовалась модель YOLOv3-608 обученная набором данных COCO. Данная модель состоит из 106-ти свёрточных слоев и хорошо распознает небольшие объекты по сравнению с предыдущими версиями этой модели. Особенностью YOLOv3-608 является то, что на выходе есть три слоя каждый из которых рассчитан на обнаружение объектов разного размера. COCO - это крупномасштабный набор данных для обнаружения и сегментации объектов, созданный проектом Google Brain [6]. В целом данная модель показала хорошую точность и быстроту распознавания. Стационарная машина обрабатывала в среднем 8 кадров в секунду, что является удовлетворительным результатом.

Также был проведен тест с моделью YOLOv3-tiny. Она является маленькой моделью, предназначенной для ограниченных сред со слабой вычислительной мощностью [3]. Результаты можно видеть на рис. 3. Распознавание определенно хуже, чем при использовании YOLOv3-608, то есть объекты распознаются на малом расстоянии. При обработке, стационарная машина выдавала в среднем 18 кадров в секунду, что можно считать хорошим показателем. Данная модель состоит из меньшего количества слоев, хуже предсказывает мелкие объекты и предназначена для небольших наборов данных.

Рис. 3. Распознавание объектов на проезжей части с моделью YOLOv3-tiny

На сегодняшний день у систем распознавания существует множество проблем, таких как несовершенные сенсоры и алгоритмы распознавания, энергоэффективность, однако, алгоритмы распознавания улучшаются, становятся быстрее и точнее.

Нейросеть YOLO показывает хорошую скорость и неплохую точность при распознавании и вполне может использоваться как система распознавания в беспилотных автомобилях.

Список используемых источников

1. Sorin Grigorescu, Bogdan Trasnea, Tiberiu Cocias, Gigel Macesanu. A Survey of Deep Learning Techniques for Autonomous Driving [Электронный ресурс] // arXiv:1910.07738v2. 2020. 28 с. URL: https://arxiv.org/abs/1910.07738v2 (дата обращения 25.03.2020).

2. Shih-Chieh Lin, Chang-Hong Hsu, Yunqi Zhang, Matt Skach, Md Emamul Haque, Lingjia Tang, Jason Mars. The Architectural Implications of Autonomous Driving: Constraints and Acceleration // ASPLOS '18: Proceedings of the Twenty-Third International Conference on Architectural Support for Programming Languages and Operating Systems. 2018.

PP. 751–766. URL: https://web.eecs.umich.edu/~shihclin/papers/AutonomousCar-ASPLOS18.pdf (дата обращения 18.03.2020).

3. YOLO: Real-Time Object Detection [Электронный ресурс]. URL: https://pjreddie.com/darknet/yolo/

4. OpenCV library [Электронный ресурс]. URL: https://opencv.org/

5. NVIDIA cuDNN library [Электронный ресурс]. URL: https://developer.nvidia.com/cudnn

6. COCO Dataset [Электронный ресурс]. URL: http://cocodataset.org/#home

УДК 004.9
ГРНТИ 49.33.29

ТЕХНОЛОГИИ РЕАЛИЗАЦИИ СЕТЕВЫХ УСЛУГ NaaS

М. В. Марыков, А. В. Росляков

Поволжский государственный университет телекоммуникаций и информатики

В статье рассмотрены особенности модели предоставления сетевых услуг NaaS как одной из моделей облачных вычислений XaaS, ее реализация и применение. Описываются технологии, архитектура и протоколы программно-управляемых сетей SDN, виртуализации сетевых функций NFV, оверлейных сетей VON. Приведены примеры наиболее распространенных решений NaaS. Описаны преимущества и перспективы развития модели NaaS.

XaaS, NaaS, Future Networks, SDN, NFV, VON, Virtualization, Virtual Networks, инфокоммуникации.

XaaS (*as a service, aaS, xaaS, everything-as-a-service*) – это общий термин, который означает предоставление чего-либо как услуги. Он подразумевает огромное количество продуктов, инструментов и технологий, которые поставщики предоставляют пользователям в качестве услуг по сети.

Существует множество примеров XaaS, но наиболее распространенные из них охватывают три основные модели облачных вычислений: программное обеспечение как услуга (SaaS), платформа как услуга (PaaS) и инфраструктура как услуга (IaaS).

Внедрение технологий виртуализации и облачных вычислений в будущих сетях (*Future Networks*) [1] и в мобильных сетях пятого поколения 5G/IMT 2020 [2, 3, 4] способствовало появлению новой модели – «сеть как услуга» NaaS (*Network as a Service*) [5, 6]. NaaS – это модель предоставления сетевых услуг на основе подписки. Основные сервисные модели

NaaS: полоса пропускания по требованию (*Bandwidth-on-Demand*), виртуальная частная сеть VPN и виртуализация (слайсинг) в мобильных сетях связи (рис. 1).

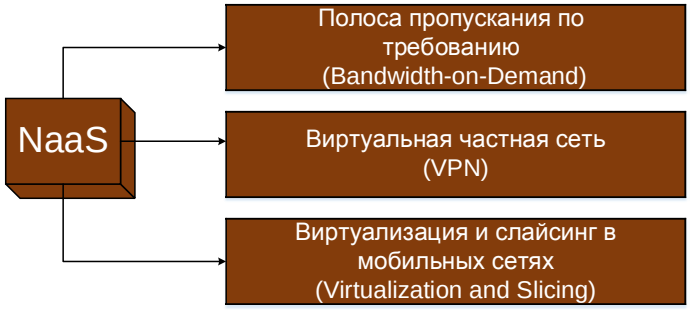


Рис. 1. Сервисные модели NaaS

При NaaS ресурсы операторов инфокоммуникационных услуг – приложения, виртуальные машины (VM), системы хранения (*Storage*) и каналы связи – реализуются на высокопроизводительных серверах с использованием облачных технологий в соответствии с текущей нагрузкой и потребностями клиента. Одной из особенностей модели NaaS является то, что вышеназванные ресурсы предоставляются с гарантированным качеством, которое запрашивают потребители услуг NaaS.

Технологии виртуализации позволяют создавать несколько виртуальных машин (VM) на одном сервере в дата-центре, при этом виртуальные машины управляются менеджером виртуальных машин, также известным как гипервизор (*Hypervisor*). Виртуальные машины обеспечивают точную имитацию интерфейса исходного сервера, при этом виртуальные машины изолированы друг от друга в рамках приложений, работающих на них. Это позволяет сетевому оператору размещать сетевые службы и функции на виртуальных машинах, используя все преимущества программируемых функций и мобильности виртуальных машин. Технологии виртуализации позволяют передавать образы виртуальных машин с загруженного сервера на любой недостаточно используемый сервер. Более того, NaaS позволяет оператору виртуализировать сетевые компоненты и создавать «виртуальной сети» (VN). Традиционные технологии виртуализации сетей, такие как виртуальные локальные сети (VLAN) и виртуальные частные сети (VPN), не предлагают модель аналогичную VN, которая отделяет сеть от физической инфраструктуры (рис. 2, см. ниже). Фактически, NaaS можно назвать «облаком» для традиционных инфокоммуникационных сетей.

Модель виртуальной сети VN подразумевает, что управляемая виртуализированная сеть не требует какого-либо ручного управления и взаимодействия с физическими ресурсами с помощью администратора сети. Подобно тому, как виртуальная машина VM является программным контейнером (логический процессор CPU, память, хранилище), обеспечивающим интерфейс, идентичный физическому интерфейсу компьютер-приложение, виртуальная сеть VN также является программным контейнером, включающим

в себя логические компоненты (маршрутизаторы, коммутаторы, межсетевые экраны и т. д.), которые представляют интерфейс, идентичный физической сети для сетевых приложений.

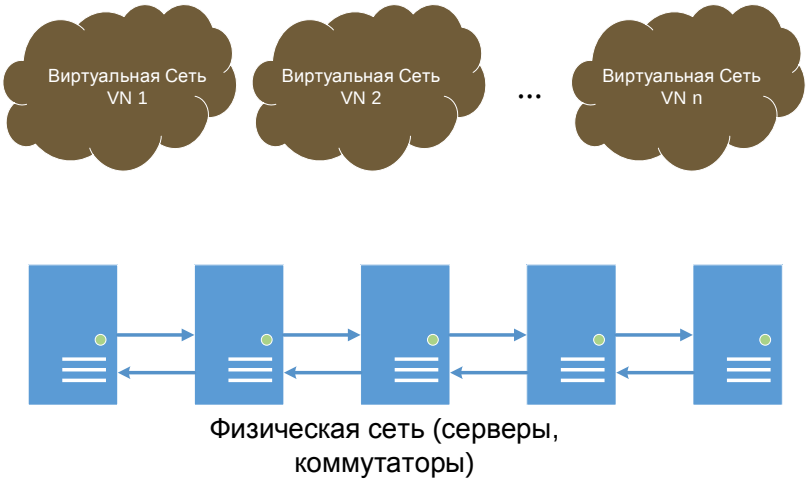


Рис. 2. Разделение виртуальных сетей от физической инфраструктуры в модели NaaS

Одной из самых перспективных технологий, основанной на модели NaaS, являются программно-конфигурируемые сети SDN (*Software Defined Networking*) [1]. Основная идея SDN состоит в том, чтобы реализовать горизонтально интегрированные системы, путем разделения плоскости управления CP (*control plane*) и плоскости данных DP (*data plane*) (рис. 3, см. ниже). Технология SDN произвела революцию в инфокоммуникациях, предоставив архитектуру для так называемого «программирования сетей». С помощью SDN операторы могут использовать все преимущества NaaS и создавать свою инфраструктуру SDN. В архитектуре SDN существует 2 основных класса прикладных программных интерфейсов API: API Southbound – определяет интерфейс между централизованным сетевым контроллером и сетевыми устройствами, и API Northbound – определяет интерфейс, предоставляемый контроллером для сетевых приложений. OpenFlow – это пример стандартного Southbound API.

В традиционных сетях плоскости управления CP и плоскости данных DP размещаются на одних и тех же устройствах для обеспечения децентрализованного управления сетью. В SDN сетях DP и CP разделены централизованным контроллером, управляющим несколькими DP, который поддерживает Southbound API для DP и Northbound API для приложений SDN.

SDN состоит из следующих компонентов и интерфейсов (рис. 3):

1. Приложения SDN. Это программное обеспечение, которое выполняют сетевые функции (например, маршрутизация).

2. Контроллер SDN. Это логически централизованный объект, который предоставляет приложениям SDN абстрактное представление о сети

и транслирует входные данные, полученные от приложений SDN, в физическую сеть.

3. SDN Datapath Это логическое сетевое устройство (или несколько сетевых устройств), которое настраивается и управляется контроллером SDN для пересылки и обработки данных (таких, как пересылка пакетов).

4. CDPI (SDN *Control to Data-Plane Interface*). Это интерфейс между плоскостями управления и данными в SDN.

5. NBIs (*SDN Northbound Interfaces*). Это интерфейсы между приложениями и контроллером SDN.

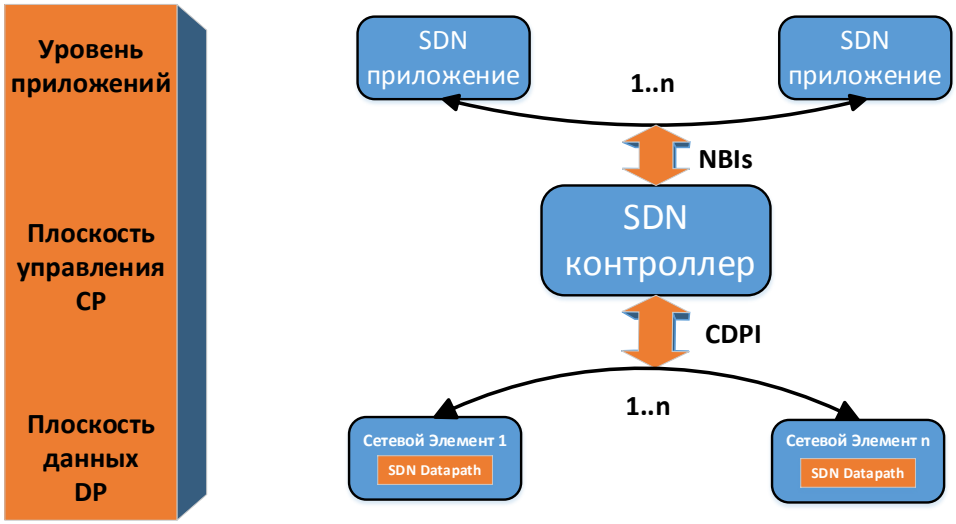


Рис. 3. Программно-управляемая сеть SDN

Технология SDN использует протоколы OpenFlow, PCEP, BGP, NETCONF, SNMP. Самые известные решения SDN: контроллеры с открытым кодом NOX, POX, Floodlight виртуальные коммутаторы с открытым кодом Open vSwitch.

С запросами операторов на виртуализацию набирает популярность технология виртуализации сетевых функций NFV (*Network Functions Virtualization*), которую тоже можно отнести к модели NaaS. Суть виртуализации сетевых функций NFV заключается в развертывании сетевых функций в программных компонентах, называемых виртуальными сетевыми функциями VNF (*Virtual Network Functions*) [1]. VNF реализуются на высокопроизводительных серверах с использованием облачных технологий. Технология NFV позволяет отделить программное обеспечение от физического оборудования.

Еще одной реализацией NaaS являются оверлейные сети (VONs – *Virtualized Overlay Networks*) [7] – это концепция, подразумевающая развертывание общей «сетевой структуры», которая может быть автоматически запрограммирована для предоставления любой услуги без необходимости

ручной настройки узлов базовой сети. Оверлейные сети работают как независимые виртуальные сети поверх физической сетевой инфраструктуры. Эти виртуальные сети позволяют поставщикам ресурсов, таким как облачные провайдеры, предоставлять и организовывать сети вместе с другими виртуальными ресурсами. Технология VON использует протоколы туннелирования, такие как VXLAN, NVGRE и STT. Самые известные VON решения – VMWare's NSX, PlumGrid, Midokuro, Nuage.

Основными преимуществами модели NaaS являются: гибкость в развертывании, масштабируемость, простота обслуживания, автоматизация, настраиваемые политики в своей собственной виртуальной сети, отсутствие проблем взаимодействия оборудования разных вендоров, эффективное использование ресурсов дата-центра, локализация сбоев, (проблема в одной VN или в одной VM не влияет на всю сетевую инфраструктуру)

Если оператор инфокоммуникационных услуг не занимаетесь сетевым бизнесом, то создание собственной сети отвлекает от основных приоритетов и бизнес-задач организации. Реализация сети по модели NaaS позволяет сэкономить средства и время, которые можно использовать для вывода на рынок конкурентных продуктов и услуг. Поэтому модель NaaS продолжит развиваться и активно внедряться в инфокоммуникации.

Список используемых источников

1. Росляков А. В., Ваняшин С. В. Будущие сети (Future Networks). Самара : ПГУТИ, 2015. 274 с.

2. Росляков А. В., Витевский В. Д. Виртуализация в будущих беспроводных сетях // Мобильные телекоммуникации. 2016. Март-апрель. С. 2–4.

3. Росляков А. В, Поддубнов И. В. Виртуализация в сетях 5G // Информационные технологии и информационная безопасность в науке, технике и образовании (ИНФОТЕХ-2019) Всероссийская научно-техническая конференция, Севастополь, 2019. С. 114–118.

4. Росляков А. В, Марыков М. В. Проблемы виртуализации в сетях 5G // III научный форум «Телекоммуникации: теория и технологии ТТТ-2019». Проблемы техники и технологий телекоммуникаций ПТиТТ-2019: материалы XXI Международной научно-технической конференции. Казань, 1–22 ноября 2019 года. – Казань : КНИТУ-КАИ, 2019. Т. 1. С. 235–236.

5. Есауленко А. Прокат сетей // Сети/Network world. 2013. No 1. P. 3.

6. Kumar G. A Review on Data Protection of Cloud Computing Security, Benefits, Risks and Suggestions // United International Journal for Research & Technology, 2019. V. 1. No 2. P. 26–34.

7. Росляков А. В., Витевский В. Д. Обзор проектов виртуализации телекоммуникационных сетей // Инфокоммуникационные технологии. 2017. Т. 15. № 3. С. 241–250.

УДК 621.396
ГРНТИ 49.27.31

ЭКСПЕРИМЕНТАЛЬНАЯ ПРОВЕРКА ОДНОЧАСТОТНОГО КВ МОДЕМА ПЕРЕДАЧИ ДАННЫХ НА ОСНОВЕ СИГНАЛОВ СТАНДАРТА ARINC 635

М. Л. Маслаков

Российский институт мощного радиостроения

В работе представлены результаты трассовых испытаний макета одночастотного модема передачи данных КВ диапазона. Рассмотрены основные технологические наработки. Проведен анализ показателей эффективности одночастотной КВ радиолинии на базе сигналов авиационного стандарта ARINC 635.

модем передачи данных, одночастотный модем, авиационная связь, ARINC 635.

По мере развития авиационной отрасли и растущими требованиями к обслуживанию воздушного движения (ОВД) [1] и воздушному оперативному управлению в океанических районах экономичным и надежным способом роль и потребность КВ линий передачи данных возрастает. Поэтому в интересах обеспечения ОВД в 1998 году компания ARINC (США) запустила единственную в мире систему КВ передачи данных (*High Frequency Data Link* – HFDL) [2]. HFDL представляет собой экономически эффективную альтернативу спутниковой системе передачи данных (ССПД), но используется совместно с ССПД, обеспечивая наиболее надежную комбинацию передачи данных в интересах дальней авиации. Кроме того, HFDL обеспечивает канал передачи данных для полярных регионов, где ухудшается производительность ССПД. Не удивительно, что число оборудованных воздушных судов (ВС) непрерывно растет и, в частности, к 2015 году составляло более 2600 самолетов [2, 3].

Система HFDL включает воздушную и наземные компоненты и описывается рядом спецификаций и протоколов. Физический, канальный и сетевой уровни канала «борт-земля» описываются протоколом ARINC 635 [4].

В настоящее время в АО «РИМР» ведется работа по созданию одночастотного КВ модема, включающая разработку: адаптивного корректирующего фильтра (КФ) или эквалайзера; модулятора/демодулятора; декодера с мягкими решениями и ряд других задач. Для экспериментальной проверки и отработки разработанных алгоритмов были произведены записи сигналов

стандарта ARINC 635, излучаемых ВС и наземными станциями и их последующая обработка.

Основной целью данного этапа работы являлась проверка и отладка алгоритмов установления синхронизации, методов настройки КФ и алгоритма демодуляции. Лучшей оценкой эффективности этих алгоритмов будет являться оценка вероятности ошибки на бит и вероятность потери блока, поэтому дополнительно были реализованы декодер сверточного кода и алгоритм проверки CRC. Отметим, что реализация алгоритма CRC в HFDL отличается от известных алгоритмов и описана в стандарте ARINC 429 [5].

В составе преамбулы передается «ключевая» информация длительностью 448 символов (249 мс), представляющая собой тон (несущую) 1440 Гц. Главная цель «ключа» позволить передатчику достичь полной мощности, а приемнику установить АРУ и получить оценку допплеровского смещения частоты.

Первой задачей при реализации приемной части КВ модема является установление синхронизации и прием служебной информации о скорости передачи данных, размере передаваемого блока (MPDU или SPDU) и длине перемежителя. Для этого в стандарте ARINC 635 в преамбуле передают три псевдослучайные последовательности (ПСП) длиной 127 символов: две одинаковые ПСП для установления тактовой синхронизации и одна, отличная от первых двух ПСП, для передачи служебной информации, за счет циклического сдвига.

Решение этих задач эффективно решается помощью корреляционного приема следующим образом:

$$R_{\cos}(t) = S(t) \otimes S_{0,\cos}(t),$$
$$R_{\sin}(t) = S(t) \otimes S_{0,\sin}(t),$$
$$R(t) = \sqrt{R_{\cos}^2(t) + R_{\sin}^2(t)}$$

где $S(t)$ – принимаемый сигнал, $S_{0,\cos}(t)$, $S_{0,\sin}(t)$ – косинусный и синусный образцовый сигнал ПСП, $\otimes$ – оператор корреляции, $R(t)$ – функция взаимной корреляции.

На рис. 1 (см. ниже) показан пример функции $R(t)$ при приеме преамбулы очередного блока данных ARINC 635.

Первые два пика корреляционной функции соответствуют началу синхронизирующих ПСП, длительность которых составляет 70,6 мс. Начало третьей ПСП, соответствует циклическому сдвигу на 72 символа «влево», что в свою очередь соответствует длительности передаваемого информационного блока 1,8 с со скоростью 300 бит/с.

Второй задачей является настройка КФ. Для решения этой задачи известно большое количество различных алгоритмов (смотри [6, 7]).

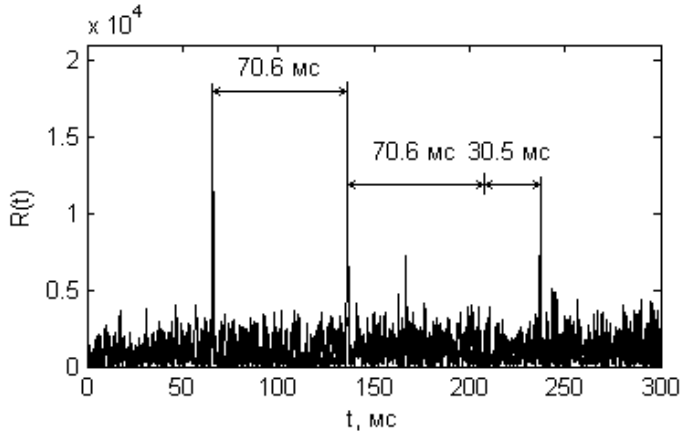


Рис. 1. Прием преамбулы ARINC 635

Для настройки КФ в состав преамбулы введены 9 тестовых сигналов длительностью 15 символов (8,33 мс), кроме того далее осуществляется периодическая вставка таких же тестов через каждые 30 информационных символов (16,67 мс). Таким образом, наблюдаются 9 пиков с интервалом 8,33 мс, и последующих с интервалом 8,33 + 16,67 = 25 мс (рис. 2). Такая структура позволяет проводить периодическую подстройку КФ на длительности всего передаваемого информационного блока.

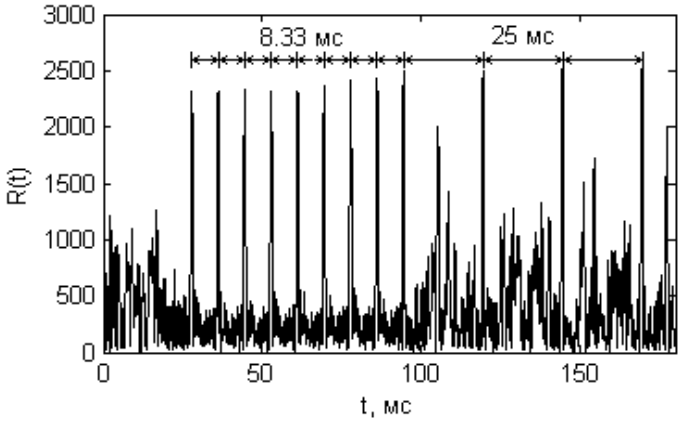


Рис. 2. Корреляционная функции тестовых сигналов

Используемая в ARINC 635 структура сигналов оказывается удобной для применения методов квазикогерентного сложения [8] для первоначального расчета импульсной характеристики КФ с повышенной точностью и последующего использования алгоритма адаптивной коррекции с обратной связью по решению [9], позволяющих значительно повысить помехоустойчивость модема. На указанные методы, получены патенты РФ [10, 11] (правообладатель АО «РИМР»).

После процедуры коррекции и демодуляции осуществляется снятие скремблирующей последовательности, операция деперемежения и декодирования.

Объем передаваемых данных с ВС и наземных станций может различаться в зависимости от типа передаваемого сообщения. Так передача блока данных скьютера (SPDU), передаваемого с наземной станции каждые 32 с, всегда осуществляется на скорости 300 бит/с в течение 1,8 с, а его размер составляет 67 байт. Напротив, размер блока данных MPDU может варьироваться от 16 до 90 байт. Для каждого блока MPDU рассчитывается свое значение CRC. Таким образом, на длительности информационного пакета 1,8 или 4,2 с может содержаться несколько таких блоков. В результате отдельной задачей становится определение длины передаваемых данных.

На базе приемо-передающей аппаратуры производства АО «РИМР» были проведены трассовые испытания макета одночастотного КВ модема, реализующего прием сигналов стандарта ARINC 635. В ходе испытаний осуществлялся прием сигналов базовых наземных станций системы HFDL, а также сигналов гражданских ВС, оснащенных соответствующими модемами.

Местоположение базовых наземных станций и используемые несущие частоты приведены в таблице 1.

ТАБЛИЦА 1. Номер и местоположение передающей станции и используемая несущая частота

Номер и местоположение передающей станции	06 Hat Yai, Thailand	07 Shannon, Ireland	16 Agana, Guam, USA	17 Telde, Gran Canaria, Spain
Несущая частота, МГц	13,270	8,942	17,919	11,348

Отметим, что на ряде выделенных частот, используемых в системе HFDL, осуществляется передача погодной информации в формате речевых сообщений. Однако большинство выделенных частот не задействованы.

Статистика принятых сообщений приведена в таблице 2.

ТАБЛИЦА 2. Статистика принятых сообщений

Длительность кадра, с	Информационная скорость, бит/с	Размер кадра MPDU, Байт	Количество принятых кадров MPDU	Количество принятых сообщений	Количество не принятых сообщений
1,8	300	67	364	817	4
	600	135	15	28	0
	1200	270	3	3	0
4,2	300	157	15	107	0
	600	315	7	48	0

В результате проведенной работы удалось отладить и оптимизировать алгоритмы синхронизации, адаптивной коррекции, деперемежения и декодирования для одночастотного КВ модема передачи данных.

Список используемых источников

1. Авиационная электросвязь. Т. 3. Системы связи. Изд. 2. Международная организация гражданской авиации, 2007.
2. Fundamentals of HF Data Link. Overview. June, 2013.
3. Fundamentals of HF Data Link. Overview. August, 2015.
4. ARINC Characteristic 635-2. HF Data Link Protocol. – Feb. 27, 1998.
5. ARINC Specification 429P3-18. Mark 33 Digital Information Transfer System (DITS), Part 3 File Data Transfer Techniques. – Oct. 12, 2001.
6. Джиган В. И. Адаптивная фильтрация сигналов: теория и алгоритмы. М. : Техносфера, 2013. 530 с.
7. Sayed A. H. Adaptive filters. New Jersey : Hoboken: John Wiley & Sons, Inc., 2008.
8. Маслаков М. Л. Методы повышения ОСШ в задачах адаптивной коррекции // Радиолокация и радиосвязь. X Всероссийская конференция, Москва. 2016. С. 267–271.
9. Маслаков М.Л. Новый алгоритм адаптивной коррекции с обратной связью по решению для передачи данных в канале с межсимвольной интерференцией // Успехи современной радиоэлектроники. 2018. № 1. С. 44–51.
10. Егоров В. В., Лобов С. А., Маслаков М. Л. и др. Устройство адаптивной настройки корректирующего фильтра с весовым квазикогерентным сложением теста. Пат. 154750 РФ; Заявитель и патентообладатель АО «РИМР». Опубл. 10.09.15.
11. Егоров В. В., Лобов С. А., Маслаков М. Л. и др. Устройство адаптивной коррекции с обратной связью по решению в каналах с межсимвольной интерференцией. Пат. 178763 РФ; Заявитель и патентообладатель АО «РИМР». Опубл. 18.04.18.

УДК 004.056.5
ГРНТИ 81.93.29

МЕТОД ОЦЕНКИ ЭФФЕКТИВНОСТИ СИСТЕМЫ ЗАЩИТЫ ИНФОРМАЦИИ ТЕРРИТОРИАЛЬНО-РАСПРЕДЕЛЕННЫХ ИНФОРМАЦИОННЫХ СИСТЕМ ПЕРСОНАЛЬНЫХ ДАННЫХ

А. А. Миняев

Санкт-Петербургский государственный университет телекоммуникаций им. проф. М. А. Бонч-Бруевича

В данной статье предложен метод оценки эффективности системы защиты информации территориально распределенных информационных систем персональных

данных. В качестве формы проведения оценки соответствия предлагается форма декларации соответствия системы защиты информации требованиям по безопасности персональных данных. Критериями являются проектные решения по защите информации, а также эксплуатационная документация на систему. В качестве метода используется метод экспертных оценок (метод комиссий).

обеспечение безопасности персональных данных; экспертные оценки эффективности систем защиты; территориально-распределенные информационные системы (ИС).

В соответствии с ежегодными отчетами международных организаций, занимающихся проблемами информационной безопасности, таких как Group-IB и Kaspersky, в которых говориться об активности так называемых проправительственных организаций, занимающихся киберпреступлениями (проведению атак) в интересах своих государств. Шпионаж остается ключевым направлением деятельности групп, спонсируемых государствами разных стран. В разделе отчета Group-IB, посвященном атакам на критические информационные инфраструктуры делается неутешительный вывод: уникальный ландшафт APT-угроз (*Advanced Persistent Threat* – «развитая устойчивая угроза», целевая кибератака), характерный для каждого региона постоянно меняется, злоумышленники стараются пользоваться широко распространенными инструментами, в том числе для тестов на проникновение, что затрудняет работу исследователей. Актуальность проблемы обеспечения безопасности информации обусловлена, также, ростом утечек информации и компьютерных атак, отражаемых в статистических данных по совершению преступлений в сфере высоких технологий, приводимыми Генеральной прокуратурой Российской Федерации и ведущими международными и организациями Российской Федерации в сфере информационной безопасности, а также законодательными нововведениями. В соответствии со сводными отчетами Генеральной прокуратуры Российской Федерации рост криминальной активности с использованием интернета и современных коммуникационных устройств в 2017 году в России составил 37 % и достиг 90 587 зафиксированных случаев по сравнению с 65 949 в 2016 году. Соответственно каждое двадцатое преступление от числа всех зарегистрированных в России преступлений квалифицируется как киберпреступление. В соответствии со статистикой основными утечками данных являются персональные данные пользователей, в частности, их учетные данные в информационных системах персональных данных (ИСПДн).

Для территориально-распределенных ИС характерно размещение серверных компонент, сетевого оборудования и автоматизированных рабочих мест пользователей на всей территории страны и, возможно, за ее пределами. В этом случае такие ИС имеют сложную архитектуру с точки зрения расположения своих компонентов и технологий обработки информации. Соответственно, возникают и сложности с обеспечением информационной

безопасности, а также при проведении оценки эффективности систем защиты информации.

Существуют следующие методы (подходы) оценки эффективности, используемых при оценке систем защиты информации.

- статистический;
- вероятностный;
- частотный;
- экспертное оценивание;
- информационно-энтропийный.
- нейросетевой метод (многокритериальная оценка);
- метод минимизации рисков;
- матричный метод (формальные модели защиты);
- многоуровневый метод;
- оптимизационный (комбинаторный).

В качестве критериев оценки соответствия предлагается использовать проектные решения по обеспечению безопасности персональных данных и эксплуатационную документацию на систему защиты информации ИС.

Для этого необходимо анализировать проектные решения на систему защиты информации ИС, эксплуатационную документацию на ИС, средства защиты информации, и организационно-распорядительной документации по ЗИ в составе: пояснительная записка с изложением решений по обеспечению ЗИ, составу средств защиты информации с указанием их соответствия требованиям технического задания на создание системы защиты информации; описание технического, программного, информационного обеспечения и технологии обработки (передачи) информации; план организационно-технических мероприятий по подготовке ИСПДн к внедрению средств и мер защиты информации; технический паспорт ИСПДн.

Для территориально-распределенных информационных систем персональных данных на основании положений ГОСТ 0043-003-2012 [1] и на основании 152 ФЗ [2] в части методики оценки соответствия была выбрана форма декларации соответствия по требованиям безопасности ИСПДн и положения о распространении результатов оценки на однотипные территориально-распределенные информационные системы персональных данных [3].

В данной статье предлагается использовать метод экспертного оценивания (метод экспертных оценок) в форме проведения декларации соответствия.

Соответственно, оценка эффективности системы защиты (W) рассчитывается следующим образом:

$$W = \frac{\sum_{j=1}^{m} X_j}{m}; 0 \leq W \leq 1,$$

где X_j – выполнение требования одного из критериев, $j = 1,m$; m – перечень показателей. Требование выполнено $X_j = 1$, требование не выполнено $X_j = 0$.

Также оценку эффективности можно рассчитывать с учетом важности выполнения требований:

$$W = \sum_{j=1}^{m} x_j a_j; 0 \leq W \leq 1,$$

где $0 \leq a \leq 1; \sum_{j=1}^{m} a_j = 1$, a – коэффициент важности требования.

При этом полагается, что минимальное значение оценки эффективности принятых мер, при которой будет считаться, что элемент системы соответствует эталонному, устанавливается экспертной комиссией, исходя из уровня защищенности ИСПДн [4].

Подтверждением того, что меры по защите ПДн применены в ИСПДн, является протокол проведения декларации соответствия СЗПДн, утвержденный экспертной комиссией [5].

Метод позволяет просто и наглядно оценивать эффективность системы защиты информации в территориально распределенных информационных системах персональных данных.

Список используемых источников

1. ГОСТ РО 0043-003 2012 Защита информации. Аттестация объектов информатизации. Общие положения. ДСП.

2. Федеральный закон РФ от 27 июля 2006 г. № 152-ФЗ «О персональных данных», 2006, 21 с.

3. Будько М. Ю., Миняев А. А. Методика оценки эффективности системы защиты персональных данных информационной системы // Проблема комплексного обеспечения информационной безопасности и совершенствование образовательных технологий подготовки специалистов силовых структур : межвузовский сборник трудов VI Всероссийской научно-технической конференции (ИКВО НИУ ИТМО, 10 декабря 2015 г.), 2016. С. 43–45.

4. Будько М. Ю., Миняев А. А. Метод оценки эффективности системы защиты персональных данных // Информатизация и связь. 2016. № 2. С. 85–87.

5. Будько М. Ю., Миняев А. А. Проблемы аттестационных испытаний информационных систем по требованиям безопасности информации // Проблема комплексного обеспечения информационной безопасности и совершенствование образовательных технологий подготовки специалистов силовых структур : межвузовский сборник трудов IV Всероссийской научно-технической конференции ИКВО НИУ ИТМО, 2014. С. 44–47.

Статья представлена заведующим кафедрой ЗСС СПбГУТ, кандидатом технических наук, доцентом А. В. Красовым.

УДК 629.391
ГРНТИ 49.33.29

УМНЫЙ ГОРОД С ПОДДЕРЖКОЙ ГРАНИЧНЫХ ВЫЧИСЛЕНИЙ

А. С. А. Мутханна, Д. Н. Никитин

Санкт-Петербургский государственный университет телекоммуникаций им. проф. М. А. Бонч-Бруевича

В настоящее время происходит значительный рост численности населения городов, а также увеличение данных, генерируемых различными устройствами, такими как смартфоны, системы глобального позиционирования, интеллектуальные камеры. В последние годы было обнаружено значительное распространение приложений, требующих большого объема вычислений, в умных городах. Такие приложения должны обеспечивать возможности вычислительной обработки с учетом задержки. Хоть граничные вычисления и являются хорошей технологией для решения вопросов, связанных с задержками, они порождают новые проблемы. В этой статье проводится общий обзор умных городов и роль граничных вычислений в них. Анализируются требования, предъявляемые к умным городам с поддержкой граничных вычислений.

умный город, граничные вычисления, 5G.

С каждым годом объем трафика, создаваемого устройствами с доступом в интернет, увеличивается в сотни раз. Прогнозируется, что общее количество устройств Интернета вещей (IoT) вырастет до 50 млрд к 2030 г. [1]. Развитие IoT и сетей 5G способствует совершенствованию такой технологии, как «Умный город».

Технология «умный город» была создана как взаимосвязанная система информационно-коммуникационных технологий (ИКТ), в том числе систем Интернета вещей (IoT) для управления городской инфраструктурой. Данная концепция позволяет упростить жизнь населения и повысить эффективность работы городских служб. Модель «умного города» может иметь такие компоненты как [2]:

1. Умный дом.
2. Умная парковка.
3. Профессиональная радиосвязь и широкополосный доступ (LTE, 5G, городские сети Wi-Fi).
4. Интеллектуальные камеры видеонаблюдения.
5. Беспилотные автомобили.
6. Приложения дополненной/виртуальной реальности.
7. Интеллектуальные транспортные системы.
8. Умное производство.

9. Единая система экстренного вызова.

Современный «умный город» взаимодействует с огромным количеством данных, генерируемых различными устройствами, для чего требуются крупномасштабные вычисления и хранилища с достаточной ёмкостью. Для исключения использования дорогостоящего оборудования были введены облачные вычисления, которые обладают такими особенностями как масштабируемость, мультиарендность, эластичность, отказоустойчивость, пул ресурсов. Однако присущие им ограничения высокой задержки, неконтролируемого поведения и отсутствие поддержки мобильности создают серьезные ограничения на их использования в интеллектуальных средах реального времени. Применение граничных вычислений для технологий «умного города» призвано решить данные проблемы.

Технология Multi-access Edge Computing (граничные вычисления множественного доступа MEC), которая раньше имела название мобильных граничных вычислений (*Mobile Edge Computing*) – одна из последних реализаций Edge computing. MEC был разработан и стандартизирован Европейским институтом телекоммуникационных стандартов (ETSI). Основной идеей данной концепции является вынесение вычислительных ресурсов на границу сети радиодоступа (RAN) [3]. MEC реализуется на основе виртуализированной платформы, использует те же принципы, что и виртуализация сетевых функций (NFV), а также применяет технологию программно-конфигурируемых сетей (SDN), которые призваны облегчить автоматизацию управления сетью [5]. Архитектура MEC состоит из следующих компонентов [4] (рис. 1):

1. Пользовательские устройства.
2. Базовые станции.
3. Серверы MEC.
4. Ядро сети.
5. Базовая инфраструктура (например, Интернет).

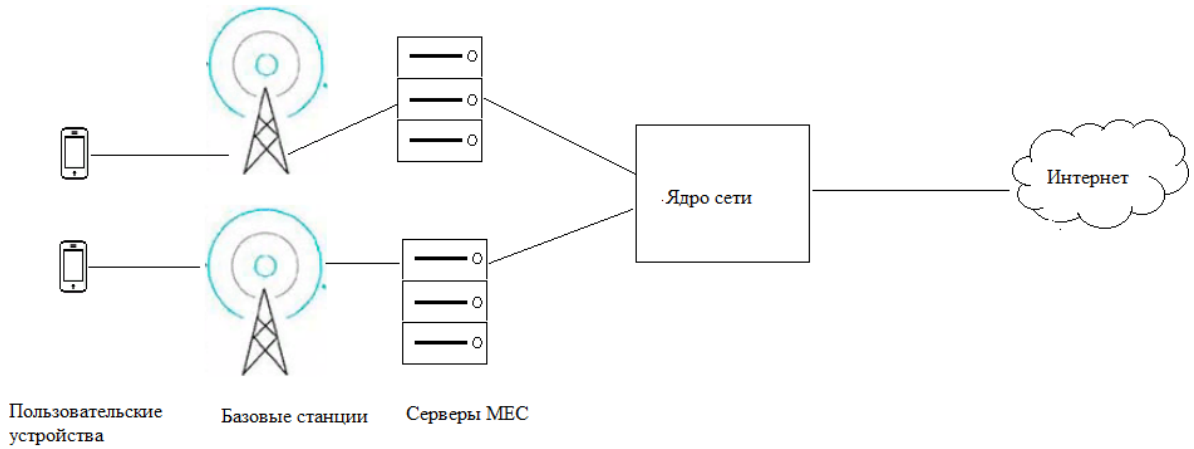


Рис. 1. Общая архитектура граничных вычислений (составлено автором)

Благодаря тому, что серверы MEC располагаются на границе сети радиодоступа (RAN) в пределах базовой станции или рядом с ней, это позволяет сократить системные задержки, что является одним из главных преимуществ при проектировке систем «умного города». К другим важным характеристикам относят:

1. Локальность.
2. Мобильность.
3. Знание контекстной информации.
4. Высокая пропускная способность [3].

Основные требования к «умному городу» с поддержкой граничных вычислений представлены на рис. 2 [2].

Рис. 2. Требования к умному городу с поддержкой граничных вычислений

Далее приводятся пояснения по каждому из элементов:

1. Масштабируемость и надежность – устойчивость к аппаратным сбоям, масштабируемое оборудование и ПО.
2. Совместимость – совместимые интерфейсы и фреймворки с открытым исходным кодом.
3. Безопасность – децентрализованная безопасность, кибербезопасность.
4. Эластичность – прогнозирование пользовательских интерфейсов.
5. Контекстная осведомленность – нагрузка и ёмкость сети, расположение умных устройств.
6. Управление ресурсами – адаптивное управление ресурсами.
7. Устойчивость – возобновляемые источники энергии, энергоэффективный дизайн.

Целью эксперимента являлась задача построить имитационную модель рассматриваемой архитектуры. Имитация работы производилась в программном комплексе AnyLogic. Модель состояла из следующих компонентов (рис. 3):

1. Устройства, генерирующее трафик.
2. Серверы MEC, расположенные на базовых станциях.
3. Облачный сервер (CS).
4. Пользователь, получающий данные.

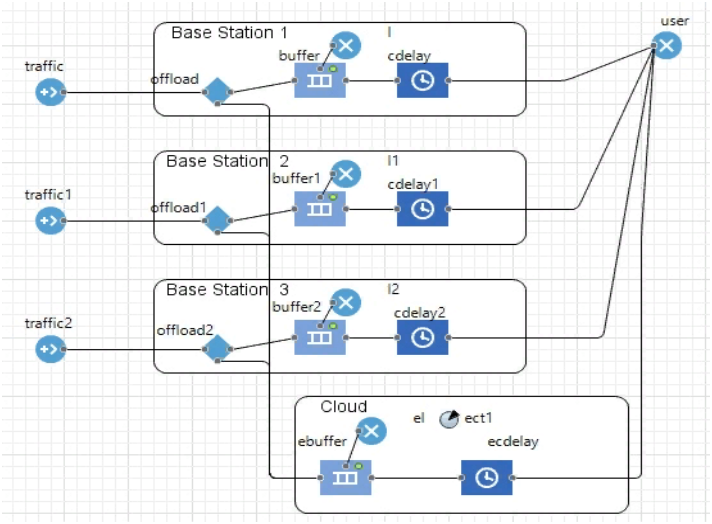


Рис. 3. Схема имитационной модели в программном комплексе Anylogic

Трафик, исходящий от устройства, представляет поток запросов, который поступает на сервер MEC. Каждый запрос может обслуживаться сервером MEC, может перенаправляться на CS или может быть потерян, если они оба слишком заняты. Предполагается, что один CS может обслуживать несколько серверов MEC. Сервер MEC описывается как сервисная система, которая обеспечивает выполнение некоторых запросов одновременно. Например, это может быть многоядерный процессор. Используются две основные модели: двухъядерный процессор для сервера MEC и восьмиядерный процессор для облачного сервера.

В данном эксперименте имитационная модель обладала следующими характеристиками:

1. Параметр p (задана от 0 до 1) – часть трафика, которая обслуживается сервером MEC. 1 – только сервером MEC, 0 – только CS.
2. Вместимость буфера равна 100.
3. Время обслуживания (задержки), распределено по экспоненциальному закону со средним значением 1 мс на базовой станции и 0,5 мс на CS

В процессе моделирования были собраны данные о задержке обработки запросов, потерях запросов и потреблении энергии и построены графики зависимости этих свойств от параметра *p* (рис. 4).

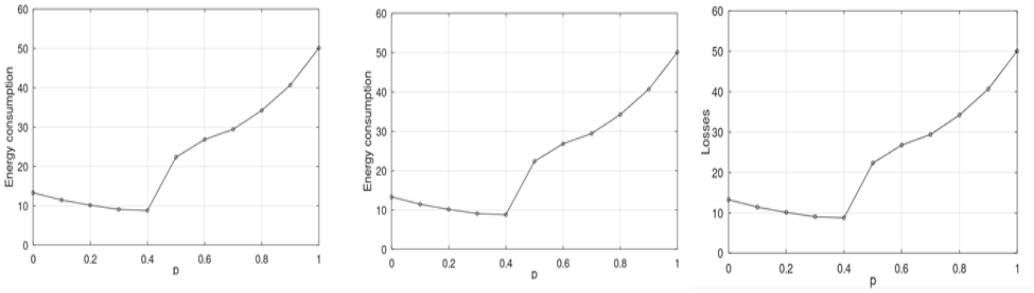


Рис. 4. Графики зависимости задержки обработки запросов, потерь запросов и потреблении энергии от параметра *p*

Результаты Эксперимента.

1. Минимальное значение задержки в точке $p = 0{,}4$. Зависимость потери пакетов имеет минимальное значение также в точке $p = 0{,}4$.

2. Понятно, что если весь трафик перенаправлен на CS ($p = 0$), то энергия, затраченная на обслуживание в сервере MEC, равна нулю. Увеличение доли трафика более 0,5 не влияет на энергопотребление, так как достигается максимальная загрузка сервера MEC.

Представленные результаты показывают, что задержка ответа и вероятность потерь зависит от части перенаправленного трафика. Мы видим, что может быть достигнуто оптимальное значение задержки и вероятности потерь путем выбора правильной части перенаправленного трафика. В свою очередь потребление энергии ниже, если доля перенаправленного трафика больше.

Список используемых источников

1. Strategy Analytics: Internet of Things Now Numbers 22 Billion Devices But Where Is The Revenue? [Электронный ресурс]. – Режим доступа: https://news.strategyanalytics.com/press-release/iot-ecosystem/strategy-analytics-internet-things-now-numbers-22-billion-devices-where. (дата обращения 10.01.2020).

2. Latif U. Khan, Ibrar Yaqoob, Nguyen H. Tran, S. M. Ahsan Kazmi, Tri Nguyen Dang, Choong Seon Hong, Edge Computing Enabled Smart Cities: A Comprehensive Survey [Электронный ресурс] // arXiv:1909.08747. 2019. 31 p. URL: https://www.researchgate.net/publication/335926328_Edge_Computing_Enabled_Smart_Cities_A_Comprehensive_Survey (дата обращения 15.01.2020).

3. Koustabh Dolui, Soumya Kanti Datta. Comparison of edge computing implementations: Fog computing, cloudlet and mobile edge computing. [Электронный ресурс] // Global Internet of Things Summit (GIoTS). 2017. 6 p. URL: https://ieeexplore.ieee.org/document/8016213 (дата обращения 20.01.2020).

4. Gabriel Brown. Mobile Edge Computing Use Cases & Deployment Options [Электронный ресур] // Heavy Reading White Paper 10 p. 2016 URL: https://www.juniper.net/assets/us/en/local/pdf/whitepapers/2000642-en.pdf (дата обращения 29.01.2020).

5. Ateya A. A., Muthanna A., Koucheryavy A. 5G framework based on multi-level edge computing with D2D enabled communication. В сборнике: 20th International Conference on Advanced Communication Technology (ICACT) conference proceedings. 2018. С. 507–512 (дата обращения 30.01.2020).

УДК 004.77
ГРНТИ 49.33.29

АНАЛИЗ МЕТОДОВ ПОСТРОЕНИЯ БЕСПИЛОТНЫХ АВТОМОБИЛЕЙ С ИСПОЛЬЗОВАНИЕМ СЕТЕВОЙ ПОДДЕРЖКИ

А. С. А. Мутханна, Н. А. Тагандурдыев

Санкт-Петербургский государственный университет телекоммуникаций им. проф. М. А. Бонч-Бруевича

Бурный рост мощности вычислительных машин и появление все новых передовых услуг и приложений приводит к огромному росту трафика сети по всему миру. Данное явление не обошло стороной и транспортную отрасль. С каждым годом появляется все больше современных приложений для автомобилей, призванные решить проблемы безопасности на дорогах, устранения пробок и обеспечения комфортной транспортной среды. Вместе с этим встает проблема выполнения требований к коммуникациям и вычислениям. Решить эти проблемы призваны технологии MEC и SDN, которые дадут толчок для развития концепции умных автомобильных сетей. MEC – технология вычисления «на месте», где вычислительные устройства находятся в непосредственной близости о источника информации, тем самым разгружая коммуникационную инфраструктуру. SDN также как и MEC снимет основную нагрузку с вычислительных устройств, разделив плоскости управления и передачи, а также даст больше возможности в гибкости и масштабируемости сети.

В данной статье производится анализ построения автомобильной сети на основе архитектуры MEC/SDN. Рассматриваются методы наиболее эффективного внедрения этих технологий для развертывания приложений и услуг IoT. Эта статья иллюстрирует функциональные особенности архитектуры транспортной сети будущего. Также показываются особенности взаимодействия автомобилей с сетевой инфраструктурой.

SDN, граничные вычисления, 5G, автомобильные сети, Интернет Вещей.

Введение

Сегодня Всемирной сетью пользуются 4,49 миллиарда человек, что составляет 58 процентов людей на Земле. Сильно растет и объем интернет трафика, что связано увеличением количества пользователей, цифровизацией всех отраслей глобальной экономики и увеличением спроса на «тяжелый контент». Как показывает исследование CISCO, в среднем трафик будет увеличиваться на 26 % каждый год. Также увеличивается и количество подключенных к Интернету устройств, количество которых к 2022 году по данным CISCO составит 28 млрд [1].

И конечно потенциал Интернета сейчас далеко не раскрыт. В настоящее время разрабатываются и обсуждаются различные концепции умного

дома, умного города, умного предприятия, тактильного взаимодействия через Интернет. Основой этих концепций является идея глобального взаимодействия всего и всех через Интернет – возможность подключения всего, что как-то может выиграть от подключения к глобальной сети.

Что нужно для реализации таких идей, чтобы концепции воплотились в реальность, а не просто оставались футуристичными проектами? Конечно, все это требует новых решений в телекоммуникационной сфере.

Основная часть

Для реализации проектов будущего необходимо реализовать услуги 5G – Embb, Mmtc, URLLC. Это создание сверхширокополосной мобильной связи (*Embb*), сверхнадежной связи с низкими задержками (URLLC) и поддержки массовой межмашинной связи (*Mmtc*). Все это является основной целью внедрения технологии 5G [2].

Сверхширокополосную связь подразумевает собой реализацию ультраширокополосной связи с целью передачи тяжелого контента. Массовая межмашинная связь подразумевает собой подключение к Интернету всего, что окружает человека, начиная от светофоров, бытовой техники до медицинского оборудования, автомобилей. Сверхнадежная межмашинная связь с низкими задержками необходима для реализации концепций Тактильного Интернета или других концепций, для которых важно понятие чувствительной задержки.

Одним из концепций, которую возможно будет воплотить в реальность благодаря услугам 5G, а именно услуге сверхнизких задержек, являются приложения беспилотных автомобилей. Ни для кого не секрет, что в настоящее время наблюдаются большие недостатки в автомобильно-транспортной сфере. Происходят огромное количество ДТП, до сих пор не решены вопросы распределения дорожного трафика на дорогах. Проблемы безопасности связаны с большой зависимостью от человеческого фактора, а проблемы с дорожным трафиком связаны с несовершенными алгоритмами распределения транспортной нагрузки.

Решить данные проблемы способны технологии 5G. 5G способно создать основу для создания приложений беспилотных автомобилей. То есть создать автомобильную среду, где обеспечивается безопасность, простота вождения и удобство.

Что собой представляет транспорт в автомобильной сети будущего? В этой сети транспортные средства будут обмениваться между собой (V2V) и с внешней инфраструктурой (V2I) огромным количеством данных [3]. Это данные, собираемые с GPS, камер, радаров, лидеров, которые ведут учет за состоянием дороги, транспорта, водителя и т. д. Для взаимодействия

с сетью транспортные средства будут оснащены устройствами, поддерживающие беспроводное взаимодействие (3GPP, IEE 802.11p, Bluetooth и т. д.) [4].

Как устроена сама сеть для поддержки беспилотных автомобилей? Существует два типа автомобильной связи в такой сети: V2V и V2I. Транспортные средства, придорожная инфраструктура могут собирать информацию об окружающей среде для обработки и обмена ею (в пределах досягаемости).

V2V означает прямое соединение между автомобилями. Такой вид взаимодействия позволяет обмениваться информацией между транспортными средствами независимо от инфраструктуры. Такая связь полезна для расширения дальности связи автомобильной сети. V2V позволяет обмениваться информацией между транспортными средствами и придорожными устройствами, когда они не находятся в зоне досягаемости друг друга. В течение всего этого процесса другие транспортные средства выступают в качестве посредников; они получают информацию и направляют ее для ввода в зону действия RSU. Но, тем не менее связь V2V относится к ограниченному диапазону. V2V используются для приложений дорожно-транспортных происшествий или приложений уличной парковки [3].

Но связью между автомобилями не обойтись, нужна связь с внешним миром. Поэтому организована связь V2I. Поскольку транспортные средства имеют ограниченные возможности обработки и хранения, большинство приложений будут использовать инфраструктуру в качестве платформы или промежуточного программного обеспечения. В некоторых случаях ожидается, что связь V2I обеспечит доступ к глобальной информации. Аналогичным образом, некоторые приложения могут извлекать информацию о погоде и заторах на дорогах через связь V2I [5].

Следует сказать, что существующая ныне архитектура сетей и инфраструктура не позволяет разворачивать приложения, реализующие такие услуги. Нынешняя сеть имеет огромные недостатки в вопросах обеспечения QoS. Приложения беспилотных автомобилей требует минимальных сетевых задержек, максимально быстрой обработки тяжелого трафика и взаимодействия огромного числа сетевых единиц.

Поэтому на рис. (см. ниже) предлагается архитектура, в которой реализуется идея граничных вычислений MEC и программно-конфигурируемых сетей SDN.

В настоящее время практически все данные обрабатываются в облаках, что является причиной огромных задержек. ЦОД-ы расположены достаточно далеко от конечных устройств. Поэтому пришла идея спустить вычислительные мощности от облаков к Fog и Edge – к географически распределенным вычислительным устройствам. Идея заключается в том, чтобы обрабатывать и хранить данные чувствительные к задержкам на границе

сети, тем самым уменьшая задержку сети и нагрузку на ядро сети. В облаке предлагается обрабатывать данные, не требующие вычислений в реальном времени. Эти данные необходимы для решений сложных вычислительных задач и данные, требующие облачного хранения. На уровне Fog-а обрабатывается данные, выходящие за возможности вычислительных возможностей границы.

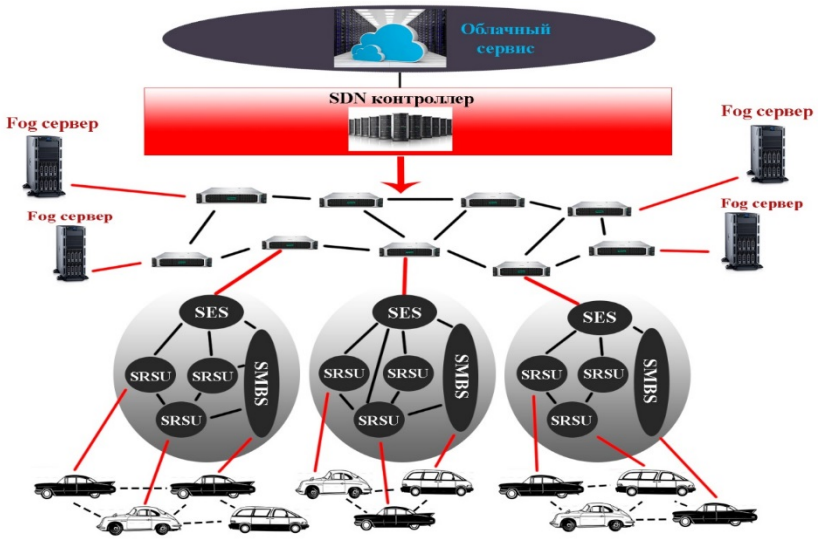


Рис. Архитектура автомобильной сети на основе технологий MEC/SDN

SDN отделит функции управления и функции физической передачи у маршрутизаторов, коммутаторов, снимая с них дополнительную нагрузку. SDN сделает сеть легко управляемой и программно-конфигурируемой, так как вся функция управления всей сетью будет реализована на программируемом контроллере. Применение SDN в гибридном режиме управления (делит функции контроллера с серверами Fog, SES, SMBS) дает положительный результат при решении задач оптимизации сети.

Таким образом, с помощью SDN, MEC и FOG будет возможно построить сеть с ультрамалыми задержками, что даст возможность реализовать идею беспилотных автомобилей.

Но конечно кроме преимуществ реализация данной архитектуры порождает и множество проблем, которые станут потенциальными задачами для возможности реализации приложений беспилотных автомобилей:

1. Распределение нагрузки. Сетевые устройства в периферийных вычислительных сетях имеют слабую вычислительную мощность. Поэтому встают задачи, которые требуют вычислений и балансировки нагрузки в соответствии с пропускной способностью оборудования пограничных сетей.

2. Безопасность и конфиденциальность. Конечные устройства более уязвимы для атак, чем централизованные устройства, так как облачные про-

вайдеры способны обеспечить более совершенную защиту данных. Облачный оператор организовывает и гарантирует шифрование, аварийное восстановление и качественную защиту от атак.

3. Маршрутизация и пересылка. Транспортные средства постоянно движутся с невероятной скоростью, поэтому трудно предсказать какое конкретное транспортное средство будет получать свои услуги от какой-либо из базовых станций или пограничных серверов. Необходима разработка алгоритмов прогнозирования местоположения транспорта.

4. Стоимость. Огромные денежные вложения для развертывания таких сетей.

5. Развертывание. Поскольку развертывание сетевого оборудования сопряжено с большими затратами, важно оптимально установить соответствующее количество сетевых элементов. Необходимо развернуть оборудование так, чтобы путь трафика проходил через меньшее количество устройств, но при этом удовлетворить все потребности транспорта в сетевой производительности.

Заключение

Реализация автомобильных сетей будущего представляют больший интерес, так как 5G в целом даст возможность построить автомобильную сеть, способную решить проблемы безопасности автомобильного движения, предотвращения пробок и равномерного распределения транспорта в сети, реализации приложений, предотвращающих аварии и уведомляющих об экстренных ситуациях и так далее. Создание такой умной сети создаст благоприятную среду для транспорта в целом. Такая сеть способна сделать транспортную среду максимально безопасной и комфортной. Все эти задачи недостижимы без технологий 5G.

Список используемых источников

1. Cisco Visual Networking Index (VNI) Complete Forecast Update. Available online: https://www.cisco.com/c/dam/m/en_us/network-intelligence/service-provider/digital-transformation/knowledge-network-webinars/pdfs/1213-business-services-ckn.pdf (accessed on 23 February 2020).

2. Услуги 5G [Электронный ресурс]. URL: http://1234g.ru/5g/uslugi-5g, режим доступа: свободный, дата обращения: 25.02.2020.

3. Raza, S., Wang Sh., Ahmed M., Anwar M. R. Survey on Vehicular Edge Computing: Architecture, Applications, Technical Issues, and Future Directions // Wireless Communications and Mobile Computing. 2019. Vol. 5. PP. 1–19.

4. Liu, S., Liu L., Yu B., Wang Y., Shi W. Edge Computing for Autonomous Driving: Opportunities and Challenges // PROCEEDINGS OF THE IEEE. 2019. Vol. 107. PP. 1–17.

5. Хакимов А. А, Суминов А. В., Мутханна А. С. А. Разработка метода организации распределения граничных вычислений в сетях VANET // Информационные технологии и телекоммуникации. 2019. Том 7. № 2. С. 47–55.

УДК 004.77
ГРНТИ 49.33.29

АНАЛИЗ МЕТОДОВ И РЕШЕНИЙ ПРИМЕНЕНИЯ ИНТЕРНЕТА ВЕЩЕЙ В СЕЛЬСКОХОЗЯЙСТВЕННОЙ ОТРАСЛИ

А. С. А. Мутханна, А. А. Хакимов, Ф. Ш. Шарофидинов

Санкт-Петербургский государственный университет телекоммуникаций им. проф. М. А. Бонч-Бруевича

Благодаря интернету вещей (Internet of Things) открылись новые оптимальные способы обработки почвы с использованием недорогого оборудования (датчики/актуаторы) и инфокоммуникационных технологий (интернет). Дистанционное управление и контроль, мониторинг состояния сельскохозяйственных культур, а также аналитика с целью прогнозирования погоды, будущего состояния культур или умная логистика и хранение урожая – вот некоторые примеры тех новых возможностей, которые открывают нам Интернет вещи. Несомненно, фермеры являются экспертами по сельскому хозяйству, но, тем не менее, далеко не каждый из них работал с устройствами Интернета вещей. Именно поэтому, исследователи, которые работают с IoT, должны участвовать в разработке, улучшая интеграцию и их использовании в данной отрасли. В этой статье проводится обзор и анализ решений и методов применения Интернета вещей в сельскохозяйственной отрасли, анализируются новые технологические решения, которые позволяют оптимизировать процесс производства в сельском хозяйстве.

интернет вещей (Internet of things), точное (прецизионное) земледелие, граничные(edge) и туманные (fog) вычисления.

Введение

Точное земледелие – это подход к управлению сельскохозяйственным объектом с помощью информационных технологий, дистанционного зондирования и непосредственного сбора, и обработки данных. Данный подход направлен на оптимизацию отдачи от вложенных ресурсов параллельно с потенциальным снижением уровня воздействия на окружающую среду. Такие данные, как температура почвы и окружающей среды, поливная вода и проводимость почвы, уровень кислотности (PH) почвы и оросительной воды, свойствах оросительной воды, о питательном составе почвы могут быть переданы и проанализированы с использованием коммуникационных технологий и парадигм искусственного интеллекта (ИИ) в режиме реального времени. Фермеры смогут с помощью их смартфона удаленно мониторить урожай и оборудования, а также анализировать некоторыми статистическими данными. Все эти технологии помогут построить концепцию точного (прецизионного) земледелия (рис. 1). В настоящее время фермеры

уже используют ресурсы, разработанные информационно-коммуникационными технологиями.

Рис. 1. Точное (прецизионное) земледелие (*Precision Agriculture* (PA))

В таблице показаны различные протоколы, используемые на уровнях архитектуры интернета вещей.

ТАБЛИЦА. Протоколы IoT

Уровни	Протоколы
Сеансовый/Приложения	MQTT, CoAP, AMQT, HTTP, SOAP, ...
Сеть	6LowPAN, RPL, CORPL, IPSec, TCP/UDP, DTLS
Восприятия/вещи	WiFi, Bluetooth Low Energy, Z-Wave, ZigBee, LoraWan, IEEE 802.15.4, LTE, …

Технологии интернета вещей, применяемые в сценариях точного земледелия

Прогресс в области электроники, вычислительной техники и телекоммуникаций позволяет разрабатывать новые устройства (датчики, исполнительные механизмы и вычислительные узлы) с возможностями беспроводной связи, устанавливаемые в любом месте, меньшие по размеру, энергоэффективные, автономные, более мощные и недорогие [1]. Недорогие устройства IoT, которые должны собирать и передавать данные датчиков и получать удаленные команды, показаны в [2, 3]. Обзор наиболее распространенных проводных и беспроводных протоколов связи, обсуждение их характеристик, преимуществ и недостатков, а также сравнительное исследование для выбора наилучшей двунаправленной сенсорной сети, состоящей из маломощных устройств, реализовано в [4]. Вышеперечисленные работы показывают степень развития технологии IoT, которая также была испытана в точном земледелии в последние годы.

Технологии Интернета вещей предлагаются в разных сценариях точного земледелия. В работе [5] эта парадигма анализируется как решение проблемы точного земледелия. Приложение IoT Smart farming включает в себя отслеживание параметров фермы, мониторинг, наблюдение за полем и мониторинг хранения продуктов производства. Рабочая платформа «Интернет вещей для интеллектуального фермерства» (IoT *Platform for Smart Farming*) [6], основанная на технологиях IoT, может автоматизировать сбор данных об окружающей среде, почве, удобрениях и ирригации; автоматически сопоставлять такие данные и отфильтровывать неверные данные с точки зрения оценки урожайности; рассчитать прогнозы урожая и персональные рекомендации по урожаю для любой конкретной фермы. Эта платформа (*SmartFarmNet*) может интегрировать практически любое устройство Интернета вещей, включая имеющиеся в продаже датчики, камеры, метеостанции и т. д. и хранить эти данные в облаке с целью анализа производительности для дальнейших рекомендаций.

В заключение статьи [6] дается оценка платформы Smart Farm Net, а также опыта и уроков, извлеченных при разработке этой системы. Smart Farm Net является первой и в настоящее время крупнейшей системой в мире, которая предоставляет анализ производительности и рекомендации по выращиванию сельскохозяйственных культур.

В работе [7] была спроектирована, разработана и испытана теплица с гидропонным растениеводством с использованием всепроникающей сенсорной сети мониторинга и управления в парадигме Интернета вещей. Экспериментальные результаты показали, что интернет-технологии и модели коммуникации умных объектов могут быть объединены для стимулирования развития точного земледелия. Они продемонстрировали дополнитель-

ные преимущества при запуске проекта, а именно: стоимость, энергия, интеллектуальное развитие, признание специалистами сельского хозяйства. Другая связанная с этим работа показана в работе [8] с технологией ZigBee: были разработаны методы с использованием искусственного интеллекта и функцией поддержки принятия решений. В данной работе разрабатываются технологии мониторинга влажности и наличия питательных веществ в почве при выращивании цитрусовых в режиме реального времени и проводятся исследования по интеграции системы поддержки принятия решений по удобрению и орошению. Результаты показали, что система может помочь производителю оптимально и научно удобрять или орошать, повысить точность работы производства цитрусовых, снизить затраты и уменьшить загрязнение, вызванное химическими удобрениями.

В работе [9] предлагается метод проектирования прецизионного земледелия с использованием архитектуры распределенных вычислений в контексте Интернета вещей. Принцип работы и различные интеллектуальные процессы реализованы с использованием распределенной модели, основанной на парадигмах граничного (*edge*) и туманного (*fog*) вычислений. В данной работе авторы предлагают ориентированный на пользователя метод проектирования интеллектуальных и адаптированных сервисов, где каждый фермер решает свою собственную установку.

Интернет вещей (IoT) направлен на то, чтобы привести в действие каждый объект (например, умные камеры, датчики окружающей среды, приборы управления, анализ машинного обучения), таким образом генерируя огромные объемы данных, которые могут подавить системы хранения и приложения для анализа данных. Облачные вычисления предлагают услуги на уровне инфраструктуры, которые могут масштабироваться в соответствии с требованиями к хранению и обработке данных в Интернете вещей. Однако, существуют такие функционалы, как сенсорный мониторинг, контроль и анализ, которые требуют низкой задержки, поэтому задержка, вызванная передачей данных в облако, а затем обратно в приложение, может серьезно повлиять на их производительность. Чтобы преодолеть это ограничение, авторами были предложены парадигмы туманных и граничных вычислений, в которых облачные сервисы расширяются до края сети, чтобы уменьшить задержку и перегрузку сети. На рис. 2 (см. ниже) более подробно описаны задачи, которые решают тот или иной уровень. Как туманные, так и граничные вычисления предполагают смещение интеллектуальных и вычислительных возможностей ближе к источникам данных, которые исходят от насосов, двигателей, датчиков, реле и т. д.

Точное земледелие-это набор методов, подходов и инструментов, которые фермеры должны детально изучить, чтобы решить, какой из них наиболее подходит для их фермы.

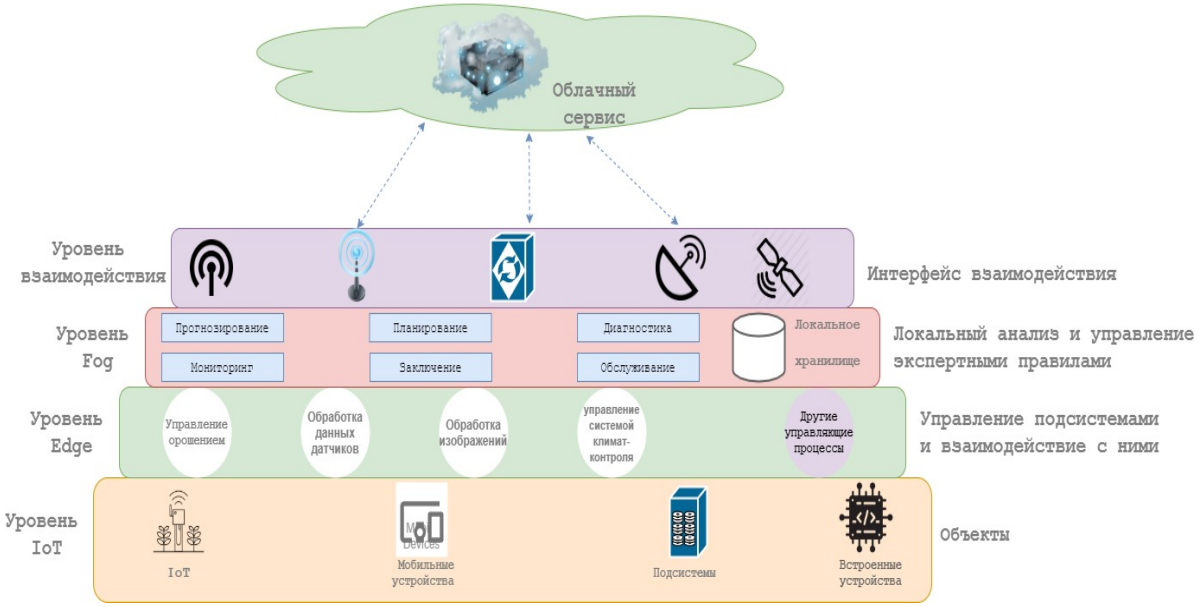


Рис. 2. Архитектура: коммуникационные уровни с различной функциональностью

Вывод

Ведется активное исследование, и разрабатываются прототипы систем для умного сельского хозяйства. Это является жизненно важной необходимостью для всего человечества из-за глобального роста населения Земли и активного развития процесса урбанизации, что говорит о значительном снижении доли населения, которая занимается сельским хозяйством. Но благодаря IoT стало возможным предотвратить глобальные вызовы в сфере продовольственной и биологической безопасности.

Список используемых источников

1. IoT-Now-Mag. The Industrial Internet: Towards the 4th Industrial Revolution. 2016 [Электронный ресурс]. URL: https://www.iot-now.com/2016/10/20/53811-the-industrial-internet-towards-the-4th-industrial-revolution (дата посещения 17.01.2020).

2. Ilchev, S., Ilcheva, Z. Internet-of-Things Communication Protocol for Low-Cost Devices in Heterogeneous Wireless Networks // In Proceedings of the 18th International Conference on Computer Systems and Technologies, Ruse, Bulgaria, 23–24 June 2017; PP. 272–279.

3. Sivanathan, A.; Sherratt, D.; Gharakheili, H.H.; Sivaraman, V.; Vishwanath, A. Low-cost flow-based security solutions for smart-home IoT devices // In Proceedings of the 2016 IEEE International Conference on Advanced Networks and Telecommunications Systems (ANTS), Bangalore, India, 6–9 November 2016; PP. 1–6.

4. Cercas, F.; Souto, N. M. B. Comparison of communication protocols for low cost Internet of Things devices // In Proceedings of the 2017 South Eastern European Design Automation, Computer Engineering, Computer Networks and Social Media Conference (SEEDA-CECNSM), Kastoria, Greece, 25–27 September 2017; PP. 1–6

5. Tech-Target. IoT as a Solution for Precision Farming. 2017 [Электронный ресурс]. URL: http://internetofthingsagenda. techtarget.com/blog/IoT-Agenda/IoT-as-a-solution-for-precision-farming (дата посещения 18.01.2020).

6. Jayaraman, P. P.; Yavari, A.; Georgakopoulos, D.; Morshed, A.; Zaslavsky, A. Internet of Things Platform for Smart Farming: Experiences and Lessons Learnt // Sensors 2016, 16, 884.

7. Ferrandez-Pastor, F. J.; Garcia-Chamizo, J. M.; Nieto-Hidalgo, M.; Mora-Pascual, J.; Mora-Martinez, J. Developing Ubiquitous Sensor Network Platform Using Internet of Things: Application in Precision Agriculture. Sensors 2016, 16, 1141.

8. Zhang, X.; Zhang, J.; Li, L.; Zhang, Y.; Yang, G. Monitoring Citrus Soil Moisture and Nutrients Using an IoT Based System. Sensors 2017, 17, 447.

9. Francisco Javier Ferrández-Pastor; Juan Manuel García-Chamizo; Mario Nieto-Hidalgo; José Mora-Martínez. Precision Agriculture Design Method Using a Distributed Computing Architecture on Internet of Things Context. Sensors 2018; 18; 1731.

УДК 681.324
ГРНТИ 49.33.29

МОДЕЛИРОВАНИЕ ОПЕРАТИВНОСТИ ЦЕНТРА ОБРАБОТКИ ДАННЫХ С СЕРВЕРОМ БАЗЫ ДАННЫХ

Д. Э. Нугзаров, О. И. Пантюхин, Г. А. Рябов, К. М. Швецов

Санкт-Петербургский государственный университет телекоммуникаций им. проф. М. А. Бонч-Бруевича

В статье рассматриваются возможности моделирования оперативности выполнения запросов для центра обработки данных с сервером базы данных. Моделирование – это метод, позволяющий описывать процессы так, как они происходили бы в действительности. Моделирование используется в разных областях, в частности для проверки характеристик оперативности компонентов автоматизированных систем, таких как ЭВМ, каналы передачи данных, компьютерные сети и центры обработки данных.

центр обработки данных, автоматизированная система, имитационное моделирование.

Поставщики информационных и облачных услуг используют для создания своих предложений сетевые технологии и системы обработки и хранения данных. Для выполнения широкого спектра требований к облачным системам необходимы центры обработки данных (ЦОД), разные типы серверов, сетей и устройств хранения баз данных. Гарантом работоспособности ЦОД, от которой зависит работа всей автоматизированной системы в целом, является правильно организованная инженерная инфраструктура [1]. Такую инфраструктуру на начальных этапах проектирования ЦОД подбирают по результатам моделирования.

Современные ЦОД являются, в сущности, ядром информационно-телекоммуникационной инфраструктуры сложных организационно-технических систем. Они представляют собой комплекс инженерной инфраструктуры, программных и аппаратных средств, организационных процедур и человеческих ресурсов. Центры предназначены для приёма, хранения, обработки и предоставления данных должностным лицам (ДЛ) сложных организационно-технических систем с требуемым уровнем качества. Центры обработки данных содержат высоконадежное серверное оборудование, системы хранения и передачи данных, программное обеспечение, архитектурно-технические решения, обеспечивающую инженерную инфраструктуру, физическую защиту помещений, комплекс организационных мероприятий, а также систему мониторинга и управления [2, 3].

Современный ЦОД широкого назначения – комплексная система управления и консолидированной обработки информации, объединяющая вычислительные, инженерные, электронные и коммуникационные системы. Эта система масштабируемая и унифицированная, что позволяет правильно хранить и обрабатывать весь необходимый для должностных лиц и автоматизированных систем (АС) массив информации [2, 4].

Таким образом, основными компонентами ЦОД являются:

- сетевая инфраструктура или локальная вычислительная сеть (ЛВС), которая объединяет серверы и системы хранения данных ЦОД, обеспечивает внешние подключения к автоматизированным рабочим местам (АРМ) или ЭВМ конечных пользователей;
- инфраструктура хранения, предоставляющая массивы хранения данных (базы данных) ЦОД;
- вычислительные ресурсы, то есть серверы, поддерживающие работу приложений ЦОД. Эти серверы предоставляют ресурсы памяти и место в локальном хранилище, выполняют обработку приложений и обеспечивают их подключение к сети;
- вспомогательные службы.

Проектирование ЦОД, как и проектирование любых крупных АС, предполагает выполнение ряда стадий, содержащих, в свою очередь, набор конкретных задач, нацеленных на создание центров с высоким качеством обслуживания. В нашей стране разработана система стандартов, определяющих содержание, состав исполнителей и порядок выполнения работ на разных этапах проектирования, а также порядок их приёмки. Государственный стандарт ГОСТ 34.601-90, например, содержит нормативные требования к содержанию стадий и задач проектирования автоматизированных систем, предназначенных для обеспечения различных видов деятельности (управление, проектирование, исследование и т. п.), включая их сочетания. Он предусматривает следующие стадии и задачи проектирования:

формирование требований к ЦОД, разработка концепции, техническое задание на создание ЦОД, эскизный и технический проект построения ЦОД, разработка рабочей документации, ввод в действие и сопровождения ЦОД.

При предпроектном обследовании объекта, в рамках которого будет функционировать ЦОД сложной организационно-технической системы, производится: сбор и обработка сведений об этой инфраструктуре (системе), особенностях её функционирования, включая данные о её взаимодействии с внешней средой и другими системами, а также выполнение процедур системного анализа и моделирования, разработка технико-экономического обоснования целесообразности создания ЦОД, выработка общих требований на его разработку и другие работы [2].

Одним из основных свойств и показателей качества функционирования ЦОД и ЛВС является их оперативность, так как именно она комплексно отражает их целевое предназначение и учитывает влияние внутренних и внешних дестабилизирующих факторов. К внутренним относятся конечная надежность средств вычислительной техники (вероятность отказа) и ошибочные действия ДЛ (вероятность ошибки), а к внешним, например, дестабилизирующее влияние вредоносного программного обеспечения [5].

От оперативности и надежности обработки информации во многих АС зависит построение информационных процессов и уровень оказания услуг потребителям. Под информационным процессом при решении задач в автоматизированных системах понимается согласованная по месту, времени и целям совокупность подпроцессов подготовки и ввода данных, проверки их на достоверность, классификации, обобщения и группирования, а также хранения поступающей информации, поиска и выдачи данных в форме, необходимой для использования при принятии решений, решении задач различных типов по функциям управления, оформления результатов в виде документов, команд или сигналов, их доведения до взаимодействующих объектов [6].

Хранение введённых в АС данных осуществляется при реализации подпроцесса хранения информации. При этом данные размещаются в базе данных, как правило, распределенной, обеспечивая тем самым: надёжность, безизбыточность, целостность и непротиворечивость хранения данных; достоверность и безопасность данных; возможность манипулирования данными (чтение, запись, изменение, удаление).

При проектировании и исследовании автоматизированных систем и комплексов средств автоматизации широко применяется имитационное моделирование с применением ЭВМ [5]. Для повышения эффективности процесса моделирования применяются специализированные средства и языки имитационного моделирования, ориентированные на конкретные объекты исследования. При моделировании АС для расчёта значений вероятностно-временных показателей оперативности и надёжности эти системы

сводятся к системам и сетям массового обслуживания (СМО, СеМО). Наиболее приспособленным средствами описания СМО являются такие инструментальные средства, как GPSS-World и AnyLogic.

Моделирование – это процесс воспроизведения и исследования определённого фрагмента действительности или управления им, основанный на представлении объекта с помощью его копии или подобия – модели. Модель обычно представляет собой либо материальную копию оригинала, либо некоторый условный образ, представленный в абстрактной форме и содержащий существенные свойства моделируемого объекта. Процедуры создания моделей широко используются как в научно-теоретических, так и в прикладных сферах человеческой деятельности.

Целью имитационного моделирования является получение приближённых знаний об объекте, не производя непосредственное измерение значений его параметров. Понятно, что это необходимо только тогда, когда измерение невозможно, или оно стоит дороже проведения имитации. При этом результаты будут определяться случайным характером процессов. По этим данным можно получить достаточно устойчивую статистику. Имитационное моделирование можно рассматривать как разновидность экспериментальных испытаний.

На основе результатов анализа информационных потребностей ДЛ АС, сделан выбор в сторону имитационного моделирования и теории массового обслуживания. Основными этапами методики оценки оперативности ЦОД являются [5]:

оценка информационной потребности пользователей при использовании ЦОД;

разработка модели оценки оперативности;

собственно, моделирование с учетом воздействия внутренних и внешних дестабилизирующих факторов.

Ядром методики является имитационная модель оценки оперативности, позволяющая определить показатель оперативности обработки сообщений, циркулирующих в АС с ЦОД и сравнить его значения с требуемыми.

Большинство компонентов АС имеет сложную структуру и характеризуется многообразием связей между элементами. В качестве компонентов можно привести персональные ЭВМ, АРМ, центры обработки данных, комплексы средств автоматизации, компьютерные сети (сети передачи данных) и др.

Возвращаясь к примеру, с ЦОД и подключёнными к нему АРМ, можно сказать, что пользователи выступают в роли источника потока запросов на выполнение задач (заявок) на сервере базы данных. Заявки, поступающие в случайные моменты времени, образуют входной поток заявок. АРМ, канал передачи данных и сервера ЦОД интерпретируются обслуживающими приборами. Заявки, которые не могут быть приняты к обслуживанию, образуют

очередь. Результаты решения задач формируются в выходной поток заявок. Результатом исследования, как правило, выступают временные характеристики процесса пребывания заявки в отдельных СМО и сети в целом.

В разрабатываемой модели с каждой АРМ пользователи могут формировать два типа запросов к базе данных (БД), ведущейся на сервере ЦОД: запросы на выдачу данных из БД (тип 1); запросы на корректировку данных в БД (тип 2). Названные типы запросов отличаются маршрутами их выполнения. Запросы типа 1 формируются на АРМ пользователей, передаются по каналам передачи данных, обрабатываются на сервере и результаты поступают по каналам передачи данных на пользовательские АРМ, где преобразуются в форму, удобную для пользователей. Запросы типа 2 также формируются на АРМ, передаются по каналам передачи данных и обрабатываются на сервере с БД. На этом их исполнение завершается.

Процесс имитации прохождения заявок в такой СеМО, можно представить последовательностью действий, называемой моделирующим алгоритмом. Схема СеМО, интерпретирующей ЦОД, представляется определённой структурой СМО.

Список используемых источников

1. Бородко А. В., Пантюхин О. И. Реализация облачных систем хранения на основе центров обработки данных // Интернет вещей и 5G (INTHITEN 2017). 3-я МНТК студентов, аспирантов и молодых ученых. СПб. : СПбГУТ, 2017. С. 62–67.

2. Бородко А. В., Пантюхин О. И. Анализ содержания типовых стадий и задач проектирования современных центров обработки данных специального назначения // Проблемы технического обеспечения войск в современных условиях. Труды IV межвузовской научно-практической конференции. СПб. : ВАС, 2019. С. 127–131.

3. Трикоз А. С. Строим ЦОД: рекомендации заказчика // ЦОДы РФ. Проектирование, строительство, эксплуатация. 2015. № 11. С. 37–44.

4. Кусакин Д. Г. Строим ЦОД: проектируем ЦОД // ЦОДы РФ. Проектирование, строительство, эксплуатация. 2015. № 9. С. 53–59.

5. Борец Д. В., Ковалёв И. С., Малышев В. С., Пантюхин О. И. Оценка оперативности локальной вычислительной сети пункта управления силового ведомства // Информационная безопасность регионов России (ИБРР-2017). Материалы юбилейной X межрегиональной конференции. 1–3 нояб. 2017г. СПОИСУ. – СПб, 2017. С.52–53.

6. Овсянников С. Н., Пантюхин О. И., Хмелевской В. П. Организация информационного процесса в системе автоматизации управления связью // Актуальные проблемы инфотелекоммуникаций в науке и образовании (АПИНО-2017). VI Международная научно-техническая и научно-методическая конференция : сб. науч. ст. в 4-х т. СПб. : СПбГУТ, 2017. Т. 1. С. 502–507.

УДК 004.75
ГРНТИ 50.39.02

АНАЛИЗ ПРИМЕНЕНИЯ ПРОГРАММНО-ОПРЕДЕЛЯЕМЫХ СЕТЕЙ SDN В УСЛОВИЯХ ПЕРЕХОДА К ЦИФРОВОЙ ЭКОНОМИКЕ

С. А. Объедков, О. Н. Пантелеева, Д. С. Савельев, С. Н. Савельев

Академия Федеральной службы охраны Российской Федерации

Программно-определяемые сети, как платформы предоставления сетевых услуг, приобретают все большую популярность в условиях перехода к цифровой экономике благодаря тому, что они позволяют операторам и предприятиям получать беспрецедентную программируемость, автоматизацию и управление, что позволяет создавать масштабируемые, гибкие сети, не требующие отдельной настройки каждого конкретного устройства, и, легко адаптирующиеся под требования заказчика.

программно-определяемые сети, цифровая экономика.

В июле 2017 года была принята Программа развития цифровой экономики в России. Особое внимание в ней уделяется развитию компьютерного и телекоммуникационного оборудования и цифровых технологий. Развитие цифровой экономики формирует потребность в новой сетевой архитектуре. Некоторые из ключевых тенденций, определяющих необходимость новой сетевой архитектуры, включают [1]:

– изменение структуры трафика, поскольку к нему требуется доступ с любого устройства сети в любое время. Современные приложения, в отличие от клиент-серверных, в процессе работы обращаются к различным базам данных и серверам, создавая большие потоки данных;

– возрастание использования информационных технологий. Пользователи стали чаще использовать персональные устройства для доступа к корпоративной среде. Вследствие этого требуется улучшенная защита корпоративных данных и интеллектуальной собственности;

– рост количества и объема облачных хранилищ. Предприятия разного рода чаще стали использовать возможность доступа к приложениям, инфраструктуре и другим ИТ-ресурсам при помощи облачных хранилищ. Вследствие этого произошел беспрецедентный рост облачных услуг;

– обработка большого количества данных требует параллельной обработки на большом количестве серверов, требующих прямых коммутаций между собой. В связи с этим, управление сетью требует постоянной оптимизации ее масштабирования;

– сложность архитектуры. Например, чтобы добавить или переместить любое устройство, необходимо организовать взаимодействие с несколькими коммутаторами, маршрутизаторами, брандмауэрами, порталами веб-аутентификации и т.д. Кроме того, в существующих сетях, необходимо учитывать топологию сети, модель коммутатора и версию программного обеспечения. Из-за данной сложности существующие сети относительно статичны, поскольку они стремятся свести к минимуму риск нарушения обслуживания;

– потребность в большом количестве времени для перенастройки списков управления доступом по всей сети, т. е. несогласованные политики, что делает существующие сети уязвимым к нарушениям правил безопасности;

– невозможность роста сети, т. к. с увеличением количества сетевых устройств, возрастают требования к их настройке и управлению.

Решением данных проблем может послужить создание программно-определяемых сетей (SDN – *Software-Defined Networking*), с помощью которых процесс управления сетью становится более простым. Программно-определяемая сеть – это сетевая архитектура, в которой осуществляется программное управление сетью, при котором управление переадресовывается в доступные сетевые устройства, что позволяет рассматривать сеть как виртуальную или программно-определяемую [2].

Программно-определяемые сети ориентированы на отделение плоскости управления, в которой непосредственно принимаются решения о пути прохождения пакетов через сеть, от плоскости данных, которая в свою очередь перемещает пакеты. В результате операторы и предприятия получают беспрецедентную программируемость и адаптивность сетей под, требования заказчика. Технология SDN предоставляет возможность автоматизированного управления всей сетью с одного устройства, то есть администратор может формировать трафик с консоли централизованного управления, не касаясь отдельных коммутаторов в сети. В сравнении с традиционными сетями, где сетевые устройства принимают решение согласно заранее определенным таблицам маршрутизации, в SDN не требуется отдельной настройки каждого конкретного устройства. Таким образом, SDN представляет собой расширяемую платформу представления услуг, способную быстро реагировать на меняющиеся потребности цифровой экономики.

На рис. показана архитектура программно-определяемых сетей. Программные контроллеры содержат информацию о структуре сети, представляющей собой совокупность приложений и механизмов политик как единого логического коммутатора. С помощью программно-определяемых сетей операторы связи получают независимый от поставщика контроль над всей сетью из одной логической точки, что значительно упрощает проектирование и эксплуатацию сети.

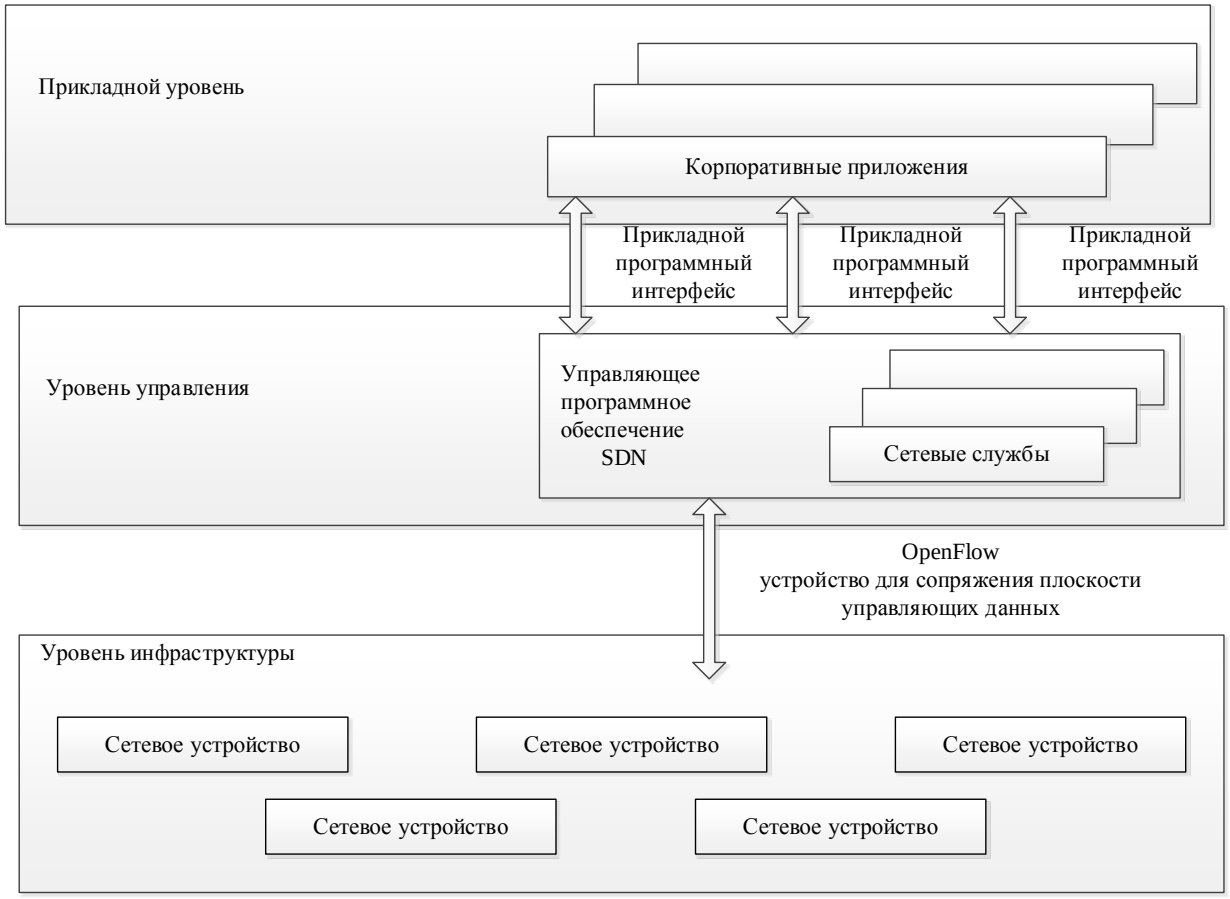


Рис. Архитектура программно-определяемых сетей

Программно-определяемые сети и связанные с ними стандарты эффективно удовлетворяют потребности сетевых операторов в каждом сегменте рынка, в том числе возможны следующие варианты их использования [3]:

– кампус – модель централизованного, автоматизированного управления и подготовки SDN. Она поддерживает конвергенцию данных, голоса и видео, а также доступ в любое время и в любом месте, позволяя ей последовательно применять политики, как в проводной, так и в беспроводной инфраструктуре. Кроме того, SDN поддерживает автоматизированную подготовку и управление сетевыми ресурсами, определяемыми индивидуальными профилями пользователей и требованиями приложений, чтобы обеспечить оптимальный пользовательский интерфейс в рамках ограничений предприятия;

– центр обработки данных. Архитектура SDN облегчает виртуализацию сети, что обеспечивает высокую масштабируемость в центре обработки данных, автоматизированную миграцию виртуальных машин, более тесную интеграцию с хранилищем, лучшее использование сервера, более низкое энергопотребление и оптимизацию пропускной способности;

– облако – независимо от использования SDN для поддержки частной или гибридной облачной среды, позволяет распределять сетевые ресурсы выгодным способом, обеспечивая быструю подготовку облачных служб и более гибкую передачу данных внешнему поставщику облачных услуг. С помощью инструментов для безопасного управления своими виртуальными сетями, предприятия и бизнес-единицы будут чаще использовать облачные службы.

Технология SDN улучшает управляемость сети, масштабируемость, ее гибкость, способствует виртуализации сети, позволяя ИТ-персоналу управлять серверами, хранилищем, приложениями и сетями с помощью общего универсального подхода и набора инструментов, как в среде оператора, так и в корпоративном центре обработки данных [4].

Развитием SDN занимается Фонд открытых сетей (ONF), который интегрирует вокруг проекта разработчиков приложений, программного обеспечения, производителей цифровых систем и цифровой элементной базы, компьютерные компании и поставщиков инфокоммуникационных услуг. Разработанный Фондом открытых сетей протокол OpenFlow уже включен в ряд инфраструктурных проектов, как физических, так и виртуальных, а также в программное обеспечение контроллеров сетей SDN. Сетевые службы и бизнес-приложения уже взаимодействуют с контроллерами SDN, обеспечивая лучшую интеграцию и координацию между ними [5].

Внедрение программно-определяемых сетей обещает превратить сегодняшние статические сети в гибкие, программируемые интеллектуальные платформы с динамическим распределением ресурсов, с поддержкой высокоавтоматизированных и безопасных облачных сред.

Список используемых источников

1. SDN: Transforming networking to accelerate business agility [Электронный ресурс]. URL: http://opennetsummit.org/archives/mar14/site/why-sdn.html (дата обращения 02.10.2019).

2. Ranjan P. A Survey of Past, Present and Future of Software Defined Networking. Vol. 7782, pp. 238–248, 2014.

3. Lopez L., Reid A., Manzalini A., Odinin M-P. Impact of SDN/NFV on Business Models. IEEE Software Defined Networks [Электронный ресурс]. URL: http://sdn.ieee.org/newsletter/january-2016/impact-of-sdn-nfv-on-business-models/ (дата обращения 29.09.2019).

4. ONF Open networking foundation [Электронный ресурс]. URL: https://www.opennetworking.org/images/stories/downloads/about/onf-what-why-2016.pdf (дата обращения 11.11.2019).

5. W. Braun and M. Menth. Software-Defined Networking Using OpenFlow: Protocols, Applications and Architectural Design Choices // Futur. Internet, vol. 6, no. 2, pp. 302–336, May 2014.

УДК 621.391.812.3
МРНТИ 49.31.01

ЭФФЕКТ ЗАМИРАНИЙ В МНОГОЛУЧЕВОМ КАНАЛЕ СВЯЗИ

Г. В. Овечкин[1], М. А. Сексембаева[2], Н. Н. Ташатов[2]

[1]Рязанский государственный радиотехнический университет
[2]Евразийский национальный университет имени Л. Н. Гумилева

В данной работе изучен механизм формирования мелкомасштабных замираний и их описание с помощью распределений Накагами, Райса и Релея, средняя продолжительность замираний.

многолучевой канал, модель цифрового канала связи, мелкомасштабное замирание, средняя продолжительность замираний/

Запишем передаваемый сигнал в комплексной форме (1):

$$s(t) = \mathrm{Re}\left\{u(t)e^{2\pi j\, f_c t}\right\}, \quad (1)$$

где f_c – несущая частота.

Низкочастотный сигнал $u(t)$ называют *комплексной огибающей* $s(t)$, имеющей вид:

$$u(t) = |u(t)|e^{j\varphi(t)} = R(t)e^{j\varphi(t)},$$

где $R(t) = |u(t)|$ – модуль огибающей, $\varphi(t)$ – фаза огибающей. Для чистого фазово- или частотно-модулированного сигнала $R(t) = \mathrm{const}$; в общем случае $R(t)$ медленно меняется по сравнению с $t_c = 1/f_c$.

Принимаемый сигнал будет иметь такую же форму, но с добавлением шумовой составляющей:

$$r(t) = \mathrm{Re}\left\{v(t)e^{2\pi j f_c t}\right\} + n(t),$$

Где $n(t)$ – шум, вносимый каналом, а $v(t)$ – эквивалентный низкочастотный сигнал, зависящий от канала связи.

Многолучевое распространение сигнала приводит к появлению замираний, поскольку амплитуда или фаза сигнала, переданного через канал, являются случайными величинами. На рис. 1 (см. ниже) показан механизм возникновения замираний при интерференции двух лучей: прямого и отражённого от поверхности земли.

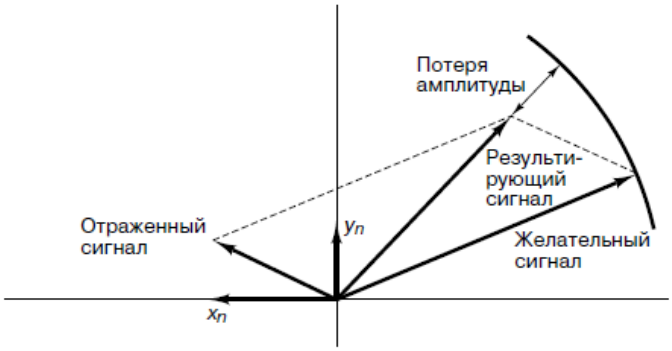


Рис. 1. Механизм возникновения замираний [1, с. 972]

Отражённый сигнал запаздывает по фазе, поскольку расстояние его распространения больше; также, он имеет меньшую амплитуду, т. к. частично поглощается при отражении. В результате суммарный принятый сигнал имеет большую фазу и меньшую амплитуду, чем передаваемый.

Различные проявления эффектов замирания в каналах показаны на диаграмме, рис. 2.

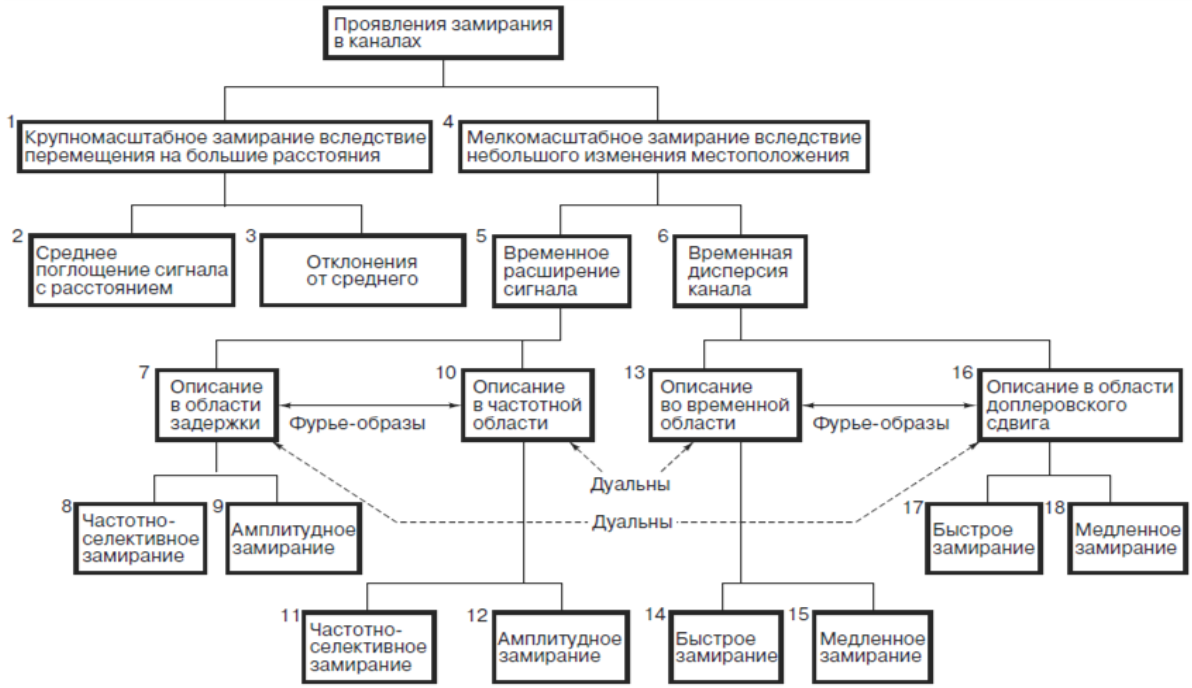


Рис. 2. Проявления эффекта замирания в каналах связи [1, с.963]

В среде с замиранием модифицированный низкочастотный сигнал можно записать в виде $\alpha(t)e^{-i\Theta(t)}g(t)$. Амплитуду $\alpha(t)R(t)$ соответствующей огибающей можно выразить через три положительных множителя (2):

$$\alpha(t)R(t) = m(t) \times r_0(t) \times R(t), \quad (2)$$

где $m(t)$ – компонента *крупномасштабного замирания* огибающей; $r_0(t)$ – компонента *мелкомасштабного замирания* (или замирание вследствие многолучевого распространения, или релеевское замирание) [1, с. 967].

На рис. 3 кривая $\alpha(t)$ наглядно демонстрирует суперпозицию мелкомасштабных и крупномасштабных замираний.

Исторически одним из первых описаний крупномасштабных замираний были графики, полученные Окумурой (Okumura, 1968). В результате аппроксимации этих кривых появилась аналитическая модель Хаты (Hata, 1980), согласно которой потери в тракте $P_r(d)$ в зависимости от расстояния d между передатчиком и приёмником, выраженного в единицах эталонного расстояния d_0:

$$P_r(d)(\text{дБ}) = P_t(d_0)(\text{дБ}) + 10n \lg \frac{d}{d_0} + X_\sigma, (\text{дБ}).$$

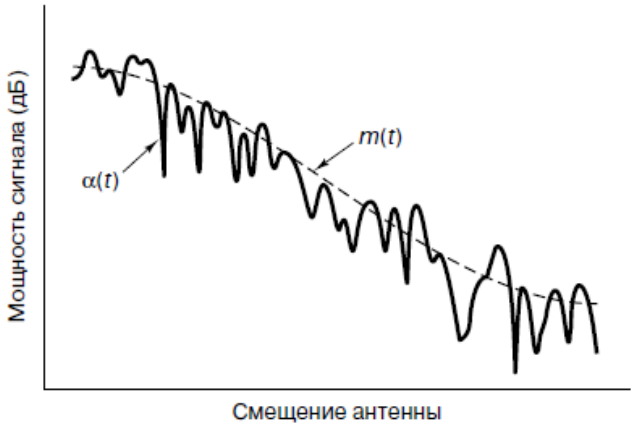


Рис. 3. $\alpha(t)$ – суперпозиция крупномасштабных и мелкомасштабных замираний

Эталонное расстояние d_0 соответствует точке, находящейся в дальнем поле передающей антенны (1 км для крупных ячеек, 100 м для микроячеек, 1 м для комнатных каналов); X_σ – случайная гауссова переменная с $\mu = 0$ и СКО равным σ, обычные значения – 6–10 дБ; n – степень потерь в тракте, в свободном пространстве $n = 2$ [1, с. 970].

Для компоненты мелкомасштабного замирания $r_0(t)$ плотность вероятности для амплитуды $p(z)$ имеет функцию распределения в форме Райса или Релея [1, с. 972].

Если полученный в многолучевом канале сигнал состоит из множества отраженных лучей и значительного незамирающего компонента, функция распределения будет райсовской (3):

$$(z) = \begin{cases} \frac{z}{\sigma^2} \exp\left(-\frac{z^2+A^2}{2\sigma^2}\right) I_0\left(\frac{zA}{\sigma^2}\right) & \text{для } z \geq 0, A \geq 0 \\ 0 \text{ для других } z, A \end{cases}, \quad (3)$$

где σ^2 – средняя мощность многолучевого сигнала; A – амплитуда незамирающего компонента (также называемого *зеркальным компонентом*), $I_0()$ – модифицированная функция Бесселя 1-го рода 0-го порядка.

При $A \to 0$ (незначительном зеркальном компоненте) распределение Райса (3) переходит в распределение Релея:

$$p(z) = \begin{cases} \frac{z}{\sigma^2}\exp\left(-\frac{z^2}{2\sigma^2}\right) & \text{для } z \geq 0 \\ 0 & \text{для других } z \end{cases}, \quad (4)$$

Релеевский замирающий компонент также называют *случайным, рассеянным* или *диффузным*.

Замирания с распределением Райса (3) характеризуются параметром замираний:

$$K = \frac{A^2}{2\sigma^2}.$$

Параметр K является отношением мощности прямого сигнала *LOS* к мощности других составляющих многолучевого процесса. При $K \to 0$ наблюдаетcz релеевское замирание (4), при $K \to \infty$ замирания отсутствуют (в канале остаётся только один луч LOS).

Пусть $\bar{P}_r$ – средняя принимаемая мощность. Подставим в (3):

$$A^2 = \frac{K}{K+1}\bar{P}_r,\ 2\sigma^2 = \frac{1}{K+1}\bar{P}_r$$

и получим выражение для распределения Райса через K и $\bar{P}_r$:

$$p(z) = \frac{2z(K+1)}{\bar{P}_r}\exp\left(-K-(K+1)\frac{z^2}{\bar{P}_r}\right) I_0\left(2z\sqrt{\frac{K(K+1)}{\bar{P}_r}}\right), \quad (5)$$

$$z \geq 0.$$

Ещё одним распределением, хорошо описывающим эмпирические данные, является *распределение замираний Накагами*:

$$(z) = \frac{2m^m z^{2m-1}}{\Gamma(m)\bar{P}_r^m}\exp\left(-m\frac{z^2}{\bar{P}_r}\right), \quad (6)$$

$$m \geq 0{,}5,$$

где $\bar{P}_r$ – средняя принимаемая мощность, Г() – гамма-функция, m – параметр замирания [2, с. 148]. При m = 1 распределение (6) сходится к замираниям Релея (4). При $m = \frac{(K+1)^2}{2K+1}$ распределение (6) даёт распределение Райса (5) с параметром K. При $m \to \infty$ замирания отсутствуют, $Z = \sqrt{\bar{P}_r} = \text{const}$.

Таким образом, распределение Накагами является наиболее общей моделью для описания замираний, из которой можно получить как распределение Райса, Релея, так и другие распределения.

Средняя продолжительность замираний – это среднее время, в течение которого огибающая сигнала находится ниже требуемого уровня Z (рис. 4).

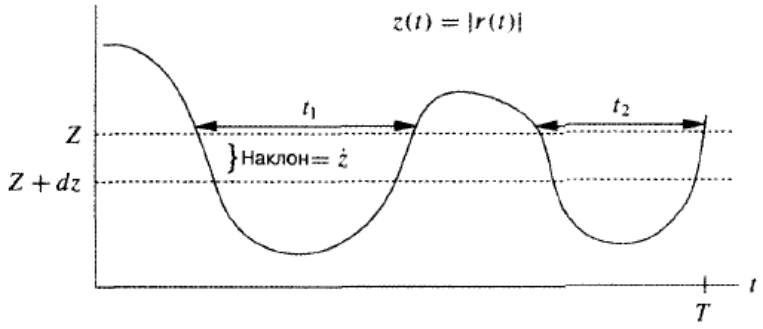


Рис. 4. Огибающая сигнала *z(t)* и требуемый уровень *Z*

Требуемый уровень может определяться качественными показателями проектируемого канала связи, например, коэффициентом ошибок по битам. При падении величины сигнала (его мощности) ниже требуемого уровня говорят о *перерыве в канале связи*.

Пусть t_i – продолжительность i-го замирания. Для достаточно большого времени наблюдения T можем записать:

$$(z(t) < Z) = \frac{1}{T}\sum_i t_i.$$

Средняя продолжительность затухания:

$$\bar{t}_Z = \frac{1}{TL_Z}\sum_{i=1}^{TL_Z} t_i \approx \frac{p(z(t)<Z)}{L_z},$$

где L_Z – скорость пересечения уровня Z (в пересечениях в секунду), на которой огибающая сигнала пересекает уровень Z вниз.

Для замираний с распределением Райса:

$$L_Z = \sqrt{2\pi(K+1)}f_D\rho\, e^{-K-(K+1)\rho^2} I_0\left(2\rho\sqrt{K(K+1)}\right), \qquad (7)$$

где $\rho = Z/\sqrt{\overline{P_r}}$, f_D – доплеровская частота [2, с. 150].

Для замираний с распределением Релея выражение (7) упрощается:

$$L_Z = \sqrt{2\pi}f_D\rho\, e^{\rho^2} I_0,$$

$$\bar{t}_Z = \frac{e^{\rho^2}-1}{\sqrt{2\pi}f_D\rho},$$

где $\bar{t}_Z$ – средняя продолжительность замирания уровня огибающей сигнала при заданном Z и средним уровнем огибающей $\sqrt{\overline{P_r}}$.

Средняя продолжительность замирания позволяет оценить количество бит, на которое повлияет глубокое замирание. Пусть длительность бита составляет T_b, и при $z(t) < Z$ вероятность ошибки высока. Тогда при $\bar{t}_Z \approx T_b$ в системе будут наблюдаться единичные случайные ошибки; при $\bar{t}_Z \gg T_b$ вероятны длительные пакеты ошибок; наконец, при $\bar{t}_Z \ll T_b$ замирания усредняются и ими можно пренебречь.

Характерным эффектом, наблюдающимся в многолучевых каналах, является замирание сигнала.

Для описания мелкомасштабных замираний в многолучевом канале используются статистические модели. Для огибающей принимаемого сигнала вводятся функции распределения вероятностей. При этом распределение Накагами является наиболее общей моделью, из которой можно получить широко используемые на практике распределения Райса и Релея, а также другие распределения. Из выбранной функции распределения можно получить величину средней продолжительности замираний, которая позволяет непосредственно оценить количество бит, принятых с ошибками в данном канале.

Список используемых источников

1. Скляр Б. Цифровая связь. Теоретические основы и практическое применение. М. : Вильямс, 2007. – 1104 с.

2. Голдсмит А. Беспроводные коммуникации. Основы теории и технологии беспроводной связи. М. : Техносфера. 2011. – 904 с.

УДК 004.41
ГРНТИ 49.45.35

РАЗРАБОТКА ПРОГРАММНОГО КОМПЛЕКСА ДЛЯ ПРОВЕДЕНИЯ ОНЛАЙН ТРАНСЛЯЦИЙ

И. В. Ожиганов, Д. А. Татаренков

Санкт-Петербургский государственный университет телекоммуникаций им. проф. М. А. Бонч-Бруевича

Для проведения качественных онлайн трансляций массовых мероприятий требуется использование нескольких телевизионных камер, из чего образуется потребность в программном обеспечении, позволяющем коммутировать видеосигналы с камер. В данной работе представлено программное обеспечение для подвижной телестудии. В функционал этого программного комплекса входит: коммутирование входных сигна-

лов с телекамер, захват изображения с компьютера выступающего (презентаций), отрисовка титров, запуск перебивок и рекламных роликов. Управление трансляцией в данной системе возможно, как с помощью микшерного пульта, так и без него.

телевидение, телевещание, программное обеспечение.

Первым звеном тракта передачи изображения при онлайн вещании является канал аппаратно-студийного комплекса. Он выполняет функции преобразования изображения в телевизионные видеосигналы, обработки этих сигналов [1]. В данной работе представлена реализация аппаратно-студийного комплекса подвижного телецентра, который может эксплуатироваться вещательной бригадой, состоящей даже из одного человека. Потоковое вещание в данном случае производится на видеостриминговые сервисы.

Для организации и проведения онлайн трансляций подвижного телецентра требуется следующее аппаратное обеспечение:

1. Сервер обработки изображений.
2. Телевизионные камеры.
3. Конвертеры видеосигнала.
4. Контроллер.
5. Коммутационные кабели.

Исходными данными в данной работе являются телевизионные камеры *SONY* серии HVR (рис. 1). Данные телекамеры обладают только SDI выходом. Для подключения камер к серверу обработки изображений требуется SDI-USB конвертер. В качестве такого конвертера используется ExtremeCap SDI-BU111.

Рис. 1. Телекамера SONY HVR (слева)
SDI-USB конвертер ExtremeCap SDI-BU111 (справа)

Для обеспечения максимальной мобильности телецентра в качестве сервера обработки изображений выступает ноутбук с рекомендуемыми системными характеристиками:

- Процессор: Intel Core i7-8750H или AMD Ryzen 7 1800X.
- Видеокарта: NVIDIA GeForce GTX 1080 (8 Гб).
- Операционная система: Windows 10 (64 бита).

– Оперативная память: 16 Гб.

В качестве контроллера выступает AKAI MidiMix, обладающий необходимым количеством кнобов и кнопок для работы с 8 каналами изображений.

Для захвата изображения с презентационного компьютера используется NDI протокол, позволяющий передавать изображение почти без сжатия по широкополосному локальному каналу, что позволяет не использовать дополнительные платы захвата или тратить ресурсы презентационного компьютера на компрессию видеосигнала.

На рис. 2 представлена схема коммутации подвижного телецентра.

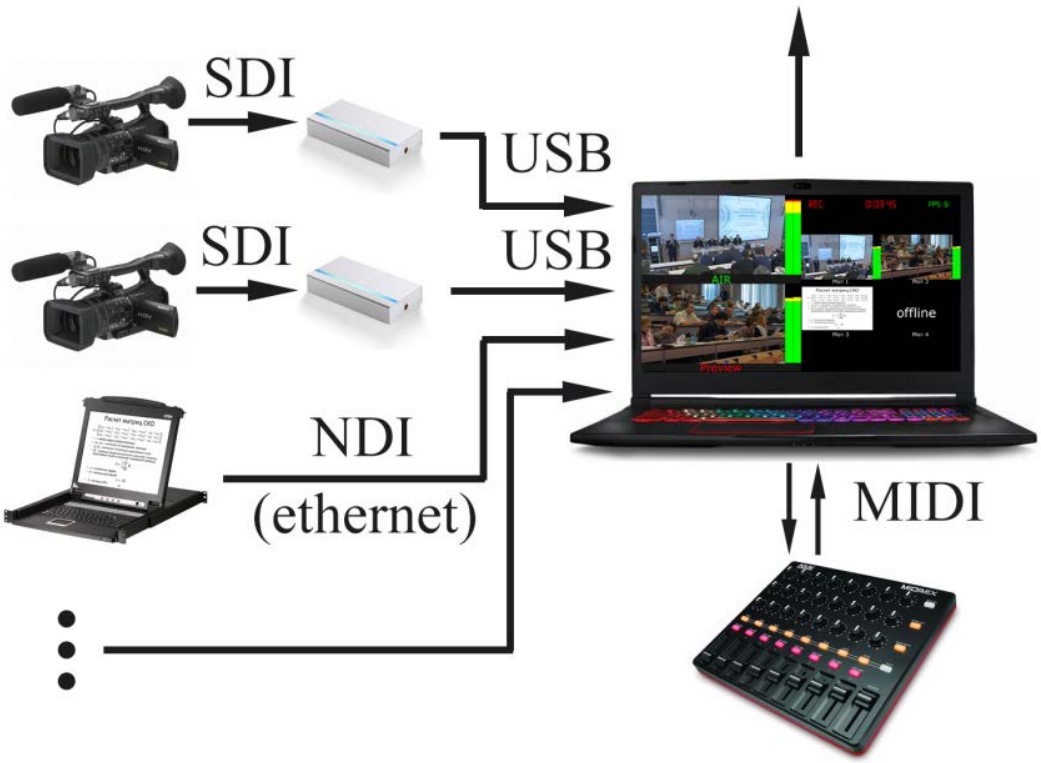


Рис. 2. Схема коммутации подвижного телецентра

Вся обработка и коммутация изображений должна происходить на сервере обработки изображений. Программный комплекс должен соответствовать требованиям [2].

В качестве языка программирования выбран визуальный язык программирования TouchDesigner, так как он отлично подходит для создания систем обработки изображений и интерфейсов управления этими системами.

Программный комплекс состоит из двух систем, каждая из которых открывается в отдельном окне:

1. Система мониторинга.
2. Система управления.

В системе мониторинга (рис. 3) осуществляется обработка и коммутирование входных видео- и аудио-сигналов. Так же эта система осуществляет компоновку выходного видеосигнала из нескольких входных, отрисовку графики, титров, воспроизведение видеофайлов и отображение видеосигналов для предпросмотра.

Рис. 3. Окно системы мониторинга

Система управления (рис. 4) представляет собой пользовательский интерфейс, позволяющий выбирать различные способы компоновки входных видеосигналов, вводить в специальное окно текст титра, запускать отрисовку титра на выходном видеопотоке. При работе с данным интерфейсом создаются управляющие сигналы, которые отправляются в систему мониторинга, где происходит переключение видеопотоков на предпросмотре, изменение выходного видеосигнала и т. д.

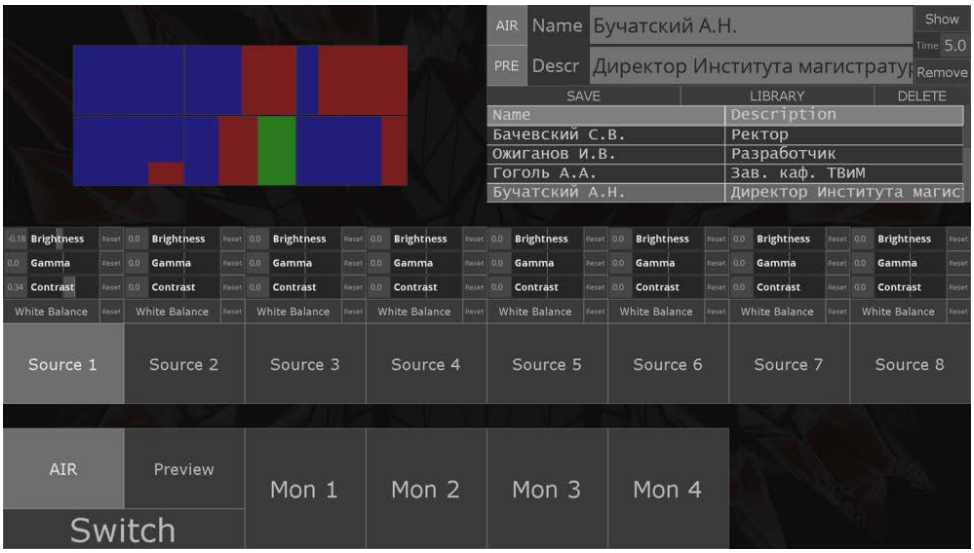


Рис. 4. Окно системы управления

Нижнюю часть на рис. 4 занимает матричный коммутатор. Над матричным коммутатором располагается панель коррекции изображения. Правый верхний угол отвечает за отрисовку титра на выходном изображении. Выпуск титра осуществляется отдельной кнопкой, содержимое титра может быть выбрано из библиотеки титров или заполнено вручную.

Представленные на рис. 4 способы компоновки (сине-красные поля) представляют собой банк значений трансформации (изменения размера и положения в кадре) нескольких видеопотоков. При выборе способа компоновки происходит отправка управляющего сигнала в систему мониторинга, где происходит обрезка входных изображений. На рис. 5 представлена часть фрагмента программы, отвечающего за компоновку выходного сигнала.

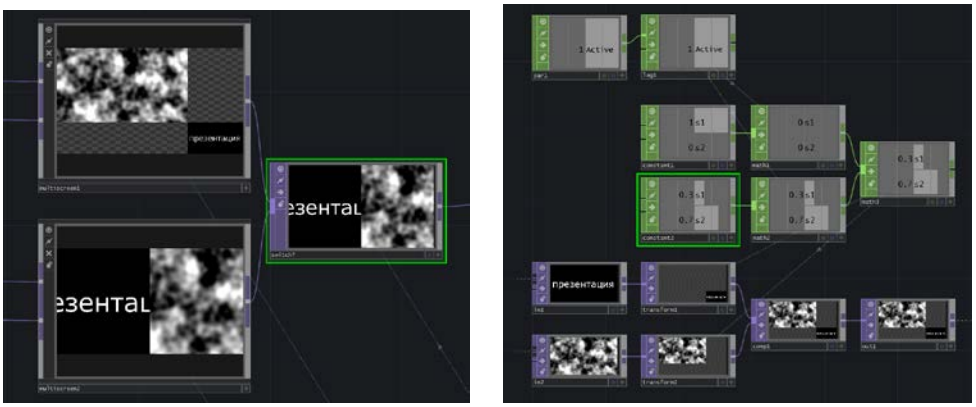


Рис. 5. Компоновка выходного сигнала

Окончательный вид программ данного комплекса представлен на рис. 6.

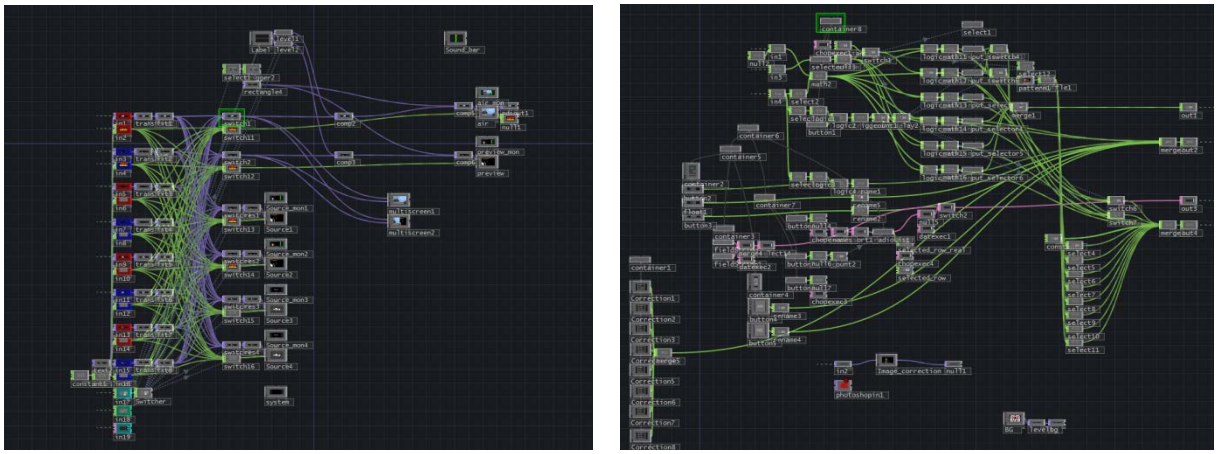


Рис. 6. Вид программ системы мониторинга (слева), системы управления (справа)

Основные возможности реализованного программного комплекса:

– микширование до 8-ми источников видеосигналов;

– коррекция изображения (баланс белого, гамма, яркость, контрастность);

– отрисовка титров;

– воспроизведение перебивок.

Ключевые особенности реализованного программного комплекса:

– отлично подходит для проведения трансляции одним человеком;

– имеет возможность конфигурации под необходимые задачи;

– имеет простой интерфейс;

– имеет суммарную задержку видеосигнала в тракте обработки менее 1 секунды;

– может работать с любыми разрешениями (зависит от производительности сервера обработки изображений);

– имеет широкий перечень источников видеосигналов: SDI, USB, NDI, RTSP, Spout, Shared Memory, DirectX texture и т. д.

Список используемых источников

1. ГОСТ 18471-83. Тракт передачи изображения вещательного телевидения. Звенья тракта и измерительные сигналы (с Изм. № 1, 2). М. : ИПК Издательство стандартов, 2001, 25 с. : ил.

2. Ozer J. Producing Streaming Video for Multiple Screen Delivery. M. : Doceo Publishing, 2013. 436 p.

Статья представлена заведующим кафедрой ТВиМ СПбГУТ, доктором технических наук, профессором А. А. Гоголем.

УДК 621.39
ГРНТИ 49.29.01

АНАЛИЗ НАПРАВЛЕНИЙ ПОВЫШЕНИЯ ИНФОРМАЦИОННОЙ ЭФФЕКТИВНОСТИ ТЕХНОЛОГИЙ ФИКСИРОВАННОГО ШИРОКОПОЛОСНОГО АБОНЕНТСКОГО ДОСТУПА

О. Н. Пантелеева, Д. С. Савельев, С. Н. Савельев

Академия Федеральной службы охраны Российской Федерации

В современном сегменте рынка инфокоммуникаций востребованы различные услуги, приближающиеся по скоростным показателям к 1 Гбит/с, а в ближайшей

перспективе от 10 до 100 Гбит/с. В связи с данным требованиями технологии фиксированного широкополосного абонентского доступа, основанные на использовании волоконно-оптического кабеля, приобретают все большую популярность. Однако, применение медных симметричных и коаксиальных абонентских линий связи, как раздельно, так и совместно также может обеспечить скоростные показатели, достаточные для предоставления услуг потребительского и коммерческого сегмента рынка.

системы фиксированного широкополосного абонентского доступа, цифровые несущие, информационная эффективность, программно-определяемые сети.

Постоянный рост требований абонентов как фиксированной, так и мобильной широкополосной связи к качеству и виду предоставляемых инфокоммуникационными системами услуг актуализирует научные исследования в области предоставления доступа на скоростях порядка 1 Гбит/с, а в перспективе от 10 до 100 Гбит/с. В настоящее время не существует универсальной технологии широкополосного доступа (ШПД), подходящей для всех случаев жизни. Несмотря на видимые преимущества волоконно-оптических решений, разработчики и производители совершенствуют технологии доступа на основе медных кабелей как симметричных, так и коаксиальных, а также активно развивают технологии фиксированного беспроводного доступа (FWA) [1]. Перспективные направления развития технологий фиксированного гигабитного доступа показаны на рис.

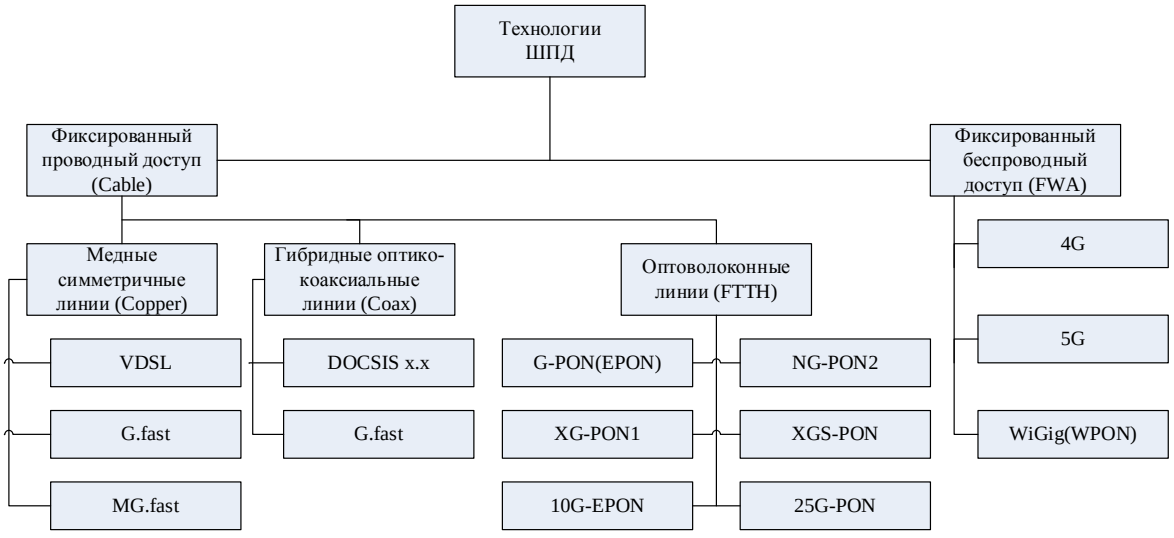


Рис. Направления развития технологий ШПД

Среди технологий доступа по медным симметричным линиям (*Copper*) можно выделить технологию G.fast, которая успешно не только конкурирует, но и дополняет полностью оптическое решение соединения абонента с провайдером (FTTH), избавляя от необходимости прокладывать оптику непосредственно на объекте. В отличие от сверхвысокоскоростной технологии VDSL2, G.fast обеспечивает симметричную передачу на расстояние

до 200–250 м теоретически со скоростью до 1 или 2 Гбит/с. Технология G.fast определяет обратную совместимость или режим возврата с VDSL, что позволяет обеспечить аппаратную совместимость и плавный переход между линиями связи. Дальнейшим развитием технологии является стандарт MG.fast, позволяющий повысить скорость передачи информации за счет повышения мощности передачи с 4 до 8 дБ, информационной плотности на поднесущей с 12 до 14 бит, а также за счет расширения спектра с 106 до 212 МГц [1].

Одним из направлений повышения информационной эффективности технологий доступа по медным симметричным линиям предлагается применение широкополосных цифровых несущих, в качестве которых наиболее целесообразно из-за простоты технической реализации использовать двоичные двухуровневые кодовые последовательности семейства функций Уолша [2]. На основе функций Уолша можно создать сверхширокополосные несущие двух видов: непрерывные и дискретные (импульсные). Выбор конкретного вида несущих Уолша зависит от возможности использования их характеристик при технической реализации систем передачи информации с цифровыми сигналами. Для сигналов Уолша применимы амплитудная модуляция, модуляция (манипуляции) по временному положению (фазе), частотная модуляция, имеющей особенностью то, что в отличие от гармонических сигналов, временное положение сигнала Уолша и его частота не связаны мультипликативно, и модуляция по периоду. Так, как сигнал Уолша является цифровым сигналом, то он допускает еще и кодовую модуляцию, которая заключается в модуляции сигнала по номеру функции Уолша. Перестройка с одного метода модуляции на другой, а также смена несущих может осуществляться программно. Для увеличения скорости передачи информации предлагается использовать квадратурно-амплитудную модуляцию цифровой несущей и спектральное (частотно-позиционное) кодирование, когда передача осуществляется без разделения на субканалы, что существенно увеличивает помехоустойчивость и упрощает декодирование. При таком методе используется линейное кодирование с основанием кода, определяемым, например, общим числом сочетаний номеров, передаваемых цифровых несущих в субканале.

Другим направлений повышения информационной эффективности предлагается применение фильтрованной многотоновой модуляции (FMT) вместо дискретной многотоновой модуляции (DMT), широко используемой в настоящее время. Технология FMT основана на преобразовании входного сигнала банком (блоком) цифровых фильтров на передающей стороне с последующим синтезом на приеме. В результате обработки сигнала в приемном устройстве ошибка восстановления имеет низкий порядок по сравнению с шумами восстановления системы с аналоговыми фильтрами,

использующий технологию DMT. При FMT банк цифровых фильтров создается путем децимации и интерполяции характеристики цифрового фильтра низких частот (фильтра-прототипа), имеющего амплитудно-частотную характеристику близкую к идеальной. Применяемые в технологии FMT для декорреляции сигнала банки цифровых фильтров, по сравнению с используемым в технологии мультиплексирования ортогональных несущих (OFDM) для декорреляции отсчетов сигнала преобразования Фурье, обладают следующим преимуществом: при кодировании решение принимается не по отдельным частотам, а по полосам частот с использованием процедуры «inverse waterfilling». В результате банки цифровых фильтров обеспечивают в среднем лучшую декорреляцию. Преимуществами технологии FMT по сравнению с применяющимися технологиями DMT и OFDM являются следующие: нет необходимости создания в кадре OFDM защитных интервалов, за счет чего в спектре создается дополнительный частотный интервал, что представляет возможность повысить скорость передачи информации; внеполосные излучения имеют гораздо меньшие уровни, т. е. уменьшается пик-фактор сигнала, характерного технологии OFDM; появляется возможность применения цифровой адаптивной фильтрации; снижаются требования к системе передачи информации по обеспечению синхронизации; уменьшается влияние межсимвольной интерференции на передаваемую информацию.

Если при синтезе банка цифровых фильтров использовать вейвлет-функции, то технологию WFMT также возможно рассматривать как одно из направлений повышения информационной эффективности цифровых абонентских линий связи. Преимуществом WFMT является то, что посредством вейвлет-преобразования для заданного числа блоков фильтров, возможно осуществить точное деление спектра сигнала на канальные субполосы на низких частотах и грубое деление на высоких частотах. Субполосы спектра, получаемые при таком делении, описываются белым шумом с дисперсией пропорциональной спектру мощности. Вейвлеты в настоящее время получили применение в следующих системах: сжатия изображений; цифровой связи, системах с широкополосными сигналами, системах скрытой связи [3].

Среди технологий доступа по оптоволоконным линиям (FTTH) можно выделить технологию NG-PON2 (Серия МСЭ-Т G.989 или TDWM-PON) с теоретической пропускной способностью до 40 Гбит/с. Одним из основных преимуществ NG-PON2 стандарта является совместимость и возможность одновременной работы со стандартом предыдущего поколения GPON в одной оптической инфраструктуре, позволяя внедрять 10G-PON технологии там, где это необходимо в первую очередь, не переделывая существующую сеть. Для операторов связи NG-PON2 представляет возможности передачи стандартов телевидения сверхвысокой четкости Ultra HD.

Технологическими вариантами NGPON-2 являются: мультиплексирование с разделением времени (TWDM), мультиплексирование с разделением по длине волны (WDM-PON) и мультиплексирование с ортогональным частотным разделением каналов (OFDM-PON).

В программно-определяемых сетях (SDN) возможно применение технологии XGS-PON, обеспечивающая скорость до 10 Гбит/с. В данном случае программное обеспечение, связывающее приемо-передающий модуль (OLT) и терминалы оптической сети (ONT), помещается в облако. Программа IEEE EPON определила стандарт 10G-EPON, позволяющий обеспечить пропускную способность 10 Гбит/с, при этом, не требуя TWDM.

Технология PON имеет такие преимущества, как: активное оборудование используется минимально; кабельная инфраструктура минимизирована; стоимость обслуживания считается низкой; присутствует возможность интеграции с кабельным ТВ; отличная масштабируемость; абонентские порты имеют высокую плотность.

Технология DOCSIS (*Data Over Cable Service Interface Specifications*) на основе коаксиального кабеля на «последней миле» предлагает те же скоростные показатели, что и оптоволоконные решения. Поскольку потребности абонентов и провайдеров продолжают развиваться, стандарт DOCSIS постепенно обновляется, так DOCSIS 3.0 значительно увеличил пропускную способность восходящего и нисходящего потоков для размещения высокоскоростных услуг передачи данных. Благодаря своей постоянной способности удовлетворять изменяющиеся потребности, поддерживать широкий спектр поставщиков оборудования и успеху на рынке, технология DOCSIS широко признана как успешная модель для совместимых продуктов, которые сохраняют сосуществование и обратную совместимость. Добавление DOCSIS 3.1 также поддерживает обратную совместимость [4].

Беспроводные решения ФШПД на основе высокоскоростных беспроводных технологий в настоящее время широко применяются в комбинации с волоконной оптикой. Речь идет о дополнении архитектуры FTTH на основе технологии WiGig (802.11ad), работающей в нелицензируемом диапазоне частот 60 ГГц – Wireless PON (WPON). Передатчики WiGig, являющиеся оконечным оборудованием линий PON, обеспечивают передачу информации со скоростью 1 Гбит/с или по радиоканалу в условиях прямой видимости до 300 м. Стандарт WPON может быть использован в целях организации абонентского доступа как в сельской местности, в пригородной застройке, так и для присоединения периферийных зданий к кампусным приложениям программно-определяемых сетей, известных как POL (*Passive Optical* LAN) [1].

В качестве беспроводного решения ФШПД может быть использован стандарт нового поколения Wi-Fi – 802.11ax, известного также как Wi-Fi 6.

В отличие от своего предшественника – 802.11ac – этот стандарт предназначен для работы как в диапазоне 5 ГГц, так и 2,4 ГГц и должен обеспечить четырехкратное увеличение пропускной способности пользователя.

Технологии фиксированного широкополосного абонентского доступа, основанные на использовании волоконно-оптического кабеля, приобретают все большую популярность. Однако, применение беспроводных решений, а также медных симметричных и коаксиальных абонентских линий связи, как раздельно, так и совместно также может обеспечить скоростные показатели, достаточные для предоставления услуг потребительского и коммерческого сегмента рынка. Главное, чтобы подключение производилось быстро и удобно для клиента, а услуги были качественными.

Список используемых источников

1. Попов С. Набоких Л. BBWF-2018: фиксированный доступ берет курс на SDN // Первая миля. 2018. № 8. С. 60–66. DOI: 10.22184/2070-8963.2018.77.8.60.66.

2. Урядников Ю. Ф., Аджемов С. С. Сверхширокополосная связь. Теория и применение. М. : СОЛОН-Пресс, 2005. 368 с.

3. Воробьев В. И., Грибунин В. Г. Теория и практика вейвлет-преобразования. СПб. : ВУС, 1999. 128 с.

4. Астахов И. Последняя миля: медь или стекло? // Первая миля. 2014. № 3. С. 16–17.

5. SDN: Transforming networking to accelerate business agility [Электронный ресурс]. URL: http://opennetsummit.org/archives/mar14/site/why-sdn.html (дата обращения: 02.10.2019).

УДК 004.056.5
ГРНТИ 81.93.29

СУЩНОСТЬ И СОДЕРЖАНИЕ ЗАДАЧ ПОИСКА УЯЗВИМОСТЕЙ ИНТЕРФЕЙСОВ В ИНТЕРЕСАХ БЕЗОПАСНОГО УПРАВЛЕНИЯ БЕСПИЛОТНЫМИ ТРАНСПОРТНЫМИ СРЕДСТВАМИ «УМНОГО ГОРОДА»

И. Б. Паращук[1,2], А. А. Чечулин[1,3]

[1]Санкт-Петербургский институт информатики и автоматизации Российской академии наук
[2]Санкт-Петербургский национальный исследовательский университет информационных технологий, механики и оптики
[3]Санкт-Петербургский государственный университет телекоммуникаций им. проф. М.А. Бонч-Бруевича

Беспилотные транспортные средства приобретают все большую популярность, особенно в рамках концепции «умный город». Одна из основных проблем их применения –

безопасность. Важным элементом, влияющим на безопасность, являются интерфейсы взаимодействия. Рассматривается подход к формулировке сущности и содержания задач поиска уязвимостей интерфейсов типа «человек – искусственный интеллект» в интересах безопасного управления беспилотными транспортными средствами «умного города». Перечень задач включает как моделирование угроз и процессов функционирования беспилотных транспортных средств, так и задачи интеллектуальной обработки данных. Решение этих задач повысит безопасность систем управления беспилотным транспортом.

беспилотные транспортные средства, умный город, интерфейс, уязвимость, угроза, данные, искусственный интеллект.

Одним из направлений развития больших социокиберфизических систем и новым поколением сетевых распределенных, но функционально взаимосвязанных социальных, физических и кибернетических инфраструктур современные исследователи называют концепцию «умного города». «Умный город» – взаимоувязанная по месту и во времени, в социальной, био- и технологической среде совокупность подсистем «умного жизнеобеспечения», «умного здравоохранения», «умного образования», «умного транспорта» и т. д. В рамках концепции «умного города» значительный рост количества транспортных средств в городах нашей страны и за рубежом создает объективные предпосылки для поиска путей и методов оптимизации транспортных потоков. Одним из подходов к решению подобных проблем на пути к созданию, например, «умного транспорта», является разработка и внедрение интеллектуальных беспилотных транспортных средств (БТС) в рамках транспортной среды «умного города» [1].

Еще одной большой проблемой «умного города» продолжает оставаться его безопасность, поскольку к комплексности угроз добавляется их многоуровневость. Она проявляется в том, что уровень угроз различен на разных пространственных, социальных, физических и кибернетических участках, а также в разных временных координатах функционирования «умного города» [2, 3].

Современные БТС «умного города» могут быть различными: беспилотные средства общественного транспорта (метро, автобусы); беспилотные средства частного транспорта (такси, дроны); беспилотные средства рабочей техники (техника для уборки дорог, вывоза мусора). Кроме того, «умный транспорт», помимо БТС, включает инфраструктуры для их навигации и функционирования (дороги, элементы дорожной разметки, знаки дорожного движения, светофоры, заправочные станции и станции подзарядки, станции техобслуживания), а также людей, представляющих собой как пользователей транспортной среды, так и персонал. Оптимально взаимодействовать этим компонентам призван помочь искусственный интел-

лект (ИИ), без помощи которого сегодня невозможно обрабатывать и анализировать поток больших данных, создаваемый множеством взаимодействующих БТС.

При этом к ключевым задачам ИИ апологеты «умного города» относят предоставление данных, необходимых человеку для взаимодействия с БТС, в удобном для восприятия человеком виде, а также сбор необходимых данных о человеке для оценки его состояния, идентификации и аутентификации БТС. Осуществляя обработку данных в режиме реального времени, ИИ может предоставить человеку информацию о загруженности транспортной среды «умного города» (трафик, наличие свободных средств передвижения и мест в них), о возможных маршрутах движения БТС и их оптимизации, о расписании движения БТС и его изменении, об авариях и инцидентах, о доступных парковочных местах, о размере очередей на заправках или станциях техобслуживания. Более того, ИИ может отвечать за сбор и обработку биометрических и цифровых данные о человеке (отпечаток пальца, сетчатка глаза, лицо, походка, голос, данные специальных карт и токенов, платежные данные), использующем или управляющем БТС.

Безопасность работы человека с ИИ, а значит и с БТС и с транспортной средой «умного города» в целом, опирается, по сути, на безопасность различных интерфейсов, призванных осуществлять взаимодействие этих компонент. При этом под интерфейсом понимается совокупность средств, методов и правил взаимодействия (управления, контроля и т. п.) между ИИ, БТС и иными элементами транспортной среды «умного города».

Как и в традиционных информационных технологиях, различают понятия «пользовательский интерфейс» (совокупность средств, при помощи которых пользователь взаимодействует с различными программами и устройствами) и «системный интерфейс» – совокупность унифицированных технических, программных и конструктивных средств, основанных на стандарте и реализующих взаимодействие функциональных элементов в транспортной среде «умного города», обеспечивающих информационную, электрическую и конструктивную совместимость этих элементов.

Наиболее перспективными из современных интерфейсов являются многомодальные, в которых предусмотрена возможность взаимодействия человека с ИИ посредством ручного и автоматического ввода и вывода текстовой и графической информации, звуков и жестов. Важность, значимость роли интерфейсов, наряду с ростом числа угроз, предопределяют объективную необходимость решения задач поиска уязвимостей таких интерфейсов в интересах безопасного управления БТС «умного города».

Сущность и содержание задач поиска уязвимостей напрямую связаны с целевой функцией – обеспечением безопасности людей, транспортных средств и объектов инфраструктуры за счет обнаружения уязвимостей ин-

терфейсов между человеком и ИИ в рамках управления БТС и в транспортной среде «умного города» в целом. Для этого предполагается разработать методы поиска уязвимостей интерфейсов взаимодействия в рамках транспортной среды. При этом содержание конкретных задач нацелено на:

1. Анализ научных работ и результатов практических исследований, посвященных методам человеко-машинного взаимодействия и типам интерфейсов, применяемых в транспортных системах. Анализу также подвергаются области: обнаружения угроз в транспортных инфраструктурах, визуализации данных, когнитивного аппарата человека и распознавания его состояния с помощью технологии машинного зрения [4].

2. Классификацию интерфейсов взаимодействия с БТС и иными транспортными системами «умного города», а также разработку метода определения типа интерфейса «человек – искусственный интеллект».

3. Классификацию возможных угроз для БТС и для транспортной среды «умного города» в целом, реализация которых прямо или косвенно возможна посредством использования интерфейсов «человек – искусственный интеллект». При этом должны быть учтены как угрозы, направленные на человека (оператора или пользователя) так и на искусственный интеллект, осуществляющий мониторинг и управление БТС и транспортной инфраструктурой «умного города».

4. Классификацию уязвимостей интерфейсов «человек – искусственный интеллект» в соответствии с классификациями интерфейсов и угроз, полученных в результате решения предшествующих задач.

5. Разработку концептуальных моделей интерфейсов взаимодействия пользователь-система, система-пользователь, оператор-система, система-оператор, включающие как явные интерфейсы взаимодействия (например, осуществление человеком некоторого воздействия), так и неявные (например, распознавание психофизиологического состояния человека). Разрабатываются модели, учитывающие интерфейсы, основанные на методах машинного зрения, визуальном, тактильном, акустическом способах взаимодействия и учитывающие особенности когнитивного аппарата человека.

6. Разработку методов поиска уязвимостей интерфейсов взаимодействия пользователь-система, система-пользователь, оператор-система, система-оператор, на основе классификации уязвимостей и концептуальных моделей интерфейсов.

7. Разработку программного обеспечения для программно-аппаратного стенда с использованием компонентов, реализующих модели интерфейсов «человек – искусственный интеллект» и методы поиска уязвимостей в этих интерфейсах. Необходимы экспериментальные исследований с разработанными методами поиска уязвимостей и методом определения типа интерфейса, интерпретация полученных результатов.

8. Разработку научно-технических предложений по внедрению полученных результатов решения задач поиска уязвимостей интерфейсов в интересах безопасного управления беспилотными транспортными средствами «умного города».

Таким образом, главной, объединяющей задачей является разработка научно-методического обеспечения, включающего комплекс взаимосвязанных методов, моделей и программных прототипов, предназначенных для поиска уязвимостей в интерфейсах «человек – искусственный интеллект», предназначенных для управления БТС и транспортной инфраструктурой «умного города» в целом. Задача решается, в том числе, в рамках визуализации данных, поступающих от ИИ в транспортной среде «умного города», анализа состояния оператора системы управления и других элементах интерфейсов. Данная задача является концептуально новой, а ее решение позволит, за счет учета аспектов безопасности, сделать качественно новый сдвиг в области систем управления беспилотным транспортом и пересмотреть эффективность текущих способов взаимодействия человека и искусственного интеллекта в обеспечении непрерывного и надежного управления транспортной средой «умного города».

Работа выполнена при финансовой поддержке РФФИ (проект 19-29-06099) в СПИИРАН.

Список используемых источников

1. Sladkowski A., Pamula W. (Eds.) Intelligent transportation systems – problems and perspectives (Vol. 32). Springer International Publishing, 2016. 303 p.

2. Котенко И. В., Паращук И. Б. Автоматизированный адаптивный мониторинг комплексной безопасности информационных систем «умного города»: целевые функции концептуальной модели // Вестник Астраханского государственного технического университета. Серия: Управление. Вычислительная техника. Информатика». 2018. № 3. С. 7–15.

3. Котенко И. В., Паращук И. Б. Анализ задач и потенциальных направлений разработки современных методов и средств обеспечения комплексной безопасности киберфизических систем типа «умный транспорт» // Научное обозрение. 2017. № 25. С. 26–30.

4. Проноза А. А., Чечулин А. А., Котенко И. В. Математические модели визуализации в SIEM-системах // Труды СПИИРАН. 2016. Вып. 46. С. 90–107.

УДК 004.056
ГРНТИ 81.96

СПОСОБЫ ЗАЩИТЫ ОТ МОБИЛЬНОГО КОДА

И. С. Поздняк, Т. В. Филиппова

Поволжский государственный университет телекоммуникаций и информатики

В настоящее время мобильный код является достаточно серьезной угрозой для информационной системы. За счет автоматического запуска из-за неосторожности пользователей, защититься от вредоносного кода сложно. В представленной работе рассматриваются общие принципы работы мобильного кода и возможные меры защиты ресурсов сети от его вредоносного воздействия посредством внедрения различных механизмов контроля, обеспечивающих предотвращение, обнаружение и удаление вредоносного кода.

мобильный код, средства защиты, JavaScript, ActiveX.

Под мобильным кодом можно понимать любой программный код, который передается по сети для запуска (в большинстве случаев, автоматического) на каком-либо устройстве или системе при минимальном взаимодействии или без взаимодействия с пользователем. В представленной работе речь пойдет о вредоносном мобильном коде, который перемещаясь через сеть, наносит ущерб безопасности компьютера пользователя путем автоматического запуска (чаще всего в веб-браузере).

Мобильный код создается с помощью JavaScript, при этом используются элементами управления ActiveX. Чтобы код начал работу, он должен попасть в систему. Из системы мобильный код получает доступ к жесткому диску. После этого вредоносный код может читать, удалять и изменять файлы.

Мобильный код, написанный на языке Java, называют апплетом (скриптом), который затем выполняется в браузере в любой системе пользователя. Поскольку последняя не доверяет работе мобильного кода, то вся его деятельность начинается с так называемой «песочницы» (логически изолированной среды). Такое решение призвано ограничить выполняемые кодом операции и уберечь от несанкционированных действий компьютер пользователя.

Если браузер совместим с ActiveX, то при появлении вредоносного программного обеспечения на основе JavaScript происходит автоматическая загрузка кода, после чего он проверяется. Далее выводится информации об авторе или компании, написавшей код. По подписи становится видно, подвергался мобильный код изменениям или нет. Дальнейшие действия

предпринимает пользователь. Только он решает, загружать ли данный код для исполнения или нет. После того, как пользователь соглашается на выполнение программы, последствия для него становятся непредсказуемыми в случае, если мобильный код являлся вредоносным. У загруженного скрипта появляется доступ ко всем файлам, но в то же время, этот код может и не нести никакой угрозы компьютеру.

Если вредоносный Java код приходит по электронной почте, то он загружается автоматически при открытии письма. В большинстве информационных систем, электронная почта является одним из самых уязвимых мест. Кроме этого, вредоносный мобильный код может скрываться и в HTML страницах. Например, если открывается инфицированная страница, то пользователю выдаётся сообщение о возможности продолжения работы, так как система нашла подозрительный код. Если пользователь соглашается, то код автоматически копируется в системную папку операционной системы, а дальше начинает свою работу. Список сайтов с опасными вирусами и вредоносными мобильными кодами постоянно обновляется. Крупные поисковые системы в настоящее время осуществляют постоянный контроль за отсутствием вирусов на индексируемых сайтах. В случае обнаружения таковых информация о заражении будет оперативно предоставлена владельцам сайта или технической поддержке.

Защитить информационную систему и компьютеры пользователей от вредоносного мобильного кода достаточно сложно. Большая проблема заключается в том, что мобильные коды могут осуществлять взаимодействие между собой. Все правила, допускающие использование таких скриптов в операционных системах, должны быть прописаны в нормативных документах каждой организации, например, в политике безопасности. Одним из способов защиты от вредоносного мобильного кода является отключение ActiveX, но это является крайней мерой. Так как в таком случае не смогут приходить обновления.

Ниже представлены наиболее простые меры защиты, которые важно применять для противодействия вредоносному мобильному коду. Некоторые из них регламентируются методическим документом «Меры защиты информации в государственных информационных системах» (утвержден ФСТЭК России 11.02.2014) [1] и могут также применяться в коммерческих структурах.

1. Регистрация событий в журнале. Необходимо обязательно записывать в журнал все действия с мобильными кодами: их загрузку, изменение, перемещение. В дальнейшем проводить анализ зарегистрированных событий.

2. Контроль мобильного кода. Необходимо прописать правила на разрешение использования в данной системе мобильного кода.

3. Ограничение мест распространения мобильного кода. Данный код должен использоваться только на определенных заранее устройствах (автоматизированные рабочие места, мобильные технические средства информационной системы), он должен иметь ограниченное место действия.

4. Наличие программного обеспечения (ПО), например, встраиваемого в антивирусы, которое позволяет производить поиск мобильного кода. При обнаружении вредоносного скрипта в системе, антивирус уведомляет администратора и предлагает стандартные действия: поместить в карантин, блокировать или удалить. Более надёжную антивирусную защиту предполагает использование антивирусов от нескольких производителей. При этом использовать необходимо последние версии ПО.

5. Отключение автоматических загрузки и выполнения неизвестных мобильных кодов.

6. Обязательная проверка подлинности источника и целостности мобильного кода.

7. Все пользователи должны быть обучены и знать меры экстренной защиты.

8. Запрет на установку нелицензионного программного обеспечения. Все программы должны устанавливаться только администратором.

9. Запрет ненадёжных сайтов. Каждый сайт должен быть проверен, а ненадёжные источники заблокированы.

Вредоносные скрипты наносят ущерб не только пользователям систем, но и владельцам сайтов. В случае с выделенным сервером ответственность за безопасность ресурса лежит преимущественно на его владельце, если речь идет об общедоступном хостинге, этим вопросом занимается непосредственно сама хостинговая компания. Тем не менее, существует ряд мер, которые помогут администраторам обезопасить свои ресурсы [2]:

– Систематическая смена паролей администратора сайта или аккаунта хостинга.

– Создание сложных и длинных паролей, состоящих из сочетания букв, символов и цифр.

– Наличие антивирусного программного обеспечения с регулярно обновляемой вирусной базой. Периодическая полная проверка сервера.

– Использование безопасного VPN-подключения при необходимости работы в открытых Wi-Fi сетях.

Таким образом, можно отметить, что большинство мер, направленных на защиту системы от вредоносного мобильного кода, являются организационными. Но существуют определенные меры, которые необходимо применять для профилактики (обучение сотрудников) и при возникновении экстренных ситуаций (отключение компьютера от сети).

Неосторожное или необдуманное действие пользователя может привести к нарушению работоспособности всей информационной системы

предприятия. Поэтому, соблюдая все перечисленные правила, есть гарантия защиты сети организации от вредоносного мобильного кода.

Список используемых источников

1. Методический документ. Меры защиты информации в государственных информационных системах: утв. ФСТЭК России 11.02.2014. – 176 с.

2. Вирус на сайте [Электронный ресурс]. URL: https://revisium.com/kb/website_virus.html (дата обращения 21.01.2020).

УДК 535.3
ГРНТИ 29.31.29

РАЗРАБОТКА ЛАБОРАТОРНОГО МОДУЛЯ ДЛЯ ИССЛЕДОВАНИЯ ПРИЗМЕННЫХ СИСТЕМ НА ЭЛЕМЕНТНОЙ БАЗЕ ОПТИЧЕСКОГО КОНСТРУКТОРА

Е. В. Полякова

Санкт-Петербургский государственный университет телекоммуникаций им. проф. М. А. Бонч-Бруевича

Понимание действия преломляющих призм позволяет правильно использовать их в оптическом приборостроении. Оптические призменные системы оборачивают, вращают и компенсируют поворот изображения, формируют излом оптической оси и изменяют направление хода оптических лучей, способствуя уменьшению габаритов оптических приборов.

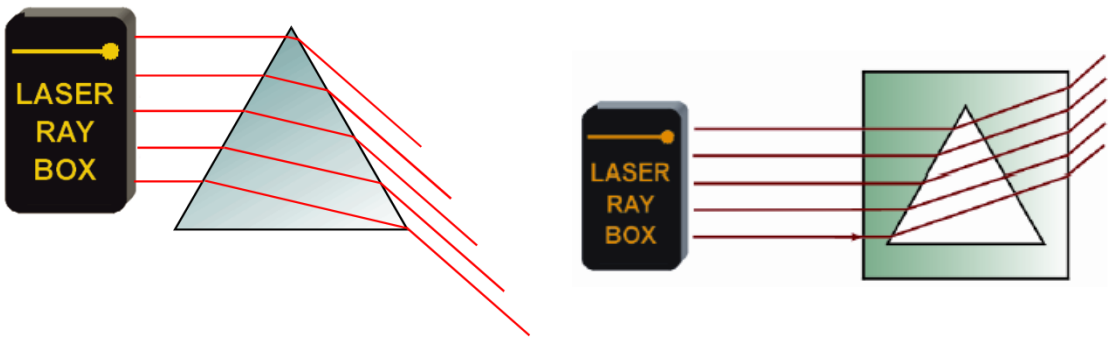
оптическая призма, оптическая призменная система, оптический конструктор.

Оптический конструктор представляет собой набор оптических деталей, позволяющих собирать экспериментальные установки для исследования физических процессов и явлений, изучаемых в дисциплинах «Введение в профессию» и «Оптическая физика» направления подготовки 12.03.03 «Фотоника и оптоинформатика». В связи с тем, что комплект деталей оптического конструктора достаточно разнообразен, представляется возможным провести эксперименты с входящими в состав оптического конструктора призмами, а также создать лабораторный макет для наглядной демонстрации законов геометрической оптики на базе оптических призменных систем. Удобство лабораторного макета обусловлено намагниченностью оснований всех оптических деталей, обеспечивающей жесткое крепление

деталей к демонстрационной поверхности во время экспериментов, и достаточной механической прочностью оптических деталей, т. к. они изготовлены из оптического поликарбоната.

В комплекте оптического конструктора имеются призмы для изменения направления хода лучей в оптической системе: пять призм с треугольным основанием и пять призм с прямоугольным основанием. Для проведения лабораторных экспериментов в комплекте модуля предусмотрен бокс из пяти лазерных диодов (LASER RAY BOX) с блоком питания 220 В. Лазерные диоды (ЛД) работают в видимом диапазоне длин волн – 635 нм, что позволяет наблюдать прохождение световых потоков через прозрачные среды. Выходная оптическая мощность ЛД меньше 1 мВт, что соответствует требованиям к эксплуатации лазерных изделий; расстояние между ЛД – 18 мм, чем обеспечивается хорошо видимый параллельный световой поток на входе в оптическую систему [1]. В рамках заявленного эксперимента на элементной базе оптического конструктора (призмах) можно провести лабораторную работу «Конструирование призменных систем для смещения и оборачивания изображения».

Целью такой лабораторной работы является исследование отклоняющих призменных систем: исследование законов преломления света на границе раздела сред и общая задача отклонения призмой светового потока (рис. 1), отклонение светового потока призмой АР-90° (рис. 2), отклонение светового потока призмой БР-180 (рис. 3), система призм АР-90° (4) система призм АР-90° и БР-180° (5), системы Порро I рода (рис. 6).



а) б)

Рис. 1. Отклонение светового потока призмами: а) показатель преломления призмы больше показателя преломления окружающего прозрачного материала; б) показатель преломления призмы меньше показателя преломления окружающего прозрачного материала

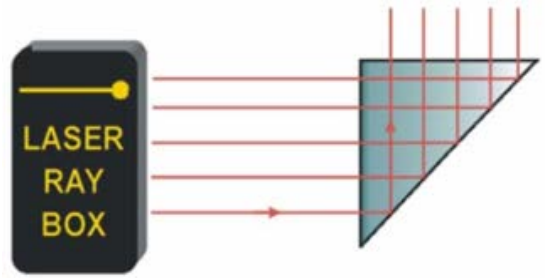


Рис. 2. Прохождения световых лучей через призму АР-90°

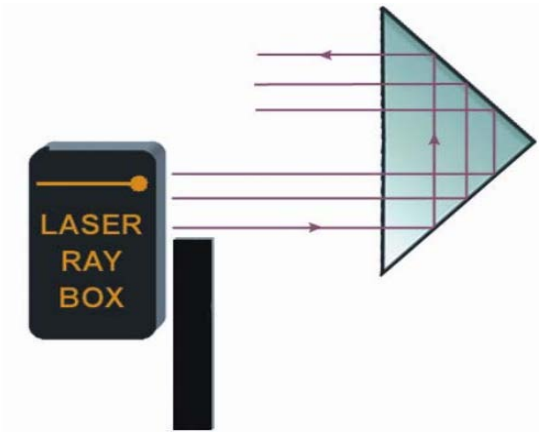


Рис. 3. Прохождения световых лучей через призму БР-180°

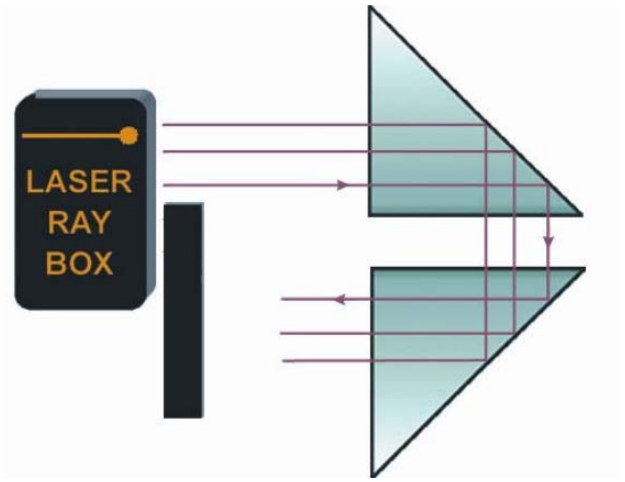


Рис. 4. Оптическая призменная система на базе призм АР-90°

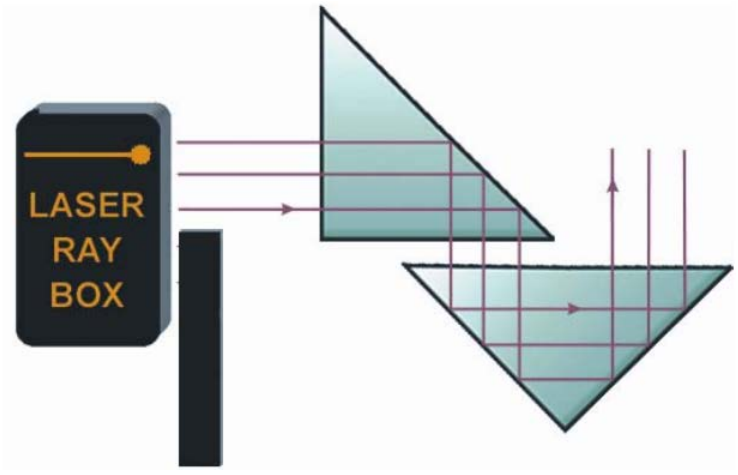


Рис. 5. Оптическая призменная система на базе призм АР-90° и БР-180°

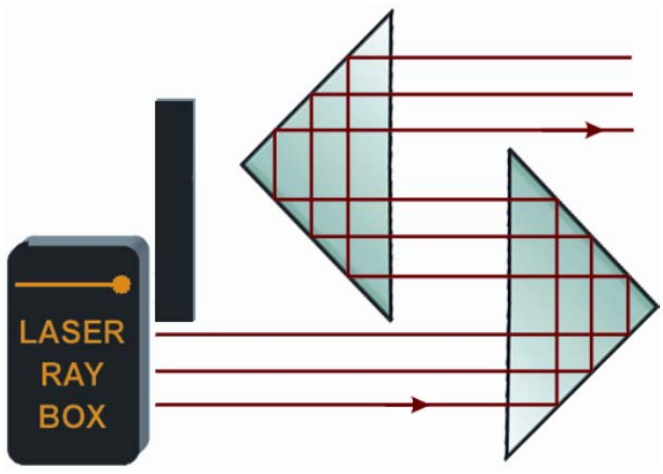


Рис. 6. Прохождение световых лучей через систему Порро I рода

В каждом исследовании необходимо правильно расположить источник излучения относительно одной или нескольких оптических деталей, получить достаточно интенсивный выходной поток. Провести измерения углов отклонения выходного луча относительно входного. Сравнить экспериментально полученные результаты с предварительным теоретическим расчетом (раздел геометрическая оптика) [2].

На базе собранной оптической системы Порро I рода возможно провести измерение диапазона смещения светового потока, зависящего от геометрических размеров и пространственного расположения призм.

Для удобства проведения опыта, луч от источника направляется выше нижней крайней точки призмы во избежание многочисленных отражений и получения четкой и понятной картины прохождения луча. Этот отступ одинаков для всех измерений и в данном оптическом конструкторе равен 5 мм. Проводятся эксперименты с целью получения минимально и максимально возможных смещений светового луча, F_1 и F_2 – расстояния, пройденные лучом в оптических деталях оптической системы (рис. 7).

В рамках проведения исследований призменных систем на элементной базе оптического конструктора требуется дополнительно выполнить работы по определению критического угла полного внутреннего отражения, сравнив полученный результат с теоретическим расчетом, и рассчитать показатель преломления оптического полимера, из которого изготовлены детали оптического конструктора [3].

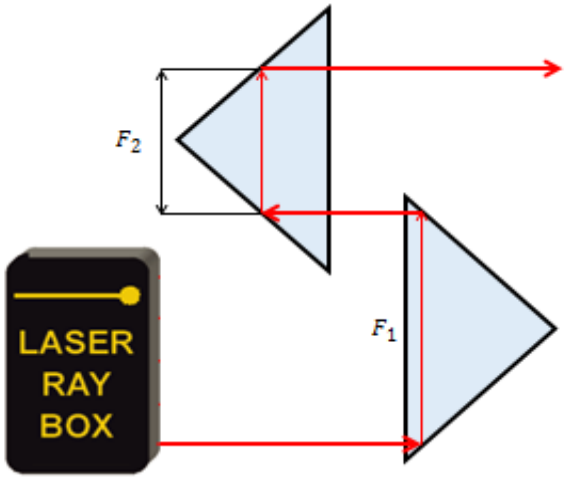


Рис. 7. Схема для расчета смещения луча

Вышеприведенные исследования способствуют хорошему пониманию закономерностей прохождения световых потоков через оптически прозрачные среды и законов геометрической оптики. Полученные студентами знания и навыки будут использованы при изучении физических процессов в технике оптической связи и оптического приборостроения.

Список используемых источников

1. Modern educational equipment by KVANT: Company KVANT, 2013. 28 с.
2. Алешкевич В. А., Оптика : учебник для студентов высших учебных заведений. М. : Физматлит, 2010. 318 с.
3. Паркевич Е. В., Использование призм, клинов и прозрачных пластинок в оптических системах : метод. пособие. М. : МФТИ, 2014. 20 с.

Статья представлена заведующим кафедрой ФиЛС СПбГУТ, кандидатом технических наук, доцентом М. С. Былиной.

УДК 681.7.064.43/621.3
ГРНТИ 49.44.33

ПРИМЕНЕНИЕ ИНТЕРФЕРЕНЦИОННЫХ ФИЛЬТРОВ В ОПТИЧЕСКИХ СИСТЕМАХ СВЯЗИ

Б. К. Резников

Санкт-Петербургский государственный университет телекоммуникаций им. проф. М. А. Бонч-Бруевича

В статье приводится описание области применения оптических фильтров, основанных на многослойных тонкопленочных структурах. Рассматривается применение фильтров в мультиплексорах для систем разделения спектрального ресурса оптического волокна. Приводится описание фильтрующей структуры мультиплексоров WDM. Рассматриваются характеристики пропускания фильтров с различным количеством слоев.

фильтр, оптическая связь, DWDM, CWDM, WDM, TFF, тонкие пленки.

Область применения фильтров

Как известно, в оптической связи применяются длины волн инфракрасного диапазона (рис. 1).

В качестве основных длин волн, которые используются в высокоскоростной волоконно-оптической связи в настоящее время [1], приняты 1310 нм (второе окно прозрачности) и 1550 нм (третье окно прозрачности).

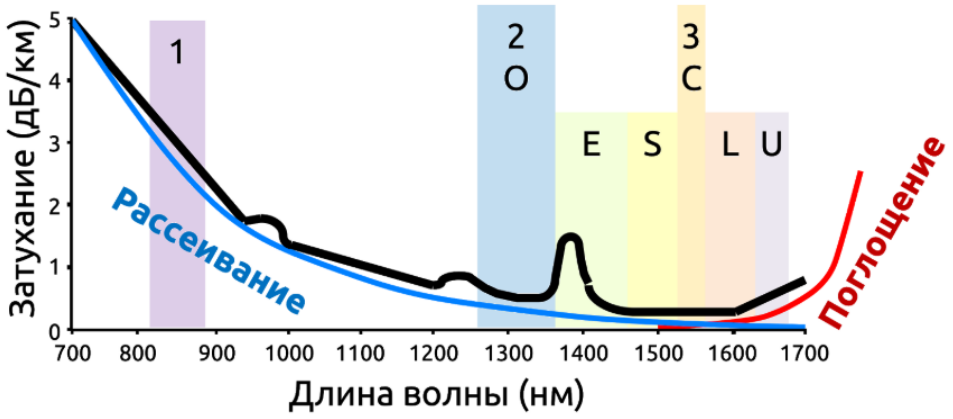


Рис. 1. Окна прозрачности оптического волокна

Изначально системы спектрального уплотнения использовали всего две длины волны – 1310 и 1550 нм (рис. 2). Это были системы, использующие SDH (синхронную цифровую иерархию).

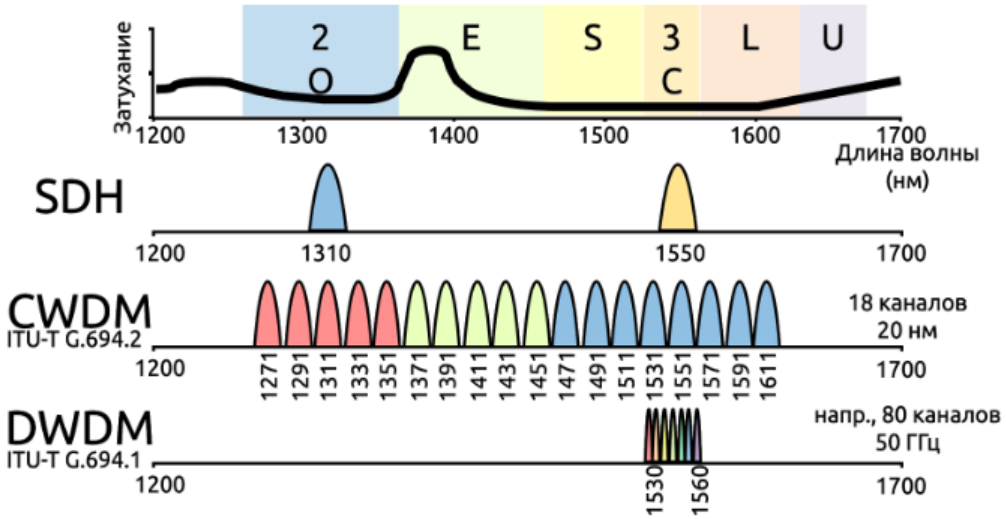


Рис. 2. Разделение спектрального ресурса оптического волокна

С развитием элементной базы технологии разделения были усовершенствованы – появились системы WDM.

WDM – разделение спектрального ресурса оптического волокна между длинами световых волн с последующим мультиплексированием. WDM на текущий момент используется в двух технологиях: CWDM и DWDM.

Технология CWDM (рекомендация ITU-T G.694.2) использует 18 оптических несущих с межканальным интервалом 20 нм [2]. Диапазон системы – от 1271 до 1611 нм. При этом, очевидно, ширина одного канала может достигать 20 нм, при условии, что каналы не накладываются друг на друга.

Технология DWDM (рекомендация ITU-T G.694.1) использует диапазон от 1530 до 1560 нм. При этом возможны различные способы использования этого диапазона - так называемая частотная сетка DWDM. В системах

DWDM принято использовать частоты, а не длины волн. При использовании этого диапазона выбирается частотный план – межканальный интервал. Используется несколько стандартизированных интервалов – 100, 50, 25, 12,5 ГГц [3]. Эти частоты отсчитываются от центральной – 193,1 ТГц, что примерно соответствует длине волны 1552,52 нм. Соответственно, система может обеспечить 40, 80, 160 и 320 каналов в используемом диапазоне (рис. 3).

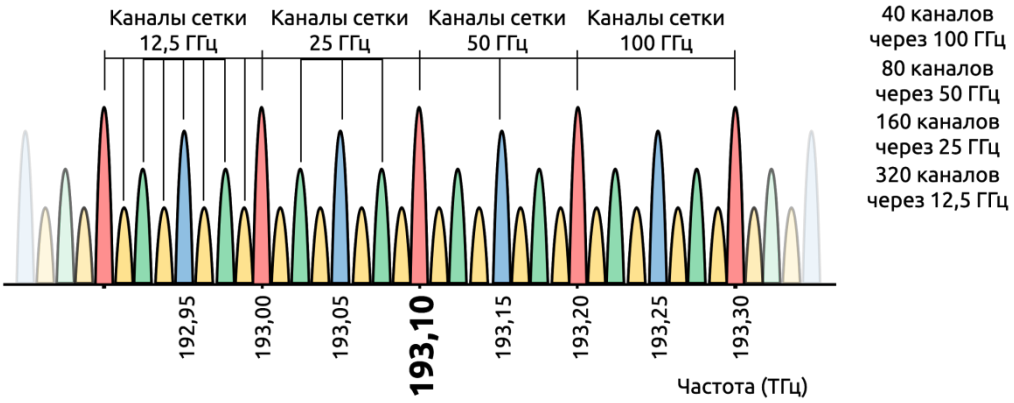


Рис. 3. Частотный план DWDM

Мультиплексоры WDM

В зависимости от используемого частотного плана выдвигаются разные требования к фильтрам в составе мультиплексоров WDM.

Фиксированные многоканальные мультиплексоры изготавливаются на основе AWG-решеток (*Array Waveguide Grating*), а малоканальные могут быть реализованы в виде набора тонкопленочных TFF-фильтров (*Thin Film Filter*). Потери на канал в мультиплексорах на основе AWG-решеток не зависят от числа каналов и составляют примерно 5 дБ.

TFF-DWDM-мультиплексор состоит из фильтрующей структуры (рис. 4, см. ниже) и системы линз, фокусирующих излучение [4]. Фильтрующая структура представляет собой диэлектрическую подложку, на которую закрепляются тонкопленочные фильтры TFF, настроенные на определенную длину волны.

Анализ требований к фильтрам

Рассматривая частотный план систем с разделением спектрального ресурса, можно выделить требования к полосе пропускания фильтра. Например, для выделения центрального канала DWDM при разных частотных планах требуются фильтры с различной избирательностью, но настроенные на одну и ту же длину волны (1552,52 нм). Таким образом, если две волоконно-оптические системы передачи используют системы с интервалом 100

и 50 ГГц соответственно, то ширина полосы из пропускания будет отличаться вдвое. Как было сказано в [5], для систем с интервалом 50 ГГц будут требоваться фильтры с большим количеством слоев, чем для систем с интервалом 100 ГГц, что влечет за собой большие экономические затраты.

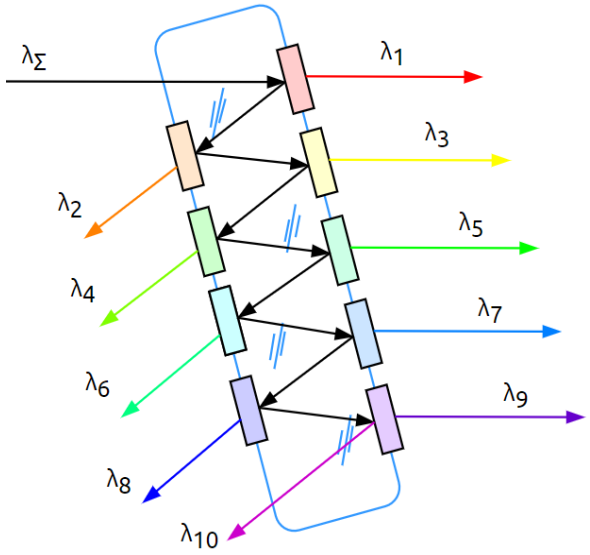


Рис. 4. Фильтрующая структура мультиплексора

Также в [5] было описано, что длина волны λ, нм, на которую настроен фильтр, состоящий из тонкопленочной периодической структуры, определяется формулой:

$$\lambda = 4\tilde{n}d,$$

где d – толщина одного слоя, нм; $\tilde{n}$ – среднее арифметическое показателей преломления двух соседних слоев.

На рис. 5 показаны характеристики пропускания тонкопленочных фильтров с различным количеством слоев. Толщина каждого слоя 433,5 нм. Каждые два слоя образуют период. Показатели преломления двух соседних слоев – 1,752 и 1,748.

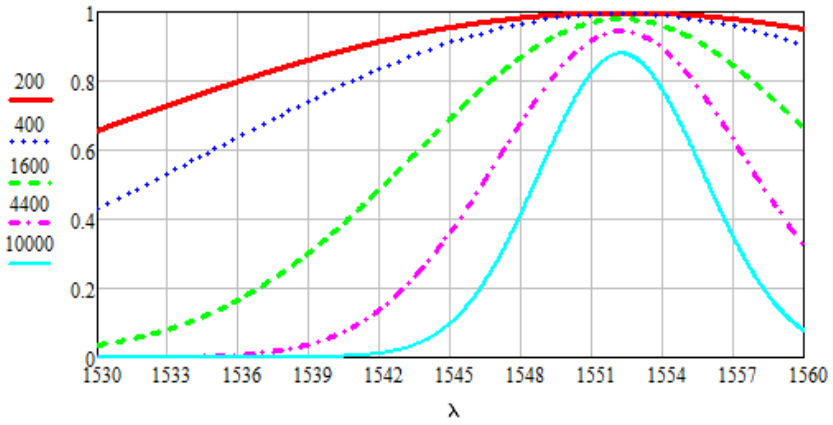


Рис. 5. Характеристики пропускания фильтров с различным количеством слоев

Список используемых источников

1. Листвин В. Н., Трещиков В. Н. DWDM-системы // ФОТОН-ЭКСПРЕСС. 2011. № 1 (89). С. 40–42.

2. Rec. ITU-T G.694.2 Spectral grids for WDM applications: CWDM wavelength grid. Geneva: 2004.

3. Rec. ITU-T G.694.1 Spectral grids for WDM applications: DWDM frequency grid. Geneva: 2012.

4. Основы технологии DWDM [Электронный ресурс]. URL: http://t8.ru/wp-content/uploads/2018/12/About-DWDM.pdf (Дата обращения 25.02.2020).

5. Былина М. С., Резников Б. К. Методика и результаты расчета оптических интерференционных фильтров / Актуальные проблемы инфотелекоммуникаций в науке и образовании. VIII Международная научно-техническая и науно-методическая конференция: сб. науч. ст. в 4-х т. СПб. : СПбГУТ, 2019. Т. 1. С. 193–197.

Статья представлена заведующей кафедрой ФиЛС СПбГУТ, кандидатом технических наук, доцентом М. С. Былиной.

УДК 621.3:004.71
ГРНТИ 49.13.15

ОБЗОР ПРОГРАММИРУЕМЫХ ЛОГИЧЕСКИХ ИНТЕГРАЛЬНЫХ СХЕМ С ОПТИЧЕСКИМИ ИНТЕРФЕЙСАМИ

Б. К. Резников, Г. В. Степаненков, Г. А. Урванцев

Санкт-Петербургский государственный университет телекоммуникаций им. проф. М. А. Бонч-Бруевича

В статье приводится сравнительных анализ программируемых логических интегральных схем, имеющих оптические интерфейсы. Рассматриваются тенденции применения программируемых логических интегральных схем на транспортных сетях и сетях абонентского доступа, а также центрах обработки данных, реализованных по оптическим средам передачи. Рассматривается концепция Softly Defined Network, SDNet.

ПЛИС, программируемая логика, оптическая связь, системы на кристалле, FPGA, SoC, SDNet.

Программируемые логические интегральные схемы

ПЛИС – электронные компоненты, которые используются для создания конфигурируемых цифровых электронных схем. Логика работы ПЛИС определяется посредством программирования [1].

Область применения ПЛИС

Одной из основных областей применения ПЛИС является электрическая связь. На сегодняшний день ПЛИС играют важную роль в сетях электросвязи, сетях центров обработки данных. На рынке ПЛИС особое место занимают две компании – Xilinx и Altera (ныне подразделение компании Intel FPGA).

В качестве основных сред передачи данных используются медная витая пара, коаксиальный кабель и оптическое волокно. При наращивании скорости передачи данных по металлическим средам производители сталкиваются с такими проблемами, как межсимвольная интерференция, джиттер, возвратные и перекрестные потери. При этом необходимо применять корректирующие фильтры, что влечет к увеличению затрат энергии на передачу одного бита (пДж/б).

В настоящее время металлические среды передачи используются на расстояниях до 10 м. При расстоянии более 10 м используется оптическое волокно [2].

В марте 2012 года компания Altera впервые продемонстрировала в работе технологию Optical FPGA. Данная разработка была призвана продемонстрировать возможность увеличения пропускной способности и снизить энергопотребление и стоимость решений, основанных на FPGA. Компания Altera заявила, что интеграция FPGA и оптических приемопередатчиков в одном кристалле позволят удовлетворить растущую потребность в пропускной способности инфокоммуникационной инфраструктуры, преодолеть ограничения, свойственные металлическим и традиционным оптическим технологиям. Разработанная система работала с трафиком 100 Gb Ethernet. В состав интеграции также вошли системы мониторинга температуры и тока смещения лазера.

DARPA и программа PIPES [3]

DARPA – Управление перспективных исследовательских проектов Министерства обороны США – учредило в январе 2018 года программу PIPES (*Photonics in the Package for Extreme Scalability*). Действие программы касалось трех областей разработок: создание технологий для интеграции оптических интерфейсов в состав кристаллов (чипов) и многокристалльных сборок (модулей), разработка технологий и методов передачи данных между чипами и модулями, разработка концепции управления множеством узлов с оптическими интерфейсами. В марте 2020 года были выбраны участники программы: Intel и Xilinx; Национальные лаборатории Сандия, Калифорнийский университет Сан-Диего, Калифорнийский университет Санта-Барбары, Колумбийский университет и Университет Пенсильвании; Калифорнийский университет в Беркли.

Xilinx SDNet [4]

В марте 2014 года компания Xilinx представляет вниманию свой проект под названием SDNet – Softly Defined Networks. SDNet представляет собой специфркационную среду для работы с программно-определяемыми сетями SDN. SDNet позволяет создавать системы обработки пакетной информации, основанных на устройствах Xilinx All Programmable FPGA и SoC. Основные функции среды: системным инженерам доступно подключение дополнительных видов обслуживания без опыта проектирования на ПЛИС, полная поддержка устройств Xilinx All Programmable.

FPGA-ускоритель, как правило, представляет собой аппаратуру в различном форм-факторе (VPX, Com-express, PCIe и т. д.), которая кроме самого чипа FPGA (или нескольких) содержит на плате память типа SRAM и DRAM, включая ультра-новые HBM (память DRAM с высокой пропускной способностью) и высокоскоростные интерфейсы ввода-вывода, такие как популярные 10/40/100 GE и PCI Express.

На рис. 1 изображена структура интерфейсного модуля Xilinx SDNet.

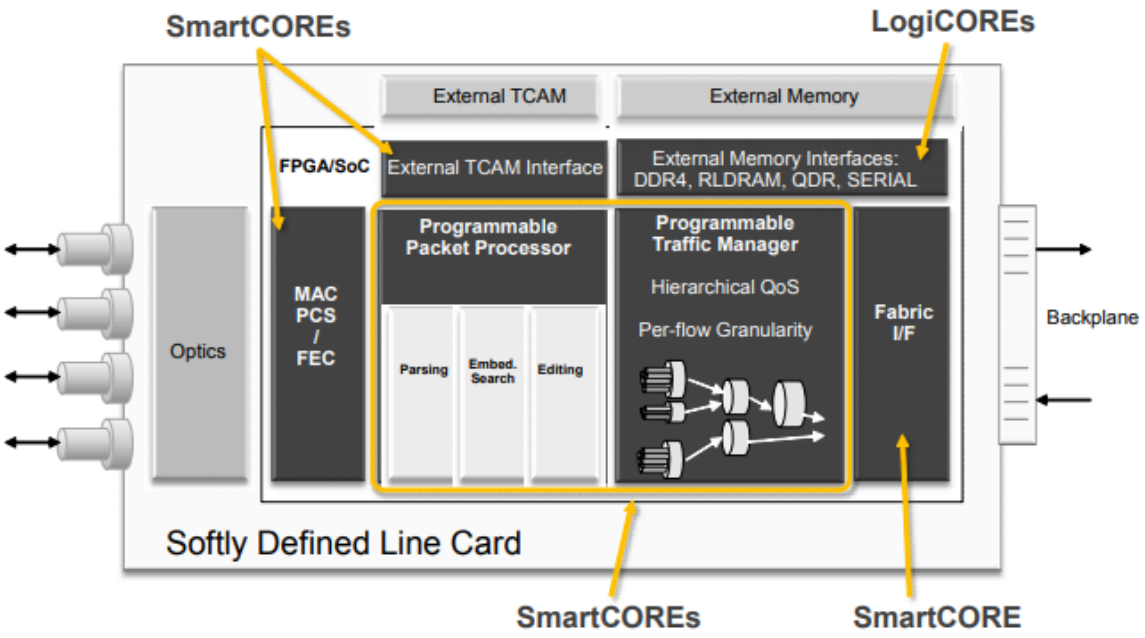


Рис. 1. Интерфейсный модуль Xilinx SDNet

Все составляющие интерфейсного модуля, кроме оптических приемо-передатчиков и внешней памяти, позволяют реализовать поддержку услуг NGN исключительно путем применения программируемых устройств.

На рис. 2 представлены области внедрения SDNet. Как видно, SDNet пригодна для внедрения почти во все ключевые узлы сетей электросвязи: от Core- и Metro-сетей до сетей абонентского доступа, реализованных на различных технологиях, а также центры обработки данных.

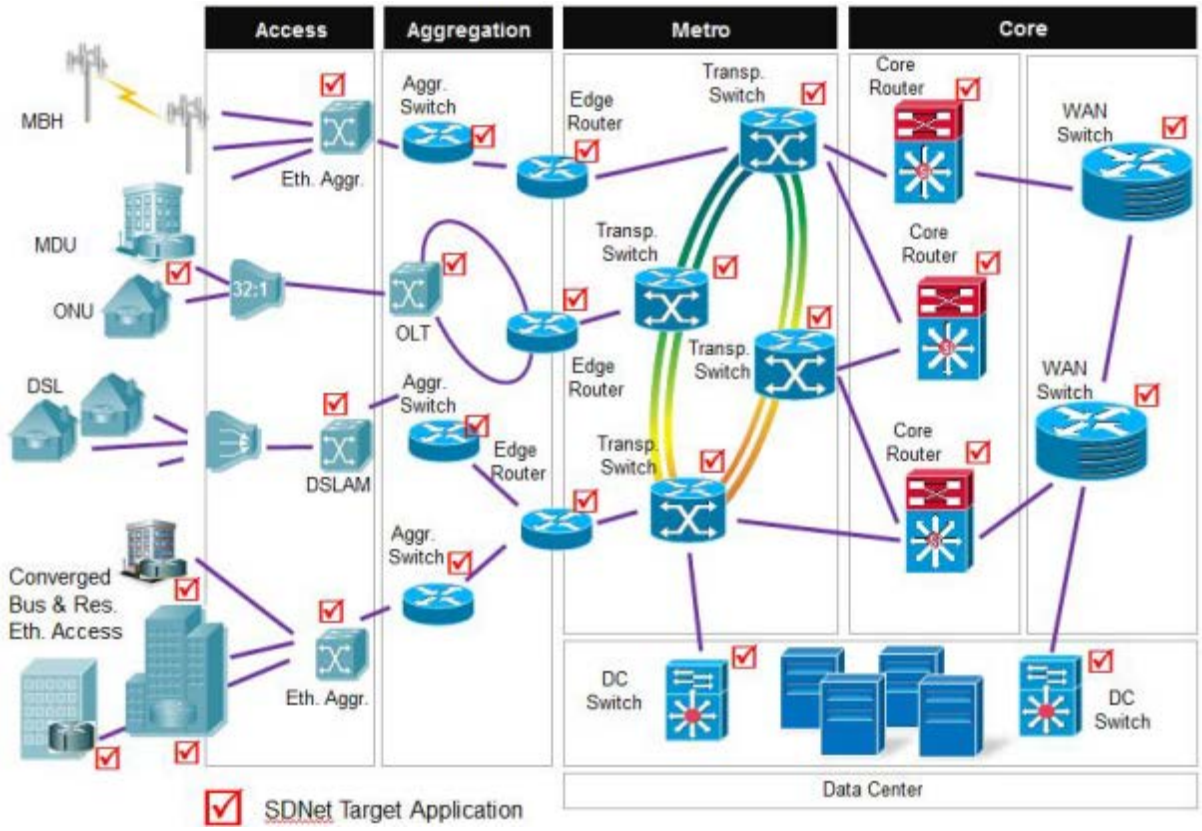


Рис. 2. Области внедрения технологии Xilinx SDNet

В таблице приведены технические характеристики некоторых систем на кристалле SDNet компании Xilinx.

ТАБЛИЦА. Технические характеристики некоторых платформ SDNet

	Скорость передачи одного трансивера, Гб/с	Количество приемо-передатчиков	Скорость передачи (полный дуплекс), Гб/с	Интерфейс для DDR3, Мб/с
Zynq-7000	12,5	16	400	2 400
Artix-7	6,6	16	211	1 066
Kintex-7	12,5	32	800	1 866
Virtex-7	28,05	96	2 784	1 866
Kintex Ultrascale	16,3	46	2 086	2 133
Virtex Ultrascale	32,75	104	5 101	2 133

SDNet представляет собой технологию, которая позволяет проектировщику сетевых систем легко реализовывать новые продукты, дополнительные виды обслуживания, в том числе и SDN. Прорыв SDNet заключается

в том, чтобы сделать системы на кристалле более доступными с помощью методологии высокоуровневого проектирования систем, которая определяет именно цели проектирования, а не пути реализации задач. SDNet – ключевой фактор, позволяющий увеличить производительность труда разработчиков сетевых систем и системных архитекторов путем использования другого подхода к проектированию систем.

Список используемых источников

1. Харрис Д. М., Харрис С. Л. Цифровая схемотехника и архитектура компьютера. Morgan Kaufman, 2013.

2. Андреев В. А., Кочановский Л. Н., Портнов Э. Л. Направляющие системы электросвязи. В 2-х т. Том 1. Теория передачи и влияния; 7-е изд., перераб. и доп. М. : Горячая линия – Телеком, 2009. 424 с. ISBN 13: 978-5-9912-0092-9.

3. DARPA – Researchers Selected to Pursue Photonic Signaling for Microelectronics System Scalability [Электронный ресурс]. URL: http://darpa.mil/news-events/2020-03-16 (дата обращения 20.02.2020).

4. Xilinx – SDNet [Электронный ресурс]. URL: https://www.xilinx.com/ (дата обращения 15.02.2020).

Статья представлена заведующим кафедрой ПИВТ СПбГУТ, кандидатом технических наук, профессором Л. Б. Бузюковым.

УДК 004.056.53
ГРНТИ 81.93.29

РАЗРАБОТКА ПРОГРАММНОГО КОМПЛЕКСА ПО АУДИТУ УСТРОЙСТВ В СЕТЯХ

А. А. Рыжков, А. Ю. Цветков

Санкт-Петербургский государственный университет телекоммуникаций им. проф. М. А. Бонч-Бруевича

Быстрый рост компьютерных сетей приводит к частым ошибкам в их работоспособности. Чтобы обеспечить эффективную работу всей системы, необходима управляющая платформа с интегрированными инструментальными средствами. Данная система позволяет быстро получать информацию о состоянии оборудования, сервисов и оперативно реагировать на возникшие сбои. Такой программный комплекс может собирать, анализировать и хранить поступающую информацию. Введение системы значительно сокращает время на поиск причин ошибок и их устранение.

аудит, компьютерные сети, ping, ICMP, SNMP, syslog, NTP, операционная система.

В любой IT-инфраструктуре аудит информационной системы необходим для того, чтобы системные администраторы своевременно были оповещены о проблемах в сети. Чтобы добиться продуктивной работы всей системы, необходима управляющая платформа с интегрированными инструментальными средствами [1, 2].

Аудитом сети называют процесс системы, выполняющий наблюдение за IT-инфраструктурой в поисках неисправных систем, и который, при обнаружении ошибок, уведомляет администратора для исправления случившейся ситуации [3]. Основной задаче системы аудита является обеспечение информации для анализа состояния сети. Постоянный аудит сети помогает избежать простоев в работе, поддерживать все сервисы в рабочем состоянии и сохранить необходимый уровень качества [4].

По мере развития систем появились составляющие компоненты, которые необходимо поддерживать в работоспособном состоянии. Все части должны правильно функционировать, что достаточно сложно без системы аудита, при создании которой можно столкнуться с некоторыми проблемами [5]:

– Аудит и контроль по частям.

Аудит каждой отдельной части осуществляется специальным программным средством, настроенным на определенную задачу. Однако процесс, который предназначен для поддержки одной части не может поддерживать другую. Использование специализированных инструментов приводит к рассмотрению каждой системы в изоляции, не учитывая окружающие системы, которые влияют на работу исходной.

– Потеря информации.

Знания о системе организации и о том, как решать возникающие проблемы должно быть систематизировано и сохранено. Данное условие поможет в будущем решать и предотвращать возникающие ошибки. Эту проблему решают с помощью создания системы базы данных, которая заполняется по мере появления различных ситуаций.

– Отсутствие связи между пользователем и администратором сети.

Взаимодействие и связь – это основной компонент, который делает работоспособной любую систему. Организация Help Desk – это способ осуществления коммуникаций, который предоставляет пользователю информацию и поддержку.

В начале развития сетевой инфраструктуры функционал для мониторинга сети развивался из менее сложного программного обеспечения. Для получения информации о сети обычно используют утилиту ping, работающую на основе протокола ICMP (*Internet Control Message Protocol*), а также на основе протокола SNMP (*Simple Network Management Proto-*

col) [6, 7]. Современные же решения включают в себя графическое представление детального анализа для всей сети. Система аудита позволяет выполнять следующие важные функции:

– Аудит устройств и сети.

Запрос ping от сервера системы аудита для проверки соединения отправляется к устройству [6]. Если устройство не отвечает на запросы, инструмент аудита отправляет сообщение об ошибке и информирует администратора сети о сбое в работе. Протокол SNMP позволяет собирать информацию от сетевых устройств и серверов, это значит аудит определенных состояний интерфейса устройств и скорости передачи данных. Инструменты для аудита сети могут получать и отправлять сообщения. Протокол Syslog является общим стандартом для отправки сообщений о событиях, которые происходят в системе всех устройств сетевой структуры [6, 7].

– Определение проблем с операционной системой.

Ошибки, которые возникают между сетью и приложением определяются на уровне ОС и любого связующего программного звена, которое влияет на правильную работу сетевой инфраструктуры.

– Анализ данных.

Важный функционал для аудита распределен вокруг анализа полученных данных от приложений. Используя детальную проверку пакетов, определяется большинство сетевых проблем. Сетевая система потоков собирает информацию о приеме/передаче данных сетевыми интерфейсами. Далее информация передается на основной сервер, анализируется с помощью специализированных инструментов для анализа, и администраторы сети могут определить источник и приемник трафика. В итоге, эти данные могут быть использованы для идентификации проблем с конфигурацией или выявления перегруженных участков в сети.

– Определение основной причины ошибки.

Сочетание функций, соединенных и автоматизированных с помощью системы аудита применяется для поиска основной причины проблемы. Сложность функции заключается в том, чтобы добиться сконфигурированности всех устройств. Протокол NTP (*Network Time Protocol*) необходим для синхронизации времени работы устройств [8]. Если данной настройки не будет, то время действий будет отличаться. Это отрицательно скажется на проводимом анализе и вывод информации о причине инцидента будет неверен.

Функционал по аудиту сети способен выполнять детальную диагностику сети, которая включает в себя мониторинг протоколов маршрутизации и вывод сообщений при возникновении каких-либо изменений. Он может быть настроен автоматически оповещать при возникновении ошибок и предпринимать меры по решению проблем.

При разработке и внедрению системы аудита нужно определиться с объектами, которые будут подвергаться слежению, а также показатели, которые определят количество оповещений при ошибках [9, 10].

Для того, чтобы обеспечить постоянную работоспособность необходимо заранее выявлять узкие места в конфигурации систем, а также быстро узнавать о наличии поломки и ее причине.

В данной работе были рассмотрены основные проблемы, возникающие при построении системы аудита и проведен сравнительный анализ основных функций, которые будут включены в работу системы.

Список используемых источников

1. Дмитрюк В. Л., Шмаков Е. А., Киреев А. П., Калмыков Д. В., Новиков В. И. Об использовании системы мониторинга ZABBIX в контролируемой корпоративной среде // Инновационные процессы в науке и образовании. Международная научно-практическая конференция : в 2 ч., Пенза, 05 января 2019 г. М. : ФГБОУ ВО ОГТУ, 2019. С. 61–64.

2. Дмитрюк В. Л., Калмыков Д. В., Новиков В. И. Универсальная система мониторинга ZABBIX // Техноконгресс: сб. тр. XXXV междунар. науч. конф. / Под ред. Никитина П. И., Кемерово : Изд-во Плутон, Точная наука, 2019. С. 2–8.

3. Ушаков И. А., Котенко И. В., Крылов К. Ю. Анализ методик применения концепции больших данных для мониторинга безопасности компьютерных сетей // Информационная безопасность регионов России (ИБРР-2015) : материалы конференции. 2015. С. 75–76.

4. Котенко И. В., Ушаков И. А. Технологии Больших данных для мониторинга компьютерной безопасности // Защита информации. Инсайд. 2017. № 3 (75). С. 23–33.

5. Зыкин М. М., Новиков С. Н. Исследование методов мониторинга телекоммуникационных систем // Первые шаги к науке: материалы магист. науч. сессии, Новосибирск, 2019. М. : СПУГиТ, 2019. С. 105–109.

6. Поляк-Брагинский А. В. Локальные сети. Модернизация и поиск неисправностей. 2 изд. М. : БХВ-Петербург, 2009. 832 с.

7. Таненбаум Э., Уэзеролл Д. Компьютерные сети. 5-е изд. М. : Питер, 2019. 960 с.

8. Красов А. В., Сахаров Д. В., Ушаков И. А., Лосин Е. П. Обеспечение безопасности передачи multicast-трафика в IP-сетях // Защита информации. Инсайд. 2017. № 3(75). С. 34–42.

9. Штеренберг С. И., Полтавцева М. А.Распределенная система обнаружения вторжений с защитой от внутреннего нарушителя // Проблемы информационной безопасности. Компьютерные системы. 2018. № 2. С. 59–68.

10. Василишин Н. С., Ушаков И. А., Котенко И. В. Исследование алгоритмов анализа сетевого трафика с использованием технологий больших данных для обнаружения компьютерных атак // Информационные технологии в управлении (ИТУ-2016) : материалы 9-й конференции по проблемам управления. Председатель президиума мультиконференции В. Г. Пешехонов. 2016. С. 670–675.

Статья представлена заведующим кафедрой ЗСС СПбГУТ, кандидатом технических наук, доцентом А. В. Красовым.

УДК 004.056.53
ГРНТИ 81.93.29

СИСТЕМА ПРОТИВОДЕЙСТВИЯ РАСПРОСТРАНЕНИЮ ВРЕДОНОСНОЙ ИНФОРМАЦИИ В СОЦИАЛЬНЫХ СЕТЯХ

Д. В. Сахаров, В. С. Шашкин

Санкт-Петербургский государственный университет телекоммуникаций им. проф. М. А. Бонч-Бруевича

Любое значимое событие вызывает общественную реакцию и резонанс. Стороны конфликтов используют это явление для ведения информационного противоборства. Современные медиа технологии, массовый доступ людей в сеть интернет и развитие социальных сетей дают огромные возможности для применения практики вброса вредоносной информации для проведения психологических операций. Массовое распространение в социальных сетях вредоносной, в том числе фейковой информации сегодня представляет серьезную угрозу безопасности личности, общества и государства многих стран.

информационная безопасность (ИБ), информационное противоборство, психологические операции, информационная атака, угроза информационной безопасности, вредоносная информация, нежелательная информация, фейки, социальные сети, распространитель вредоносной информации в социальной сети.

Введение

Обратной стороной стремительного развития интернета и создания социальных сетей является то, что они неизбежно становятся объектами и средствами информационного управления сознанием людей, а также ареной информационного противоборства. Социальные сети сегодня – один из ключевых и наиболее эффективных инструментов информационного влияния, в том числе средство для манипулирования личностью, социальными группами и обществом в целом [1, 2].

В информационных войнах объектом воздействия выступает массовое и индивидуальное сознание, а эффективность определяется восприимчивостью населения противоборствующей стороны к восприятию доносимой информации.

Несомненно, средствами ведения информационных войн могут выступать все имеющиеся в наличии средства передачи информации, но наиболее эффективными инструментами являются именно социальные сети. Их преимуществом перед подавляющим большинством средств массовой инфор-

мации является интерактивность. Социальные сети позволяют выражать отношение человека к происходящему и предоставляют для этого различные возможности, создают иллюзию сопричастности [3].

Потенциал информационно-пропагандистского воздействия социальных сетей чрезвычайно высок. Перепроверить информацию, размещенную в Интернете, найти ее первоначальный источник или источник вброса достаточно сложно.

Информационный вброс – это комплекс пропагандистских мероприятий. Суть этого мероприятия проста – резкое создание мнения в обществе, чаще всего негативного.

Мониторинг информации в социальных сетях – это сложный процесс, связанный со стремительным появлением и распространением новых объектов наблюдения. Специфической чертой такого мониторинга является то, что система анализирует и видит, как правило, не всё явление, событие, мероприятие в целом, а только одну или несколько из частных характеристик, например, содержание.

С развитием Интернета всё большее значение стали приобретать фальшивые или фейковые новости, которые используются для манипуляции сознанием людей. Особенно остро вопрос встал во время выборов президента США в 2016 году, на которых победил Дональд Трамп. В настоящее время, в том числе в связи с пандемией короновируса COVID-19, актуальным стал вопрос выявления фейковых новостей в социальных сетях.

Постановка задачи

В настоящее время разработаны различные модели нарушителя ИБ для телекоммуникационных сетей, например, таких как в работе [4]. Цели таких нарушителей могут быть различны от нарушения функционирования сетей до хищения или разрушения циркулирующей в ней информации. В то же время задачей распространителей вредоносной информации в социальных сетях является доведение такой информации до сознания конкретных пользователей. Возникло противоречие между научным обеспечением технических и информационно-психологических аспектов ИБ. Поэтому постановка задачи разработки модели распространителя вредоносной, недостоверной, нежелательной или так называемой фейковой информации в социальных сетях является актуальной.

Решение

По полученным из социальных сетей сведениям аналитики и системы мониторинга могут создавать представление о нарушении в частности или о противозаконной операции в целом. При этом полнота и достоверность воссоздаваемого представления целиком и полностью зависят от пол-

ноты и достоверности выявления частных характеристик объектов и некоторых частных элементов нарушения [5, 6]. Зависят и от их количества, степени изученности предыдущих представлений, которые служат аналогом при формировании оценки выявленного, т. е. от качественного и количественного состава полученных информационных признаков.

Фейки (вредоносная информация, нежелательная информация в социальных сетях) становятся основным источником информационно-сетевых каскадов, в которых основным фактором лавинообразного распространения информации является стадное поведение.

Фейковый аккаунт — это аккаунт, который является недостоверной копией аккаунта какого-либо пользователя, зарегистрировавшегося на том же ресурсе. Распространены фейковые аккаунты в соцсетях, ведущиеся от имени известных людей, вплоть до давно умерших вроде Адольфа Гитлера. Для борьбы с этим явлением настоящие аккаунты известных людей обычно проходят верификацию и потом показываются как верифицированные (подтвержденные) с галочкой или другим аналогичным по смыслу знаком.

Модель фейковой страницы в социальной сети может быть представлена в виде следующей таблицы (табл.).

Так как перед нами стоит задача автоматизировать анализ профилей пользователей, нам требуется составить общую формулу по расчету шанса фейковости страницы.

$$P = \sum_{i=1}^{n} X_i * P_i,$$

где P – вероятность фейковости страницы; P_i – вес признака; n – количество возможных условий по определению фейковости; X_i – переменная, принимающая значение 1 – если условие выполняется, и 0 – если условие не выполнено.

ТАБЛИЦА. Модель фейковой страницы в социальной сети

Признак	Обычный пользователь	Фейк	Вес признака
Дата создания страницы	Сравнительно старые	Страница создана недавно	0,05 – 0,07
Кол-во постов и/или репостов на странице	Посты и/или репосты от разных дат	Несколько постов и/или репостов от одной даты, с незначительно отличающимся временем, с явно прослеживающийся периодичностью	0,1 – 0,2

Признак	Обычный пользователь	Фейк	Вес признака
Дата размещения аватарки	Аватарки с разной датой размещения	Несколько аватарок от одной даты, с незначительно отличающимся временем, с практически идентичной датой установки	0,1 – 0,2
Лайки от потенциально фейковых аккаунтов	Преимущественно лайки от реальных пользователей	Подавляющее большинство лайков от фейковых аккаунтов	0,1 – 0,15
Комментарии от потенциально фейковых аккаунтов	Преимущественно комментарии от реальных пользователей	Подавляющее большинство комментариев от фейковых аккаунтов	0,1 – 0,2
Подписка на группы и сообщества находящиеся в топе	Разнообразные подписки на группы	Преимущественно подписки на самые популярные сообщества	0,05 – 0,08
Наличие фейковых аккаунтов в друзьях	В основном реальные пользователи в друзьях	Подавляющее большинство фейковых аккаунтов в друзьях	0,05 – 0,1

Теперь выведем формулу под наш конкретный случай:

$$P = D * P_D + R * P_R + A * P_A + L * P_L + K * P_K + G * P_G + F * P_F \leq 1.$$

Примем значение P = 0,5 как минимальный порог для признания страницы фейковой.

Вывод

В статье рассмотрен важный инструмент информационного вброса – фейковые страницы, описана модель злоумышленника. Предложена общая формула по расчету шанса фейковости страницы. Определены критерии измерения веса каждого признака, входящего в процесс вычисления фейковости страницы. В дальнейшем предполагается разработка скрипта для автоматизации определения надежности аккаунта в социальной сети и его применения в системе аудита [7].

Список используемых источников

1. Виткова Л. А., Потехин И. Ю., Сахаров Д. В. Проблема выявления информационно-психологического воздействия в информационной инфраструктуре Российской

Федерации // Актуальные проблемы инфотелекоммуникаций в науке и образовании (АПИНО 2017). VI Международная научно-техническая и научно-методическая конференция : сб. науч. ст. в 4-х т. 2017. С. 166–170.

2. Виткова Л. А. Обзор степени разработанности темы мониторинга и противодействия угрозам информационно-психологической безопасности в социальных сетях // Информационные технологии и телекоммуникации. 2018. Т. 6. № 3. С. 1–9.

3. Виткова Л. А., Проноза А. А., Сахаров Д. В., Чечулин А. А. Проблемы безопасности информационной сферы в условиях информационного противоборства // Актуальные проблемы инфотелекоммуникаций в науке и образовании (АПИНО 2018). VII Международная научно-техническая и научно-методическая конференция : сб. науч. ст. в 4-х т. 2018. С. 191–195.

4. Бирих Э. В., Сахаров Д. В. Модель нарушителя распределенной информационно-вычислительной сети // Актуальные проблемы инфотелекоммуникаций в науке и образовании. V Международная научно-техническая и научно-методическая конференция. 2016. С. 235–238.

5. Гамидов Т. О., Десницкий В. А., Дудкина О. С., Сахаров Д. В. Методы и методики анализа нежелательной информации в социальных сетях // Актуальные проблемы инфотелекоммуникаций в науке и образовании (АПИНО 2019). VIII Международная научно-техническая и научно-методическая конференция : сб. науч. ст. в 4-х т. 2019. С. 317–320.

6. Проноза А. А., Виткова Л. А., Чечулин А. А., Котенко И. В., Сахаров Д. В. Методика выявления каналов распространения информации в социальных сетях // Вестник Санкт-Петербургского университета. Прикладная математика. Информатика. Процессы управления. 2018. Т. 14. № 4. С. 362–377.

7. Костарев С. В., Липатников В. А., Сахаров Д. В. Модель процесса передачи результатов аудита и контроля в автоматизированной системе менеджмента предприятия интегрированной структуры // Проблемы информационной безопасности. Компьютерные системы. 2015. № 2. С. 120–125.

УДК 004.41.42
ГРНТИ 81.96

АНАЛИЗ ПРОТОКОЛА АНОНИМНОГО ВЫЧИСЛЕНИЯ ТОЧЕК ИНТЕРЕСА ПОЛЬЗОВАТЕЛЯ НА ОСНОВЕ СЕГМЕНТАЦИИ КАРТЫ ПРИВЯЗКИ

Е. А. Серёжин, В. А. Яковлев

Санкт-Петербургский государственный университет телекоммуникаций им. проф. М. А. Бонч-Бруевича

Проведен анализ протокола скрытого определения местоположения точек интереса мобильного пользователя с учетом типа POI, с использованием гомоморфных криптосистем Пэйе и Рабина. Рассматривается вариант, когда карта местности имеет

большие размеры и содержит много POI. В результате сервер может получить большое количество запросов, что приведет к большому объему обмениваемой информации между пользователями и сервером. С целью снижения вычислительной нагрузки на сервер и уменьшения времени получения ответа от сервера предложена модификация протокола путем сегментации карты привязки и применения двухэтапного запроса, в результате чего уменьшается объем передаваемой информации от сервера к пользователю. Приведены количественные характеристики эффективности протокола.

анонимное вычисления, точки интереса, геокарты, гомоморфное шифрование.

Одно из направлений защиты персональных данных заключается в решении задачи обеспечения анонимности запросов пользователей к сетевым ресурсам и в частности, обеспечение скрытого получения мобильным пользователем координат точек своего интереса (*Points of interest*, POI).

В [1, 2] приведено описание и анализ протокола скрытого определения точек интереса мобильного пользователя. Пользователь имеет карту местности, разделённую на $n \times n$ ячеек, каждая из которых $M \times M$ метров. В каждой ячейке располагается точки интереса пользователя (гостиница, кафе, парковка и т. д.) закодированными числами d. Пользователь, находясь в ячейке (a, b), хочет узнать координаты точек интереса типа t в ячейке (i, j). Для этого он обращается к серверу по открытому каналу. Сервер имеет базу данных всех точек интереса и на запрос пользователя предоставляет ему такую информацию. Целью протокола является получение информации о ближайших POI определенного типа без раскрытия серверу другим пользователям своего местоположения и типа запрашиваемых точек интереса.

Протокол состоит из четырех алгоритмов: генерация ключей, формирование запроса пользователя, формирование ответа сервера, получение ответа пользователем.

Генерация ключей

Пользователь генерирует две пары (закрытых, открытых) ключей. Первая пара ключей $-\{p_1, q_1\}, \{g_1\ N_1\}$, вторая пара ключей $-\{p_2, q_2\}, \{g_2\ N_2\}$, $p_1 * q_1 = N_1,\ p_2 * q_2 = N_2$, где $N=p*q$.

Открытые ключи должны соответствовать условиям:

1. $g\ mod\ 4 = 3$.

2. Числа g генерируются из множества $Z^*{}_{N^2}$, удовлетворяющие условию:

$$\gcd(g^{\lambda} mod N^2 - 1, N) = 1.$$

где, λ – наименьшее общее кратное чисел $(p-1)$ и $(q-1)$, $Z^*{}_{N^2}$ – множество целых чисел, взаимно простых с N^2.

3. Числа $p_2,\ q_2,$ должны соответствовать диапазону $\sqrt{N^2{}_1 \cdot 100} < p_2,\ q_2 < \sqrt{N^4{}_1}$.

Формирование запроса пользователя

Сначала пользователь, используется алгоритм шифрования Пэйе, вычисляет криптограммы: для t типа запрашиваемой точки интереса, используя первый ключ.

Для этого для каждого $l \in \{1, 2, \dots, m\}$, где $-\ m$ число типов точек интереса, пользователь выбирает случайное целое число $r_l \in Z^*{}_{N_1}$ и вычисляет криптограммы c_l:

$$c_l = \begin{cases} Encrypt\ (1, pk_1) = \ {g_1}^1 {r_l}^{N_1} \left(\mathrm{mod}\ {N_1}^2\right), \text{если } l = t \\ Encrypt\ (0, pk_1) = \ {g_1}^0 {r_l}^{N_1} \left(\mathrm{mod}\ {N_1}^2\right), \text{если } l \neq t. \end{cases}$$

Далее пользователь вычисляет криптограммы первой своей координаты, используя второй ключ.

Для каждого $l' \in \{1, 2, \dots, n\}$, где n – размер карты, пользователь выбирает случайное целое число $r_{l'} \in Z^*{}_{N_2}$ и вычисляет криптограммы $c'_{l'}$:

$$c'_l = \begin{cases} Encrypt\ (1, pk_2) = \ {g_2}^1 {r'_{l'}}^{N_2} \left(mod\ {N_2}^2\right), \text{если } l = i \\ Encrypt\ (0, pk_2) = \ {g_2}^0 {r'_{l'}}^{N_2} \left(mod\ {N_2}^2\right), \text{если } l \neq i, \end{cases}$$

где i – первая координата ячейки, в которой находится пользователь.

Далее пользователь шифрует вторую свою координату j на втором открытом ключе, выбирает случайное целое число $r \in Z^*{}_{N_2}$ и вычисляет еще одну криптограмму c:

$$c = Encrypt(j, pk_2) = \ {g_2}^j r^{N_2}\ \left(\mathrm{mod}\ {N_2}^2\right).$$

Далее пользователь отправляет открытые ключи $(g_1\ N_1, g_2\ N_2)$ и запрос $(c_l\ c'_l\ c)$ серверу.

Формирование ответа сервером

Сервер, получив запрос пользователя вместе с открытыми ключами, используя шифрование Рабина и Пэйе, вычисляет $\mathrm{C}_{\alpha,\beta}$ на первом открытом ключе, где $\alpha \in \{1, 2, \dots, n\}$, $\beta \in \{1, 2, \dots, n\}$, $d_{\alpha,\beta,l}$ – составное число определяющее координат и типа POI:

$$C_{\alpha,\beta} = \prod_{l=1}^{m} {c_l}^{{d_{\alpha,\beta,l}}^2} (\mathrm{mod}\ {N_1}^2)\ .$$

Далее происходит повторное шифрование второй координаты j на втором открытом ключе.

Для каждого $\beta = \{1,2, \dots, n\}$ выбирается ω_β – целое число из множества $Z^*{}_{N_2}$ и вычисляется ответ $R = \{C_1, C_2, \dots, C_n\}$:

$$C_\beta = \left(\frac{c}{g^\beta}\right)^{\omega_\beta} \prod_{\alpha=1}^{n} {c'}_\alpha{}^{C_{\alpha,\beta}{}^2} \left(\mathrm{mod}\ {N_2}^2\right).$$

Сервер отправляет вычисленные криптограммы $R = \{C_1, C_2, \dots, C_n\}$ пользователю.

Получение ответа пользователем

Пользователь выбирает только криптограмму C_j, которая соответствует его запросу и расшифровывает ее в следующем порядке.

$$C'_j = PallierDecrypt(C_j, sk_2),$$

$$C''_j = RabinDecrypt(C'_j, sk_2),$$

$$C'''_j = PallierDecrypt(C''_j, sk_1),$$

$$d = RabinDecrypt(C'''_j, sk_1),$$

где sk – секретный ключ, d – информация запрашиваемая информация о точке интереса.

В результате пользователь получает нужную информацию d о ближайших точках типах t относительно своей ячейки.

Наибольшую сложность в протоколе составляет в третий алгоритм – шифрование всех точек. Временная сложность этого алгоритма $O(n^2)$.

При больших размерах карты, большом количестве запросов, ограниченных ресурсах сервера формирование ответа может привести к перегрузке сервера и увеличению времени создания ответа.

Для устранения этого недостатка предлагается следующая модификация протокола. Карта разделяется на сегменты, каждая из которых содержит $n \times n$ ячеек, в том числе ячейку в которой находится пользователь. Пользователь знает координаты своей ячейки в этом сегменте.

В этой модификации протокола вводится дополнительный этап – формирование открытого и закрытого ключа сервера. В результате содержит следующие алгоритмы:

– Формирование открытого (g, n) и закрытого ключа сервера и передача открытого ключа пользователю.

– Формирование запроса $s, c_l, {c'}_l, c$, где s – зашифрованный номер сегмента.

– Формирование ответа сервером.

– Получение ответа пользователем.

Рассмотрим первый и второй алгоритм более подробно.

Сервер генерирует и отправляет маскирующие сообщение $X=Encrypt(x)$, зашифрованное по схеме Пэйе, пользователю вместе с открытым ключом (g, n). Пользователь формирует криптограмму m сегмента, используя гомоморфное свойство криптосистемы Пэйе.

$$s = X * g^m \bmod n^2.$$

И включает его в запрос серверу. Количество криптограмм в этом случае определяется размерами сегмента, а не всей карты. Длинна запроса в данном случаи будет меньше, так как размер криптограммы координат не превышает размеры сегмента.

Сервер получив запрос, расшифровывает номер сегмента с вычетом маскирующего сообщения.

$$Decrypt(s) - x = m.$$

Сервер использует параметры сегмента для формирования ответа. Поскольку в сегменте существенно меньше ячеек, это снижает объем вычислений.

На таблице представлены параметры исходного и модифицированного протокола.

ТАБЛИЦА. Сравнение параметров исходным и модифицированным протоколом

Параметры протоколов	Исходный протокол	Протокол формирования сегмента
Размер карты (сегмента), км	100×50	10×10
Размер ячейки, м	100×100	100×100
Количество ячеек	500 000	10 000
Количество криптограмм в запросе c'_l	10 000	1 000
Количество криптограмм $C_{\alpha,\beta}$	500 000	10 000
Количество криптограмм в ответе C_β	10 000	1 000

Из таблицы видна существенная разница в количестве посылаемых от пользователя к серверу криптограмм. При одинаковых размерах ячеек, исходному протоколу нужно обработать 500 000 ячеек, а при сегментировании 10 000.

Предложен альтернативный вариант модификации протокола. Вместо сегментации всей карты, пользователь сам создает сегмент n×n случайным центром, внутри которого находится пользователь. Используя открытый

ключ сервера, он создает криптограмму шифруя криптограмму параметры сегмента.

Также возможен третий вариант модификации протокола. Пользователь создает сегмент из случайных ячеек и среди них одна ячейка, интересующая пользователя. Далее он шифрует открытым ключом сервера созданный сегмент и отправляет криптограмму вместе с запросом.

Таким образом, модернизация протокола путем сегментации карты привязки, позволяет уменьшить вычислительную нагрузку и время передачи ответа. Если в приведенном примере необходимо обработать 500000 ячеек всей карты, то при сегментации всего 10000 ячеек. Также серверу нужно меньше выделять памяти на шифрование POI, что позволить распределить ее на другие задачи. Однако уменьшение объема информации идет, которой обмениваются пользователь и сервер, за счет дополнительного алгоритма шифрования сегмента.

Список используемых источников

1. Yi X. et al. Practical k nearest neighbor queries with location privacy // 2014 IEEE 30th International Conference on Data Engineering. IEEE, 2014. PP. 640–651.

2. Rohilla A., Khurana M., Singh L. Location privacy using homomorphic encryption over cloud //International Journal of Computer Network and Information Security. 2017. Vol. 11. №. 8. P. 32.

УДК 004.41.42
ГРНТИ 81.96

АНАЛИЗ СТОЙКОСТИ ПРОТОКОЛОВ ФОРМИРОВАНИЯ КЛЮЧА НА ОСНОВЕ ИСПОЛЬЗОВАНИЯ ПРОГРАММЫ AVISPA

Ю. Д. Сизова, В. А. Яковлев

Санкт-Петербургский государственный университет телекоммуникаций им. проф. М.А. Бонч-Бруевича

Рассматриваются характеристики и возможности программы AVISPA по автоматическому анализу безопасности криптографических протоколов. На основе программы сделан анализ протокола формирования ключа Диффи-Хеллмана, протокола на основе магнитометрических данных MagPairing. Сделаны предложения по использованию программы AVISPA в учебном процессе при изучении дисциплины «Криптографические протоколы».

аутентификация, программа AVISPA, анализ безопасности, криптографические протоколы, Диффи-Хеллман, MagPairing.

Одним из инструментов анализа защищенности протоколов передачи данных является использование программы AVISPA (*Automated Validation of Internet Security Protocols and Applications*), позволяющей не только находить уязвимости у того или иного протокола, но и определять возможные атаки на него [1]. В работе проведен анализ протоколов распределения ключей программой AVISPA и сделаны предложения по её использованию в учебном процессе.

AVISPA представляет собой инструмент для автоматизированного анализа безопасности криптографических протоколов. На рис. 1 представлено окно программы и опции, доступные в нём. Главное окно AVISPA представляет собой область для описания протокола на языках HLPSL или CAS+. В верхней части окна расположено меню, позволяющее открыть и сохранить HLPSL и CAS+ файлы. Внизу расположена панель с кнопками: «сохранить файл», «показать CAS+», «показать HLPSL», «симуляция протокола», «симуляция нарушителя» и «активный перехват» [2].

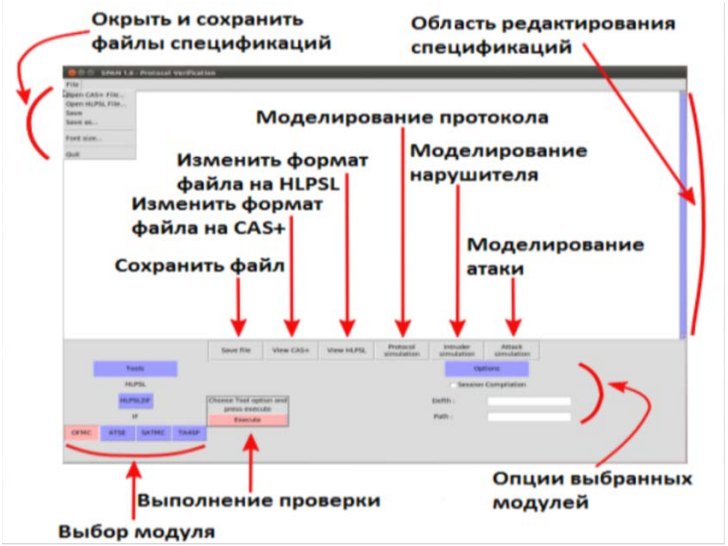


Рис. 1. Интерфейс программы AVISPA

Кнопка «Protocol simulation» позволяет в интерактивном режиме увидеть порядок обмена сообщениями между пользователями. Кнопка «Intruder simulation», позволяет добавить в схему обмена сообщениями злоумышленника. С помощью кнопки «Attack simulation» можно увидеть схему атаки с участием злоумышленника, при условии, что такая обнаружилась в ходе анализа. При использовании языка CAS+ в можно компилировать CAS+код в синтаксис языка HLPSL, который затем переводится в более низкоуровневый язык IF, за счет которого и осуществляется верификация [2].

Архитектура программы AVISPA включает в себя: транслятор HLPSL2IF, который переводит описание протокола из HLPSL в специальный Intermediate Format и четыре модуля верификации OFMC (*on-the-fly Model-Checker*), AtSe (CL-*based Attack Searcher*), SATMC (SAT-*based Model-Checker*), TA4SP (*Tree Automata-based Protocol Analyser*).

Анализ безопасности протокола производится следующим образом: код протокола на языке CAS+ подается на вход одного из четырех модулей, затем программа на основе встроинной логики ищет возможность перехвата передаваемых сообщений по конкретным каналам связи, описанным в коде протокола. В данной статье для анализ протоколов был использова модуль OFMC. Модуль OFMC, является анализатором моделей и включает в себя два метода анализа: использование инертных типов данных, позволяющих сократить бесконечное пространство состояний до конечного и применение метода моделирования злоумышленника согласно модели Долева-Яо [3]. Для сокращения числа вариантов поиска строится редуцированная модель за счет рассмотрения бесконечных типов данных и оперирования свободными переменными.

В модуле OFMC реализован подход, в ходе которого вводится символическое представление инертного нарушителя вместо изменения нумерации сеансов протокола, а вместо имен вводятся роли участников, обозначаемые переменными. В процессе поиска переменные унифицируются и принимают значения, равные именам участников, либо остаются переменными [1].

Проведем анализ безопасности протокола распределения ключей Диффи-Хеллмана [4].

При нажатии на кнопку «Protocol simulation» в главном окне программы можно увидеть порядок обмена сообщениями между пользователями по протоколу Диффи-Хеллмана. Описание протокола Диффи-Хеллмана в синтаксисе языка CAS+ представлено на рис. 2.

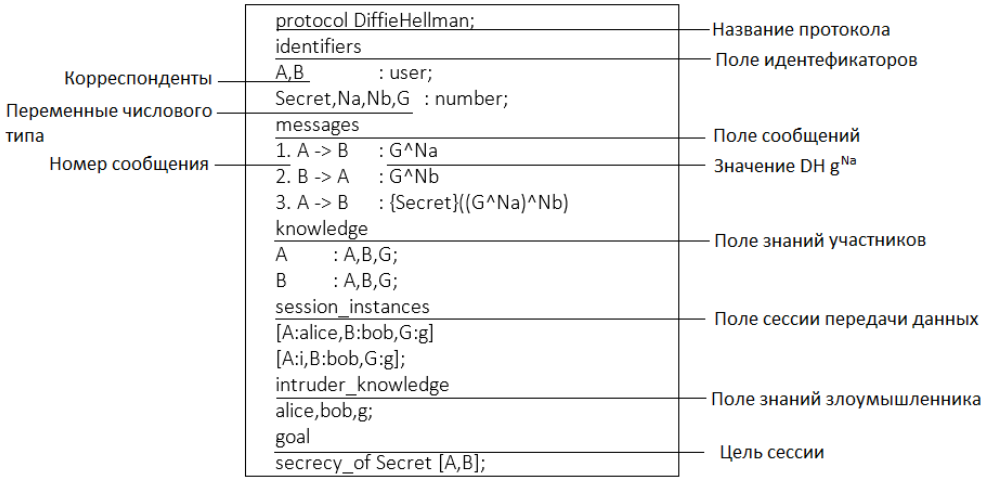


Рис. 2. Код протокола DH

Тип передачи сообщений корреспондентами в протоколе описан по модели Долева – Яо, в соответствии с которой оценка возможности противостоять противнику в канале связи осуществляется на основе сетевого графа. Противник помимо прослушивания трафика может производить быструю подмену сообщений в определенных ветвях графа. Последнее, в частности означает, что воздействие противника приравнивается к воздействию некоторого шума в обобщенном канале связи. В поле сессии передачи данных помимо передачи сообщений Алисы и Боба друг с другом так же добавлена возможность моделирования нарушителя под видом Алисы. Целью данной сессии будет проверка секретности формируемого общего ключа.

Результат атаки на протокол выводится на экран программы (рис. 3), после чего успешно реализованные атаки (если программа нашла уязвимость в протоколе) можно наглядно воспроизвести симуляцией активного перехвата (рис. 4).

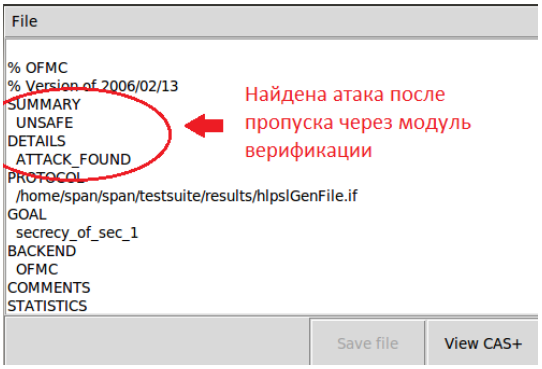


Рис. 3. Запись о нахождении атаки на протокол DH

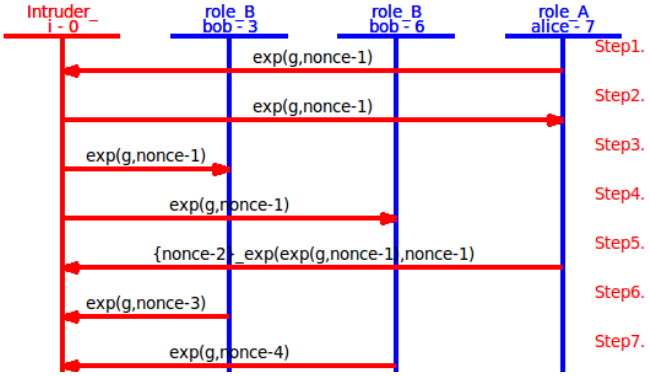


Рис. 4. Визуализация атаки на протокол DH

Очевидно, что перехватив сообщение exp(g,nonce-1) злоумышленник осуществляет обмен сообщениями не напрямую между A и B, а через себя, что позволяет подменять сообщения. Таким образом, протокол DH не защищен от атаки «человек посередине».

Проведем далее анализ безопасности протокола на основе магнитометрических данных MagPairing, описание которого приведено в [5].

Когда два смартфона расположены рядом, их магнитометры считывают магнитные поля практически в одной точке, это позволяет использовать показания магнитных датчиков для генерирования совпадающих с большой вероятностью случайных битовых последовательностей, позволяющих аутентифицировать ранее рспределенный ключ Диффи-Хеллмана и тем самым предотвраить атаку «человек посередине»[6].

Описание протокола аутентификации на основе магнитометрических данных MagPairing в синтаксисе языка CAS+ приведено на рис. 5.

```
identifiers
A,B : user;
Secret,C01,D01,C1,D1,C02,D02,C2,D2,E01,E1 : number;
messages
1. A -> B : C01,C1
2. B -> A : D01,D1
3. A -> B : C02,C2
4. B -> A : D02,D2
knowledge
A : A,B,C01,C1,C02,C2;
B : A,B,D01,D1,D02,D2;
session_instances
[A:alice,B:bob,C01:c01,D01:d01,C1:c1,D1:d1,C02:c02,D02:d02,C2:c2,D2:d2,E01:e01,E1:e1];
Intruder_knowledge
alice,bob,e01,e1;
goal
secrecy_of Secret [A,B];
```

Рис. 5. Описание протокола MagPairing

После пропуска кода через модуль OFMC была выявлена атака на протокол (рис. 6). Затем была проведена визуализация перехвата сообщений злоумышленником (рис. 7), из которой следует, что используя атаку «человек посередине», нарушитель может установить соединение с одним из корреспондентов, выдав себя за другого корреспондента, что позволяет сделать вывод о недостаточной стойкости данного протокола аутентификации ключей.

```
File

% OFMC
% Version of 2006/02/13
SUMMARY
  UNSAFE
DETAILS
  ATTACK_FOUND
PROTOCOL
  /home/span/span/testsuite/results/hlpslGenFile.if
```

Рис. 6. Запись о нахождении атаки на протокол MagPairing

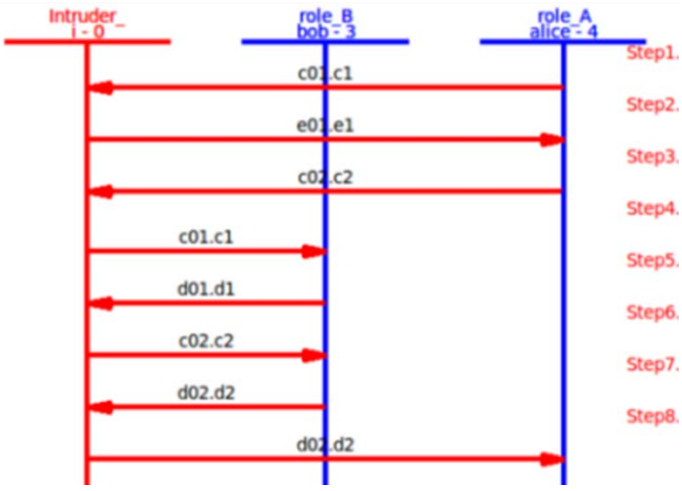


Рис. 7. Визуализация атаки на протокол MagPairing

На основе программы автоматизированного анализа протоколов безопасности AVISPA были проанализированы протокол Диффи-Хеллмана и протокол на основе магнитометрических данных MagPairing. Анализ позволил обнаружить уязвимости и атаки.

В перспективе планируется исследовать протокол MagPairing на основе магнитометрических данных, с использованием универсальных хэшфункций и протокол аутентификации с участием доверенного центра с применением физически не клонируемых функций.

Целесообразно при изучении дисциплины «криптографические протоколы» введение курса лабораторных работ, по использованию программы

AVISPA в учебный процесс, а именно по исследованию протоколов безопасности, по изучению основ языка CAS+ для модификации протоколов и по обнаружению атак при работе с модулями OFMC, AtSe, SATMC, TA4SP.

Список используемых источников

1. Черемушкин А. В. Криптографические протоколы. Основные свойства и уязвимости: учебное пособие. М . : Изд. центр «Академия», 2009. 272 с.

2. Программа AVISPA+SPAN Project Number: IST-2001-39252. URL: http://www.avispa-project.org/

3. D. Dolev, A. Yao. On the security of public Key Protocols // IEEE Transactions on Information Theory, 29 (2):198–208, Mar., 1983.

4. Diffe M., Hellman M. New directions in cryptography // IEEE Transactions on Information Theory. 1976. vol. 22, no. 6, pp. 644–654.

5. Jin R., Shi L., Zeng K., Pande A., Mohapatra P. MagPairing: Pairing Smartphones in Close Proximity Using Magnetometer // IEEE Transactions on Information Forensics and Security. 2016. no. 6, pp. 1304–1319.

6. Яковлев В. А. Аутентификация ключей, распределяемых методом Диффи–Хеллмана, для мобильных устройств на основе аутентифицирующих помехоустойчивых кодов и магнитометрических данных // Тр. СПИИРАН, 18:3 (2019), 706–741.

УДК 004.421
ГРНТИ 50.41.25

ПРИЁМ СЕТЕВЫХ ПАКЕТОВ В JAVA НА КАНАЛЬНОМ УРОВНЕ С ИСПОЛЬЗОВАНИЕМ КОЛЬЦЕВОГО БУФЕРА

А. В. Тарлыков

Санкт-Петербургский государственный университет телекоммуникаций им. проф. М. А. Бонч-Бруевича

В статье рассмотрен вопрос повышения скорости приёма сетевых пакетов для платформы Java с использованием таких механизмов ядра Linux, как пакетные сокеты и отображаемые в память кольцевые буферы. Рассмотрен формат кольцевого буфера версии TPACKET_V3 и возможность его непосредственного использования прикладным кодом платформы Java. Приведены результаты применения предлагаемого подхода на реальной задаче.

пакеты, кольцевой буфер, linux, java.

При разработке высоконагруженных сетевых приложений достаточно часто встаёт задача минимизации затрат на приём и обработку сетевых пакетов, это могут быть пакеты как стандартного типа, например – UDP, так и пакеты частных протоколов системы. В случае разработки системы на основе платформы Java [1] возникают дополнительные вопросы при разработке сетевой подсистемы, это связано с ограниченными возможностями стандартной библиотеки в этой части. Так, в библиотеке представлена возможность использования UDP пакетов, но присутствуют достаточно высокие накладные расходы, связанные с многократным копированием данных и большим количеством системных вызовов – нет возможности группового приёма пакетов.

Возможным вариантом снижения накладных расходов является разработка дополнительных внешних библиотек с использование инструментария java native interface [2] и использования специальных функций для приёма группы пакетов за один системный вызов (например, *recvmmsg* [3]). Этот вариант позволяет повысить пропускную способность приёма пакетов и, в ряде случаев, снизить нагрузку на систему сборки мусора путём отказа от использования промежуточных буферов. Тем не менее, в случае сильного роста объёма принимаемых сетевых пакетов, такой подход оказывается ограничен сетевым стеком операционной системы, потребляющим достаточно много ресурсов на обработку и доставку принятых пакетов прикладному приложению.

а) поток пакетов б) приём 1 / 16 / 256 пакетов за вызов

Рис. 1. Загрузка системы при групповом приёме

Как можно видеть из рис. 1, простой приём потока величиной 500 Kpps без обработки пакетов приводит к сильной загрузке ядра процессора, выделенного на обработку. Использование режима группового приёма снижает суммарную нагрузку на несколько процентов.

Одним им путей дальнейшего снижения накладных расходов является переход к получению сетевых пакетов на втором, канальном уровне модели OSI [4] – использованию пакетных сокетов (AF_PACKET [5]) с поддержкой кольцевого буфера. Подобный вариант позволяет исключить большую часть обработки принимаемых пакетов сетевым стеком, пакеты передаются приложению практически сразу после приёма сетевым драйвером. Но дан-

ный подход не лишён и подводных камней, в частности, приложение получает доступ ко всему потоку пакетов сетевого интерфейса, что приводит к необходимости фильтрации поступающих данных.

При использовании кольцевого буфера для приёма пакетов существует поддержка нескольких версий данного режима, в данной статье будет рассмотрена третья версия (TPACKET_V3 [5, 6]), как наиболее производительная. Буфер представляет собой последовательную область памяти, разделённую на блоки одинакового размера. Блоки, в свою очередь, также делятся на фреймы одинакового размера (рис. 2). Таким образом, объём используемого программой буфера указывается с использованием размера фрейма, количества фреймов на один блок и количества блоков. Данный формат буфера является общим для всех версий режима приёма, тем не менее, используется буфер по-разному, в зависимости от режима. Так, для рассматриваемой версии, деление блоков на фреймы носит сугубо условный характер и используется только для указания размера блока, в процессе приёма сетевых пакетов деление на фреймы не используется, формат блока определяется отдельно.

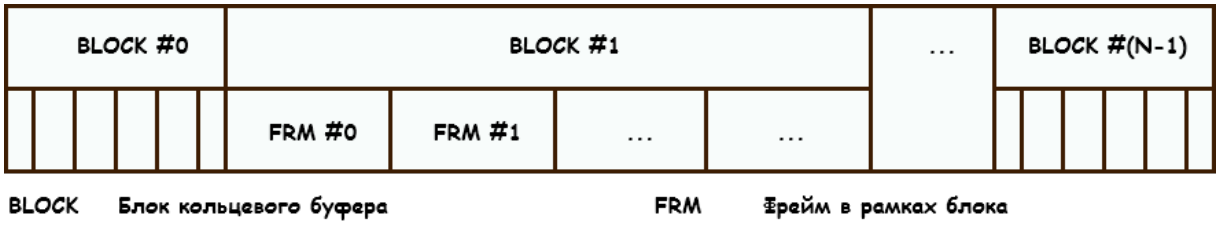


Рис. 2. Общий формат кольцевого буфера

Каждый блок имеет заголовок, описывающийся структурой tpacket_block_desc, в составе которой находятся такие поля, как block_status, num_pkts и offset_to_first_pkt. Поле block_status указывает текущего «владельца» данного блока – ядро системы (TP_STATUS_KERNEL) или пользовательский процесс (TP_STATUS_USER). Ядро обеспечивает приём и асинхронное размещение пакетов в блоках, относящихся к ядру, после формирования блока ядро меняет «владельца» блока, сигнализируя пользовательскому процессу о возможности обработки соответствующего блока. После обработки блока пользовательский процесс должен сменить «владельца», что позволит ядру использовать данный блок для дальнейшего приёма пакетов. После формирования блока ядром и доступности его пользовательскому процессу, поля num_pkts и offset_to_first_pkt указывают количество принятых пакетов в блоке и смещение в блоке до первого пакета (рис. 3).

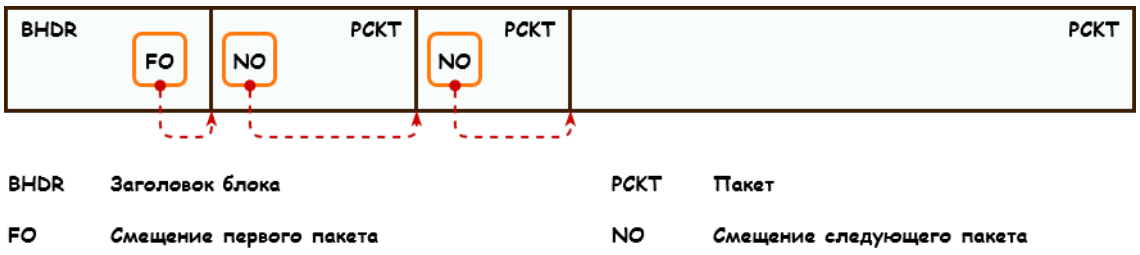


Рис. 3. Структура блока после приёма пакетов

Размещённые в блоке пакеты имеют заголовки определённого формата, описываемого структурой tpacket3_hdr. Данная структура включает такие поля, как tp_next_offset – смещение следующего пакета относительно текущего, tp_mac – смещение заголовка канального уровня и tp_net – смещение к данным сетевого уровня в рамках пакета. Использование данной информации позволяет прикладному приложению фильтровать необходимые пакеты и обрабатывать их.

Таким образом, использование режима кольцевого буфера достаточно просто и в случае прикладного кода, имеющего доступ к стандартным функциям ядра, реализуется достаточно прозрачно, по следующей схеме:

– создание сокета и указание используемого режима,
– задание режима кольцевого буфера и его размера,
– предоставление доступа прикладному процессу к буферу,
– циклическая обработка пакетов блоками.

В случае же прикладной системы, реализуемой на платформе Java, возникает несколько проблем: первая – использование функций ядра решается достаточно просто с использованием инструментария java native interface, вторая и основная – обеспечения доступа к кольцевому буферу – может быть решена несколькими способами. Самым простым вариантом является последовательный разбор принимаемых блоков на уровне внешней библиотеки, реализованной с использованием jni, и копирование необходимых пакетов в структуры, доступные программной части, реализуемой на языке Java. Для оптимизации данного похода можно использовать стандартные механизмы класса ByteBuffer [7], позволяющего выделять фиксированные блоки памяти, доступ к которым из внешней библиотеки достаточно прост и не имеет сильных накладных расходов.

Другим вариантом является предоставление прикладному Java коду прямого доступа к области памяти кольцевого буфера. Данный вариант лишён недостатков предыдущего варианта и обеспечивает максимальную скорость. Проблемой в данном случае является отсутствие стандартных безопасных механизмов для реализации подобного доступа. Тем не менее, решить подобную задачу можно следующим образом. Используемый в первом сценарии класс ByteBuffer при функционировании в режиме direct [ссылка на доку] использует внутренние поля с указанием прямого адреса памяти, где размещён буфер и размера буфера. После создания

подобного буфера существует возможность подмены внутренних полей объекта на значения, соответствующие реальному кольцевому буферу. Подобный вариант является опасным, требует аккуратного обращения, в частности – сохранения и восстановления параметров исходного буфера после окончания работы с кольцевым буфером. Таким образом, приведённая выше схема работы трансформируется в следующий вариант:

– открытие сокета и подготовка режима кольцевого буфера,
– создание временного Java буфера и сохранение его параметров,
– подмена параметров для указания на кольцевой буфер,
– циклическая обработка пакетов блоками,
– восстановление параметров временного буфера,
– закрытие исходного кольцевого буфера и сокета.

Детальное рассмотрение механизмов замены внутренних полей объекта выходит за рамки данной статьи. Необходимо отметить, что данное действие зависит от используемой версии платформы Java и может изменяться в будущем, вплоть до невозможности подобной реализации.

Проводя анализ производительности подобного варианта приёма сетевых пакетов можно отметить кардинальное снижение накладных расходов (рис. 4). В данном тестовом сценарии также был использован входящий поток в 500 Kpps, в течение первого промежутка времени приём производился с использованием группового приёма (аналогично варианту, представленному на рис. 1), в ходе второго промежутка времени приём осуществлялся с использованием описанного выше подхода. Также, в процессе приёма с использованием кольцевого буфера, осуществлялся базовый разбор блоков и принимаемых пакетов с целью фильтрации и учёта пакетов, относящихся к специфичному протоколу прикладной системы.

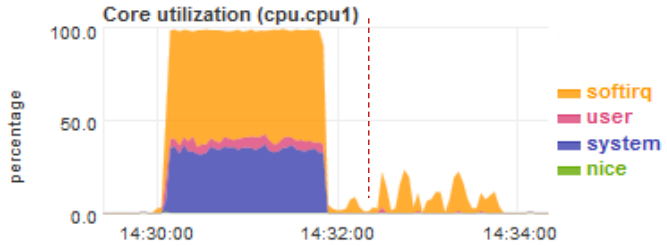


Рис. 4. Загрузка системы в групповом режиме приёма
и режиме кольцевого буфера

Таким образом, предложенный вариант оказывается работоспособным и, более того, позволяет сильно повысить производительность приёма пакетов. Тем не менее, ряд рассмотренных выше ограничений не позволяет рекомендовать его для всех случаев. Также использование данного подхода не исключает необходимость настройки сетевого стека системы для оптимизации низкоуровневых механизмов приёма и обработки пакетов системой.

Список используемых источников

1. Java Language and Virtual Machine Specifications [Электронный ресурс]. Электрон. дан. 2020. URL: https://docs.oracle.com/javase/specs/index.html, свободный. Загл. с экрана. Яз. англ.

2. Java Native Interface Specification Contents [Электронный ресурс]. Электрон. дан. 2020. URL: https://docs.oracle.com/en/java/javase/13/docs/specs/jni/index.html, свободный. Загл. с экрана. Яз. англ.

3. Recvmmsg – receive multiple messages on a socket [Электронный ресурс]. Электрон. дан. 2020. URL: http://man7.org/linux/man-pages/man2/recvmmsg.2.html, свободный. Загл. с экрана. Яз. англ.

4. OSI model [Электронный ресурс]. Электрон. дан. 2020. URL: https://en.wikipedia.org/wiki/OSI_model, свободный. Загл. с экрана. Яз. англ.

5. Packet – packet interface on device level [Электронный ресурс]. Электрон. дан. 2020. URL: http://man7.org/linux/man-pages/man7/packet.7.html, свободный. Загл. с экрана. Яз. англ.

6. This file documents the mmap() facility available with the PACKET socket interface [Электронный ресурс]. Электрон. дан. 2020. URL: https://www.kernel.org/doc/Documentation/networking/packet_mmap.txt, свободный. Загл. с экрана. Яз. англ.

7. Class ByteBuffer [Электронный ресурс]. Электрон. дан. 2020. URL: https://docs.oracle.com/en/java/javase/13/docs/api/java.base/java/nio/ByteBuffer.html, свободный. Загл. с экрана. Яз. англ.

Статья представлена проректором по информатизации СПбГУТ, кандидатом технических наук, доцентом А. А. Зарубиным.

УДК 004.41.42
ГРНТИ 81.96

АУТЕНТИФИКАЦИЯ КЛЮЧЕЙ, РАСПРЕДЕЛЯЕМЫХ НА ОСНОВЕ EVSkey-СХЕМЫ И ИСПОЛЬЗОВАНИЯ ФИЗИЧЕСКИ НЕКЛОНИРУЕМЫХ ФУНКЦИЙ

И. О. Хворова, В. А. Яковлев

Санкт-Петербургский государственный университет телекоммуникаций им. проф. М. А. Бонч-Бруевича

Рассматривается система формирования ключа между двумя корреспондентами по открытым каналам связи, в основе которой лежит модифицированная EVSkey-схема.

Нарушитель имеет возможность контролировать каналы связи между корреспондентами и каналы между корреспондентами и доверенным центром и проводить активные атаки в них, в том числе атаку человек посередине. Предложен протокол аутентификации ключа, формируемого корреспондентами, на основе осуществления

обмена сигналами запрос-ответ между доверенным центром и корреспондентами с использованием физически неклонируемых функций, имеющихся у каждого корреспондента.

формирование ключей, аутентификация ключей, физически неклонируемые функции, хеш-функции

Предположим, что два корреспондента А и В сформировали общий ключ K_s по алгоритму Диффи-Хеллмана (ДХ) [1] или какому-либо другому протоколу формирования ключей на физическом уровне, в частности, по протоколу EVS-key+ [2]. Корреспонденты хотят быть уверенными, что в процессе формирования ключа нарушитель не проводил атак: человек посередине, повторения, отражения или, если такие атаки были, то эти атаки должны быть обнаружены.

В данной работе предлагается, разработанный авторами, способ аутентификация ключей с использованием доверенного центра, физически неклонируемых функций при ограниченной вычислительной мощности корреспондентов.

Рассмотрим следующую схему взаимодействия корреспондентов А и В при наличии доверенного центра Т в присутствии активного нарушителя Е. Нарушитель имеет возможность контролировать как каналы связи между корреспондентами, так и каналы между корреспондентами и доверенным центром и проводить активные атаки в них, в том числе атаку человек посередине (рис.).

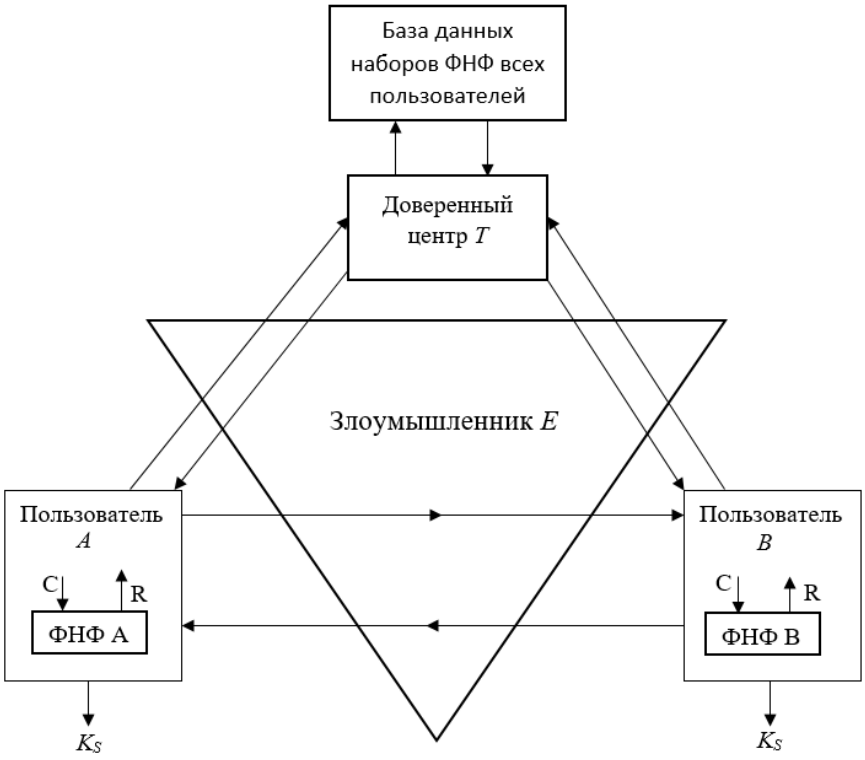


Рис. Аутентификация ключей с использованием доверенного центра и ФНФ

Корреспонденты имеют двухстороннюю связь с доверенным центром *T*, где они прошли аутентификацию с использованием протоколов, на основе использования сертификатов (протокол SSL/TLS или IPsec), или протоколов с использованием ФНФ, например, протокола PEAR [3].

Предположим, что корреспонденты A и B сформировали сеансовый ключ F_i по протоколу DH или EVS-key и хотят быть уверенными, что нарушитель E не проводил атаку человек посередине или же они должны эту атаку обнаружить.

Будем полагать, что корреспонденты имеют в составе своих компьютеров блоки, реализующие физически неклонируемую функцию (ФНФ).

По определению [4] ФНФ – это физическая система (устройство), неотъемлемым свойством которой является неклонируемость (неповторяемость) некоторых её параметров, характеристик, свойств и функций. ФНФ приобретает эти свойства на этапе производства системы и использует случайности, присущие элементам из которых строится устройство. ФНФ описывается значениями пар входных и соответствующих им выходных параметров $\overline{R} = f\left(\overline{C}\right)$. Входной сигнал $\overline{C} = C_1, C_1, \ldots, C_k$ называется запросом, выходной сигнал $\overline{R} = R_1, R_1, \ldots, R_k$ называется ответом (откликом).

ФНФ обладает тем свойством, что для одного и того же запроса $\overline{C}$ отклики разных устройств (функций) будут различны. То есть ФНФ для каждого устройства уникальна, а разные запросы для одной и той же ФНФ будут давать различные отклики. Причем повторение одного и того же запроса для одной ФНФ дает одинаковые отклики [5].

Предположим доверенный центр имеет достаточно большое подмножество F_i случайно отобранных пар $\left[\overline{C}_{ij}, \overline{R}_{ij}\right]$, где индекс *i* – номер ФНФ, *j* – номер запроса-отклика ФНФ для устройства каждого корреспондента. Обозначим количество таких пар для одного устройства $\left|F_i\right|$. Мы предполагаем, что выполняется условие $\left|F_i\right| \ll 2^{\boldsymbol{k}}$. Смысл этого ограничения состоит в том, что если нарушитель будет «зондировать» устройство, посылая на него случайные запросы, то вероятность выбрать запрос из подмножества F_i, будет ничтожно малой.

Протокол аутентификации ключа включает следующие шаги:

1. Доверенный центр посылает корреспондентам A и B запрос *C*.

2. Корреспондент A вычисляет значение своей ФНФ $\overline{R}_A = f\left(\overline{C}_A\right)$.

Корр. B вычисляет аналогично значение своей ФНФ $\overline{R}_{\boldsymbol{B}} = f\left(\overline{C}_{\boldsymbol{B}}\right)$.

Представим отклик $\bar{R}_A$ в виде конкатенации из трех частей $\bar{R}_A = R_{A1} \| R_{A2} \| R_{A3}$, где $R_{Ai} \in GF(N)$, аналогично отклик $\bar{R}_{\boldsymbol{B}}$ представим в виде $\bar{R}_B = R_{B1} \| R_{B2} \| R_{B3}$, где $R_{Bi} \in GF(N)$.

3. Корреспондент А формирует ответ доверенному центру в виде

$$S_A = \left[R_{A1} \oplus h(K_s) \right] \times R_{A2} \, mod N,$$

где $h(K_s)$ – хеш-функция от сформированного корреспондентами ключа, $h(K_s) \in GF(N)$ и отправляет его Т.

Корреспондент В формирует ответ доверенному центру в виде

$$S_{\boldsymbol{B}} = \left[R_{B1} \oplus h(K_s) \right] \times R_{B2} mod N,$$

и отправляет его Т.

4. Получив S_A и $S_{\boldsymbol{B}}$, доверенный центр выполняет преобразования:

$$S_A \cdot R_{A2}^{-1} mod N = R_{A1} \oplus h(K_s), \; S_{\boldsymbol{B}} \cdot R_{B2}^{-1} mod N = R_{B1} \oplus h(K_s),$$

а затем

$$R_{A1} \oplus h(K_s) \oplus R_{B1} \oplus h(K_s) = R_{A1} \oplus R_{B1} = R_1.$$

Полученное значение сравнивает с $R_1' = R_{A1}' \oplus R_{B1}'$, где R_{A1}' и R_{B1}' эталонные отклики ФНФ устройств А и В, которые хранятся в базе данных доверенного центра Т. Если $R_1' = R_1$, то центр убеждается, что ключи у А и В совпадают, то есть атаки человек посередине не было.

5. Центр оповещает корреспондентов А и В о том, что ключи совпадают, то есть аутентификация пройдена. Для этого он посылает корреспондентам А и В сообщения R_{A3}' и R_{B3}' соответственно.

6. Корр. А, приняв R_{A3}', проверяет равенство $R_{A3}' = R_{A3}$, корр. В, приняв $R_{\boldsymbol{B}3}'$, проверяет равенство $R_{\boldsymbol{B}3}' = R_{\boldsymbol{B}3}$. Если эти равенства выполняются, то корреспонденты уверены в том, что они сформировали одинаковые ключи, т. е. ключ аутентифицирован. При невыполнении равенства $R_1' = R_1$, центр оповещает корреспондентов инверсными значениями R_{A3}' и R_{B3}'.

Заметим, что в данном протоколе нет сложных вычислений. У корреспондентов наиболее сложная операция – умножение в конечном поле на маскирующий множитель. В центре наиболее сложная операция обращение элемента по модулю, но она может быть выполнена заранее, после отправки запроса корреспондентам.

ФНФ $f_A(\bar{C})$ и $f_B(\bar{C})$ выполняются автоматически встроенными устройствами, функция хеширования ключа $h(K_s)$ может быть вычислена по стандартному алгоритму: MD-5, SHA-2, ГОСТ Р34.11-2012.

Основное отличие данного протокола от известного протокола аутентифицированного распределения ключей Нидхема–Шредера, состоит в том, что доверенный центр используется только для аутентификации ключей, но не участвует в их формировании и, следовательно, не имеет к ним доступа.

Рассмотрим 2-й вариант аутентификации с использованием ФНФ, который не требует выполнения операции умножения больших чисел у пользователей и операции нахождения обратного элемента по модулю в доверенном центре.

1. Доверенный центр посылает корреспондентам А и В запрос *C*.

2. Корр. А вычисляет значение своей ФНФ $\bar{R}_A = f(\bar{C}_A)$, корр. В вычисляет аналогично значение своей ФНФ $\bar{R}_B = f(\bar{C}_B)$. Представим отклики $\bar{R}_A$ и $\bar{R}_B$ виде конкатенации двух частей $\bar{R}_A = R_{a1} \| R_{a2}$, $\bar{R}_B = R_{B1} \| R_{B2}$ соответственно.

3. Корреспонденты А и В формируют ответы:

$$S_A = h(K_s), h(R_{A1} \| h(K_s)),\ S_B = h(K_s), h(R_{B1} \| h(K_s)),$$

где $h(.)$ – хеш-функция.

4. Получив S_A, доверенный центр выделяет значение хэш-функции $h(K_s)$ и вычисляет $h(R'_{A1} \| h(K_s))$. Далее он сравнивает $h(R'_{A1} \| h(K_s))$ с $h(R_{A1} \| h(K_s))$, полученным от А во второй части отклика.

Аналогично, используя S_B, доверенный центр находит $h(R'_{B1} \| h(K_s))$ и сравнивает его с $h(R_{B1} \| h(K_s))$, полученным от В. Если сравнения выполняются и первые части сообщений S_A и S_B совпадают, то А и В используют один и тот же ключ.

Предположим, что злоумышленник перехватил сообщения: $S_A = h(K_{AE}), h(R_{A1} \| h(K_{AE}))$, $S_B = h(K_{BE}), h(R_{B1} \| h(K_{BE}))$.

Тогда с целью обмана доверенного центра он может предпринять следующие шаги: нарушитель транслирует сообщение $S_A = h(K_{AE}), h(R_{A1} \| h(K_{AE}))$ в доверенный центр и пытается сформировать сообщение $S_B = h(K_{AE}), h(R_{B1} \| h(K_{AE}))$.

Однако для формирования второй части этого сообщения нужно преобразовать или $h\left(R_{B1} \| h\left(K_{BE}\right)\right)$, или $h\left(R_{A1} \| h\left(K_{AE}\right)\right)$ в $h\left(R_{B1} \| h\left(K_{AE}\right)\right)$.

Так как R_{A1} и R_{B1} злоумышленнику не известны, то эта задача равносильна нахождению ½ аргумента хеш-функции по заданному хеш-коду. Современные хеш-функции устойчивы к коллизионным атакам такого рода.

Таким образом, проведенный анализ показал, что предлагаемый протокол аутентификации устойчив к атаке человек посередине. Защита от атаки повторения обеспечивается тем, что при каждом новом установлении сеанса связи доверенный центр посылает новый запрос, на основе которого корреспонденты вычисляют значения своих ФНФ, используемых для формирования уникальных ответов. При этом, полученное в результате преобразования ответа значение сравнивается с эталонным откликом ФНФ, хранящимся только в базе данных доверенного центра.

Список используемых источников

1. Diffe M., Hellman M. New directions in cryptography: IEEE Trans. Inf. Theory, 1976. vol. 22, no. 6, pp. 644–654.

2. Korshik V., Yakovlev V., Starostin V., Rabarov M., Gerasimovich A., Zhuvikin A., Morales-Luna G. Information theoretical secure key sharing protocol for noiseless public constant parameter channels without cryptographic assumptions // Proceeding of Federatad Conference on Computer Science and Information Systems, 2019 (Leipzig), pp. 361–366.

3. Kerr S., Kirkpatrick M S., Bertine E. PEAR: A hardware Based Protocol Authentication System// In proceedings of the 3rd ACM SIGSPATAIL International Workshop on Security and Privacy in GIS and LBS. 2010. N 10. PP. 18–25.

4. Ярмолик В. Н., Вашинко Ю. Г. Физически неклонируемые функции// Информатика. 2011. № 2. С. 92–104.

5. Maes R. Physically Unclonable Functions: Constructions, Properties and Applications: Katholieke Universiteit Leuven, 2012. 234 pp.

УДК 608.4
ГРНТИ 81.93.29

ОБЕСПЕЧЕНИЕ ТЕХНИЧЕСКОЙ ЗАЩИТЫ ИНФОРМАЦИИ В ВОЛОКОННО-ОПТИЧЕСКИХ СИСТЕМАХ ПЕРЕДАЧИ

Е. В. Шустова

ООО «Техцентр»

Разработка системы мониторинга оптоволоконных линий связи и обеспечение технической защиты информации, циркулирующей в телекоммуникационных системах

и автоматизированных системах управления технологическими процессами различного назначения, с передачей данных ограниченного распространения по волоконно-оптическим линиям связи, выходящими за пределы контролируемых зон.

оптоволоконные системы передачи данных, рефлектометрический метод, система мониторинга.

В настоящее время тема защищенной передачи большого объема данных на дальние расстояния максимально актуальна. Всеобщая глобализация и информатизация проникла во все сферы человеческой жизни. Мы записываемся к врачу, платим налоги и оформляем документы через глобальную сеть Интернет. Количество сфер жизни людей, которые переходят в информационную плоскость увеличиваются с каждым годом. По сети передают уже не только информацию развлекательного характера, но и с принятием необходимых мер информацию конфиденциального характера, составляющую коммерческую, служебную, государственную тайны и персональные данные. Органы власти, государственные корпорации и крупные коммерческие организации могут себе позволить объединить информационные сети структурных подразделений, расположенных за тысячи километры друг друга используя как открытую информационную среду Интернет, так и сети электросвязи общего пользования, выделенные и ведомственные сети связи. Объемы передаваемой информации растут в геометрической прогрессии. Потребности к увеличению доступности и скорости передачи данных в сетях связи ведут к увеличению использования в них ВОЛС (волоконно-оптических линий связи). За счет высокой несущей частоты осуществляется большая скорость передачи информации по одному волокну. Затухание сигнала в оптоволокне достаточно мало, что позволяет строить без ретрансляции линии, протяженность которых может составить более 100 км. Волоконно-оптический кабель прекрасно защищен. Он не имеет побочного радиоизлучения, поэтому передаваемую информацию по нему довольно сложно перехватить, не нарушив при этом целостность волокна. Чтобы исключить такие попытки перехвата информации необходима система мониторинга, которая автоматически обнаружит, мгновенно подаст сигнал тревоги и отключит передачу данных по скомроментированному каналу до восстановления линии [1, 2, 3, 4].

Основные проблемы передачи по волоконно-оптическим линиям связи информации, содержащей сведения, доступ к которым ограничен федеральными законами:

– необходимость обеспечения целостности, доступности и конфиденциальности информации, содержащей сведения ограниченного доступа, персональных данных, служебной и технологической информации систем управления производством или технологическими процессами при передаче данных за пределы контролируемой зоны;

– обвальное снижение потенциала (скорости) передачи информации по волоконно-оптическим линиям связи (далее ВОЛС) в десятки раз при использование криптографической защиты;

– большая стоимость оборудования для шифрования высокоскоростного трафика;

– сложная и дорогостоящая настройка и обслуживание средств шифрования, требующего наличия высококвалифицированного технического персонала.

Экономически обоснованным решением проблем является непрерывный мониторинг состояния оптических волокон линии связи и блокировка передачи данных по ним, в случае выявления угроз безопасности информации в виде ее утечки, вследствие несанкционированного доступа злоумышленника к оптическим волокнам.

ПАК «СИМВОЛ» – программно-аппаратный комплекс мониторинга оптических линий связи и блокирования передачи данных

ПАК «СИМВОЛ» позволяет выявлять все возможные деструктивные действия на волоконно-оптической линии связи (далее ВОЛС), проявляющиеся в виде изменения коэффициентов отражения, локального и общего затухания, длины волокна (далее Авария).

Комплект поставки ПАК «СИМВОЛ»

Модуль мониторинга, включающий:

– рефлектометрический модуль;

– оптический коммутатор;

– оптические ключи;

– сервер управления, включающий:

– операционную систему специального назначения Astra Linux Special Edition «Смоленск»;

– программный модуль обработки рефлектограмм;

– защищенный Web-сервер;

– базу данных PostgresSQL.

ПАК «СИМВОЛ» позволяет:

1. Защитить от несанкционированного доступа высокоскоростные волоконно-оптические линии передач информации (далее ВОЛП).

2. Упростить и тем самым уменьшить стоимость технического обслуживания волоконно-оптической сети.

3. Уменьшить время простоя волоконно-оптической сети.

Принцип работы ПАК «СИМВОЛ»

ПАК «СИМВОЛ» в автоматическом режиме проводит мониторинг контролируемой ВОЛС, сравнивая полученные рефлектограммы с эталонной. При достижении величины любого из контролируемых параметров выше допустимого значения система регистрирует событие и принимает решение о дальнейшем отключении передачи информации по скомпрометированной ВОЛС.

Передача данных идет через ПАК «СИМВОЛ» и не требует дополнительного коммутационного оборудования для построения защищенных волоконно-оптический систем передачи данных (далее ВОСП).

Отключение передачи информации по волоконно-оптической линии связи осуществляется автоматически на физическом уровне посредством оптических ключей.

Конкурентные преимущества ПАК «СИМВОЛ»

1. Снижение стоимости системы защиты конфиденциальной информации в ВОСП.

2. Снижение времени обслуживания ВОЛС.

3. Снижение трудоемкости обслуживания ВОЛС.

4. Работа с любой приемопередающей аппаратурой.

5. Использование всего скоростного потенциала приемопередающего оборудования ВОСП.

6. Доступность системы:

– наличие отечественного сертифицированного метрологического оборудования;

– полностью отечественная разработка.

Основные возможности ПАК «СИМВОЛ»:

1. Непрерывный мониторинг физического состояния ВОЛС (выявление старения оптического волокна и деградации соединительных муфт).

2. Контроль локального и общего затухания ВОЛС, выявление аварии на линиях (обрыв волокна, удлинение волокна, изменение отражений).

3. Гибкая настройка параметров событий.

4. Одновременный мониторинг 8 оптических волокон одним измерительным комплексом.

5. Масштабируемая система мониторинга (возможность объединения до 12 измерительных комплексов на сервере управления).

6. Автоматическое отключение передачи данных по каналу связи при Аварии.

7. Автоматическое определение расстояния до события.

8. Мониторинг состояния аварийного волокна, после отключения информативного оптического сигнала.

9. Отображение маршрута прокладки оптоволоконной линии на плане местности.

10. Возможность загрузки своих карт, планов и схем местности.

11. Разграничение прав пользователей ПАК «СИМВОЛ».

12. Ведение журнала действий пользователей системы и событий на линии.

13. Инструментальные панели отображающие контролируемые параметры волокна, места Аварии на линии и географической карте, историю событий ВОЛС.

14. Соответствие требованиям РД ФСТЭК России (планируется получение сертификата ФСТЭК на соответствия МД о ТЗИ ВОС-К, ТУ и НДВ к 4-ому кварталу 2020 г.).

15. Автоматический режим работы 24/7.

16. Дополнительное сигнализирование об Авариях оператора посредством отправки snmp сообщений, email.

17. Световая сигнализация.

18. Отображение схемы контролируемых волокон и их состояния.

19. Хранение «Аварийных» рефлектограмм, возможность просмотра архивных событий для анализа.

Предлагается:

– высококачественное оборудование полностью российской разработки;

– пусконаладочные работы по внедрению/переходу с другого оборудования;

– проведение сертифицированного обучения для специалистов и выдача сертификатов;

– техническую поддержку;

– возможность доработки под требования заказчика.

Список используемых источников

1. Листвин А. В., Листвин В. Н. Рефлектометрия оптических волокон. М. : ЛЕСАРарт, 2005.

2. Сборник методических документов по технической защите информации ограниченного доступа, не содержащей сведений, составляющих государственную тайну, в волоконно-оптических системах передачи (МД по ТЗИ ВОСП-К), Москва, 2005 г.

3. Гауэр Дж. Оптические системы связи: пер. с англ. : . М. : Радио и связь, 1989.

4. Основы волоконно-оптической связи: пер. с англ. / Под ред. Е. М. Дианова. – М. : Сов. радио, 1980.

Статья представлена деканом факультета ИСиТ СПбГУТ, доктором технических наук, профессором И. А. Зикратовым.

ANNOTATIONS

PLENARY MEETING

Gerasimovich A., Kabardov M., Korzhik V., Starostin V., Yakovlev V. Secure Key Sharing Protocol Executing over Constant Parameter Channels under the Conditions of Noiseless Eavesdropping and Perspective of a Future Quantum Computer Implementation. – PP. 5–15.
It is proposed a cryptographic key sharing protocol over constant (like Internet) channels under the conditions of ideal passive eavesdropping In contrast of well known protocol executing public key cryptosystem (Diffie-Hellman cte.) the proposed protocol has nothing cryptographic assumptions and hence it cannot be compromise by the use of quantum computers in the future.
Key words: key sharing, constant channels, artificial noise, matrix eigenvalues, quantum computers.

INFORMATION AND COMMUNICATION NETWORKS AND SYSTEMS

Хамза Д. Д., Ковцур М. М. Виртуализация серверов (VMWARE VSPHERE). – С. 16–19.
Рост компаний по всему миру за последние 10 лет просто невероятный. Это увеличило размеры и потребности компаний. В 2018 году оборот мирового рынка серверов вырос на 43,7 % в годовом исчислении и во втором квартале достиг $ 22,5 млрд. Мировые продажи серверов выросли на 20,5 % в годовом исчислении до 2,9 млн единиц. Мировой рынок серверов продолжает испытывать исторический спрос, и 2КВ18 ознаменовал четвертый квартал подряд двузначным ростом продаж и самым высоким показателем за всю историю. Объем выручки серверов увеличился на 42,7 % до $18,4 млрд, в то время как выручка серверов среднего уровня увеличилась на 63,0 % до 2,5 млрд долларов. Высокотехнологичные системы выросли на 30,4 % и оцениваются в 1,7 миллиарда долларов. В 2019 году общая мировая выручка серверов выросла на 7,5 процента в годовом исчислении до 25,4 миллиарда долларов в четвертом квартале, в то время как поставки серверов выросли на 14 процентов до чуть более 3,4 миллиона единиц. Объем выручки серверов вырос на 12 % в годовом исчислении до $ 19,7 млрд наряду с ростом на 9 % в системах высокого класса до $ 2,4 млрд. С этим расширением компаний физическое оборудование становится более дорогим, более потребляющим, более трудным в управлении и более занимающим пространство. Виртуализация серверов поможет решить эти проблемы.

Ключевые слова: виртуализация серверов, VMware, сервера ESXi, vCenter, и технологии виртуальных машин, повысить отдачу, графический интерфейс, ресурсов, оперативной памяти, ДРС, физическая архитектура, процессор, ЦОД, ха, копированию, футов.

Abilov A., Vasiliev D., Kaisina I. Data Streaming in UAV Networks for Single-source Scenarios: a General Overview of Research Results. – PP. 19–24.
This article offers a general brief review of previous research related to data transmission in Flying Ad Hoc Networks. Where the following scenarios were considered: source-node – destination-node; source-node – relay-node– destination-node; source-node – swarm of relay-nodes–destination-node. In these scenarios, methods and algorithms for improving the Quality of Service (QoS) metric through the Packet Delivery Rate were reviewed. Recommendations on the use of the results were given.
Key words: UAV, FANET, streaming data, QoS, relay, PDR.

Abramov S., Abramova E., Myshkin V., Pavlov I., Pavlova M. Overview of Wave Types for Wireless Underwater Communications. – PP. 24–28.
The article discusses various types of information exchange systems with objects located in the water column. These communication systems differ in the wavelengths used: acoustic, radio waves, and optical radiation. The results of experiments with underwater bistatic optoelectronic communication systems, in which scattered laser radiation is used as a data carrier, are considered.
Key words: underwater optical communication, optical waves, wireless communication, types of waves.

Abramov S., Abramova E., Pavlov I., Pavlova M. General Concepts of Adaptive Radio Communication System. – PP. 29–33.
Protection of communication systems for various purposes from radio interference is one of the most important tasks that arise both in the development and practical use of radio devices. The problem of a priori uncertainty of the interference situation in radio communication channels is currently being solved in several directions. One of the directions can be called adaptive, it consists in adjusting the structure and parameters of the system when the conditions of its functioning change.
Key words: adaptation, radio communication, noise immunity, signal, adaptive system.

Avdeeva M., Ushakov I., Filippov A. Comparative Analysis of the OpenStack Cloud Concept and Traditional Virtualization Architecture. – PP. 33–38.
Cloud computing is gaining popularity in the modern world. Users no longer need to ask questions: how to process data? Where to process them? When? This article will compare solutions based on the traditional virtualization architecture, as well as open source infrastructure – OpenStack. Cloud computing is a technology that provides comfortable network access upon request to some common set of information computing resources.
Key words: cloud computing, cloud technologies, cloud computing, OpenStack, VMware vSphere, IaaS, virtualization technologies.

Ageev S., Levshun D., Saenko I. Architecture of the Verification System for Information Access Control Policies in Cloud Infrastructures. – PP. 38–43.
The architecture of the verification system for information access control policies in cloud infrastructures focused on the ABAC access control model and UPPAAL verification tool is discussed. The composition of modules in the proposed architecture is defined. Results of architecture implementation in a specific subject area have been carried out.
Keywords: verification, policy, access control, cloud infrastructure.

Ageeva A., Biryukova N., Elagin V. 6G Network with Artificial Intelligence Support. – PP. 43–48.
The 5G network is gradually launching around the world, which will provide a new core technology that supports future industry and society, along with Artificial Intelligence (AI) and the Internet of Things (IoT). But it is assumed that due to the exponential growth of data transfer, in a few years the speed and capabilities of 5G will be missed.
6G mobile technology can be a breakthrough technology that can deliver speeds up to 400 times faster than 5G. Artificial Intelligence will play a critical role in the development and optimization of 6G architecture, protocols, and operations. AI will be able to provide ways to implement the search for knowledge, intelligent resource management, automatic network configuration and intelligent provision of services.
In this report, we will examine the relationship between the 6G network and Artificial Intelligence technology, as well as the use of artificial intelligence methods to efficiently and effectively optimize network performance.
Key words: 6G, 5G, Artificial Intelligence, AI, Internet of Things, IoT.

Alzaghir A., Muthanna A. Unmanned Aerial Vehicles use Cases in 5G Networks. – PP. 49–53.
The technology of 5G applied to the issues of vehicle to everything communication (V2X), utility applications and industrial automation, primary broadband access services, virtual and augmented reality services, as well as wireless healthcare services. Furthermore, the performance criteria for low latency, enhanced reliability, high speed, peak throughput per connection, system spectral efficiency, low power consumption, connection and capacity density will be introduced by 5G. The Unmanned Aerial Vehicle is capable of solving challenges. In this study, some of UAV use cases are presented in 5G networks.
Key words: UNMANNED Aerial Vehicle, UAVs, Drones, 5G.

Alshaev V., Tsvetkov A. Development of a Module for Differentiating Network Traffic to Increase the Level of Protection in the Virtualization Platform VmWare vSphere – PP. 53–57.
This article addressed the issue of improving information security in a virtual infrastructure. In view of the rapid development of virtualization, this issue is very relevant. Most large IT companies smoothly move into the virtual sphere and, accordingly, they need high-quality protection of their information. There are several methods to enhance security in VMware vSphere. These technologies will enable companies to solve many problems associated with the theft or loss of confidential data. Advanced technologies are able to provide information protection for any company, as they can use a very flexible algorithm that represents a unique solution.
Key words: virtualization, security, VMware vSphere, security domain, virtual machines, privacy label, levels.

Andreev D., Andreeva E., Sergeev A., Sumkin V. Influence of Optical Cable Bending in Fiber Optic Systems Video Surveillance and Subscriber Access with Spectral Multiplexing: Experimental Test. – PP. 57–61.
The technique of measuring the spectral dependence of losses in an optical cable caused by its bending has been experimentally tested. A comparison is made of the use of sources with single-frequency lasers and Fabry-Perot lasers for these purposes. Qualitative assessment can be done using testers with additional sources operating at auxiliary wavelengths.
Key words: fiber optic networks, fiber optic fiber, optical losses, bending losses.

Andreev V., Bourdine A., Burdin V. To the Question of the Application of Fiber Optics for onboard cable networks. – PP. 62–65.
In this work, we propose a solution for fiber-optic onboard cable networks, including a method for installation of optical cables on board, a specialized multimode optical fiber with an increased core diameter and optimized profile, and the modular network transport equipment for data transmission.
Key words: optical fiber, optical cable, onboard cable networks, blown cable installation method, cable duct, data transmission equipment.

Andreev V., Burdin V., Nizhgorodov O. To the Question of the Application of Fiber Optics for onboard cable network Model for forecast of an installed optical cable lifetime. – PP. 65–68.
In the presented work, a model for predicting the lifetime of an installed optical cable is proposed. The model takes into account the "life history" of the optical fiber in the cable and the random nature of mechanical influences on the optical fiber during cable manufacture, installation and technical operation of the cable line.
Key words: optical fiber, optical cable, reliability, lifetime.

Andreeva E., Valyukhov V., Kopalin K., Kuptsov V., Sumkin V. Influence of Optical Cable Bending in Fiber Optic Systems Video Surveillance and Subscriber Access with Spectral Multiplexing: a Technique. – PP. 68–72.
To identify the bending of an optical cable, a technique for measuring the spectral dependence of losses can be used. A comparison is made of the use of sources with single-frequency lasers and Fabry-Perot lasers for these purposes. It is shown that for a more accurate measurement of the spectral dependence of losses at the macrobends of an optical cable, a technique using single-frequency lasers provides.
Key words: fiber optic networks, fiber optic fiber, optical losses, bending losses.

Andreeva E., Valyukhov V., Kuptsov V., Spiridonov S. Fiber-Optic Acoustic Sensor for Security Monitoring System. – PP. 73–75.
Fiber optic sensors are widely used in the maintenance of a branched fiber optic network. The developed acoustic fiber-optic sensor with high sensitivity in adjusted spectral range was tested. The potential convenience of such sensor is the ability to integrate into hybrid data acquisition system, including with spectral multiplexing.
Key words: security systems, video systems, optical sensors.

Andrianov V., Bakhtin D., Shterenberg S. DLP System for Protecting Corporate or Personal Data. – PP. 75–80.

Loss of information is one of the main problems of our time. Currently, more and more dangerous damages than attackers outside it.

The term DLP (Data Loss Prevention) is a software product designed to prevent confidential information from leaking out of the corporate network. The principle of operation of a DLP system consists of the analysis of all data: incoming, outgoing and visible data within the company. The system requires the use of certain algorithms, and also requires the transfer of data and / or the presentation of this responsible employee.

Key words: DLP, DLP-systems, data leak prevention, information protection tools, information. security.

Andrianov V., Stasyuk V., Shterenberg S. Analysis of Existing Pen Test Laboratories. – PP. 80–84.

Now, there is no pentest laboratory as such based on the SCS department, which could be used for continuous training and development of skills among employees and students. Students themselves deploy tools and vulnerable systems for testing, which takes a lot of time to install, configure and start operating a temporary laboratory. The training course at the Department of ZSS is aimed at studying the vulnerabilities of personal computers running Windows 7 and Windows XP operating systems, vulnerabilities of wireless networks with WPA protection and below, and vulnerabilities of web pages. The testing tool was a complex of Raspberry Pi 3 or a stationary personal computer and the Kali Linux operating system with standard tools.

Key words: Pentest, Kali-linux, Penetration test, Pentest, information. security.

Anisimov A., Kukunin D. Application of Hybrid Positioning Systems in the Industrial Internet of Things Concept. – PP. 85–88.

Internal positioning systems – technology aimed at tracking the objects location in real time, collecting and analyzing the data obtained to improve safety and increase the efficiency of the enterprise. Article contains technologies review, methods and approaches used in indoor positioning systems. Issues of existing solutions related to industrial Internet of things were identified.

Key words: Indoor Positioning Systems, Industrial Internet of Things, Bluetooth Low Energy, Wi-Fi.

Anisimov D., Dunaytsev R. A Study of Wi-Fi Performance in the St. Petersburg Metro – PP. 89–93.

Three years ago, a public Wi-Fi network called MT_FREE was put into operation on the orange (also known as the fourth) railway line of the St. Petersburg metro. Today, all trains and metro stations in St. Petersburg are equipped with Wi-Fi access points. This paper presents results of a conducted wireless site survey including the physical location of access points, the Wi-Fi channels and frequency bands used inside the trains and on the platforms of the metro stations.

Key words: MT_FREE, Wi-Fi, wireless local area network, wireless site survey, access point.

Anufrenko A., Rusin I., Shchukin A. RS485 Data Transmission Standard. – PP. 94–98.
RS485 (Recommended Standard 485 or EIA / TIA-485) is the recommended standard for transmitting data through a two-wire half-duplex multipoint serial symmetric communication channel. Joint development of associations: Electronic Industries Alliance (EIA) and Telecommunications Industry Association (TIA). The standard describes only the physical levels of signal transmission. The standard does not describe a software exchange model and exchange protocols. RS485 was created to expand the physical capabilities of the RS232 interface for transmitting binary data.
Key words: recommended standard, development, connector types, distortion level, exchange protocol.

Aptrieva E., Elagin V., Spirkina A. Setting up a Stand for Analyzing the Network Characteristics of BLOCKCHAIN Systems. – PP. 98–103.
In In the article, the authors talk about setting up a stand for analyzing network characteristics associated with the technology of Blockchain systems. The authors describe the elements of the Blockchain network and the network structure at the experimental stand. The authors show which resources were used, which operating system they used, and on which servers the stand was deployed. The article discusses the problems associated with the transmission of Blockchain data on the network. How traffic affects the network, which network load creates, is it possible to completely load the network using Blockchain data. The authors presented the results of the experiments and conducted an analysis of the data obtained (graphs of the results of the experiment and estimates of the effectiveness of the experimental network).
Key words: Blockchain, Ehereum blockchain, DPI, Deep Packet Inspection.

Ahrameeva K., Dokshin A., Kiseleva A. Research of Approaches for Authorization of Wireless Network Users Using Various LDAP Solutions. – PP. 103–106.
This article describes in detail the mechanism for authenticating IEEE 802.1 x users when connecting to a wireless network using a RADIUS server. A detailed comparison of solutions that support the RADIUS Protocol is provided. There are also various LDAP databases for organizing authentication and authorization of wireless corporate network users, namely Windows Active Directory, FreeIPA, and OpenLDAP.
Key words: IEEE 802.11, wireless network security, RADIUS, FreeRADIUS, Windows Active Directory, FreeIPA, OpenLDAP.

Akhrameeva K., Kovtsur M., Mikhailova A. Ensuring Database Information Security Web Application. – PP. 107–110.
This article discusses the mechanisms for ensuring information security of web application databases. The result of the analysis of modern databases is presented, the most relevant databases are identified when creating a web project. The main threats aimed at databases, as well as ways and solutions for their protection, are investigated.
Key words: information security, database, web application, threats.

Batenkov K., Korolev A., Mironov A., Oreshin A. Wave-Like Nature of Heterogeneous Requests Losses on Available Channel Resource. – PP. 111–114.
The dependency graphs obtained in this work allow us to assert that the greater the difference between the required resources for servicing each request of different services, the more wavy

the dependence of the probability of losses on the change of the channel resource of the multi-service communication network link will be.
Key words: multiservice communication network, heterogeneous traffic, analytical model, Kaufman-Roberts method/

Batenkov K., Oreshin A., Fokin A. The Forming of Many Multiple Trees in Telecommunication Networks. – PP. 114–119.
Issues related to analyzing the reliability of telecommunications networks remain in the focus of attention when upgrading or designing them. The model of a telecommunications network can be represented as a generalized model of Erdesh-Renya, which is used to generate a set of multi-pole trees for networks with multi-pole connectivity.
Key words: network, graph, model, tree, connectivity probability, stability, reliability.

Bakhtin U., Bushuyev S., Gaifulina D., Zhernova K., Ivanov A., Komashinskiy V., Kotenko I. Methods of Experimental Evaluation of the Effectiveness of Human-Computer Interaction in Visual Analytics. – PP. 120.–123.
An analysis of computer security incidents currently requires processing more and more data. At the same time, the ever-increasing volume of processed information requires increasingly complex visualization models. However, with the increasing complexity of visualization, the need for developing new, more effective ways of human-computer interaction for managing data presented in graphic display increases. New models of interaction with visualization models in visual analytics systems require an assessment of effectiveness in order to recognize how suitable this visualization is for a specific task. In this paper, we propose a possible methodology for assessing interaction with visualization.
Key words: human-computer interaction, information security, user interfaces, data visualization, efficiency evaluation, touch screens.

Bezuglov M., Olimpiev A. Current State of Transport Networks of Synchronous and Plesiochronous Digital Hierarchies. – PP. 124–128.
The article considers the aspects of synchronous and plesiochronous transport networks related to the stage of commissioning of lines and telecommunications equipment. The question about the sufficiency of the maintaince signals variety for telecommunications equipment setup is raised.
Key words: synchronous digital hierarchies, plesiochronous digital hierarchies, maintaince signals.

Belov S., Makarov L. Technology and Network ZigBee. – PP. 128–130.
The relevance of the topic is that with the help of ZigBee technology in wireless communication network applications that do not have a high data transfer rate, it is possible to provide stable scaling of the multi-step wireless network, thereby contributing to the rapid change in technology for operating software systems in the consumer market. The scope has been expanded to meet the needs of both a private user and a company, for example: automate the street cleaning process; use the automated smart home management process.
Key words: ZigBee network, APS, RTLS, IEEE 802.15.4 standard, wireless sensor networks.

Berezina E., Vitkova L. IoT Threats Model in Software-Defined Networks. – PP. 130–134.
Fifth-generation mobile networks, based on 5G technologies, are being actively implemented and deployed. Growing number of mobile devices and services and its variety, as well as increasing requirements for bandwidth, obliges most countries to follow the path of the 5G rapid deployment. At the same time, the threats, faced by such communication networks, are obvious for information security specialists. There is no unified international center, which would take responsibility for developing a model of threats and violators in such networks. In this paper, authors consider possible threats and vulnerabilities for a new generation wireless network, using the example of the IoT network, and offer their own approach to systematization of threats.
Key words: Internet of Things (IoT), IoT security, IoT threats model.

Bobrova K., Kanaev A., Saharova M. Simulation Model of Multiservice Network Functioning on the Principles of the Network Functions Virtualization Concept – PP. 135–140.
The trend of modern multiservice networks (MN) evolution has shown that the MN development next stage is based on the NFV conception that should provide numeral reduction of equipment, flexibility of customization and scalability of resources.
At the same time, the planning and designing stage of MN, as a complex technical system, should include a number of complex procedures for estimate of key figures of service quality and NVF network reliability.
The simulation model has been developed by way of AnyLogic environment on the basis of discrete-event simulation methods, by taking into account the features of conformation, processing and delivery of the traffic, backend processes of NVF communications centers equipment functioning.
The result of the simulation allowed to receive the probabilistic and temporal characteristics assessment of the MN functioning processes on the basis of NFV, and the presented model is functional and sensitive to changes in the source data.
Key words: multiservice network (MN), Network Function Virtualization (NFV), Quality of Service (QoS), flexibility, scalable.

Bogdanova L., Kleverov D., Kleverov M. The Overview of Models and Algorithms for Detecting Abnormal Signalization in IoT. – PP. 141–145.
The development of telecommunications originates very fastly. One of the important stages of this process is the emergence of a new mobile communication architecture and Internet of Things. The article discusses possible threats inherited from previous generations of mobile communication, in addition to that, an overview of machine learning algorithms for detecting abnormal signaling in IoT is provided. The authors also investigate four main categories of methods for detecting anomalies in traffic, i. e. classification, statistical methods and clustering.
Key words: IoT, IoT security questions, IoT security threats, abnormal signalization, machine learning.

Boiko A., Taranov M. The Model of Interfaces Linking Device for Telecommunication Facilities of the Field and Stationary Components of Special Assignment Transport Telecommunication Network. – PP. 145–148.

Nowadays Transport Telecommunication Network of the Russian Armed Forces is presented by two components: the field and the stationary. These two components interconnect by the linking of complex telecommunication apparatus facilities and trusted operator's communication centers.

In order to provide the selection of digital channels and group paths in the receiving points the facility which provides linking between the components of transport telecommunication network interfaces and increase the efficiency is needed. There is no such a facility for the present moment in Russia.

Keywords: Telecommunication Network of The Russian Armed Forces (TNoTRAF), linking, physical interfaces, efficiency of the provision of services.

Borodina P., Vladimirov S. Determination of Data Network Quality Classes by Estimating Delay Time on UNI-UNI Interfaces – PP. 148–153.

The paper presents the results of data transmission networks segments testing in order to assess the network quality class in accordance with ITU-T recommendations Y.1540, Y.1541 and Y.1543. Testing the networks delay time for packet transmission is carried out by a software tester developed at the Department of Communication and Data Networks of St. Petersburg State University of Telecommunications. The testing operation with the recording of results is performed by the measuring server based on UNI-UNI interfaces. The testing software do not require to synchronize the clocks of the client and server sides. The main goal of the work is the practical development of network testing options and analysis of the results.

Key words: Data transmission network quality class, QoS, service indicators, SLA, packet delay time, jitter, IP packet loss.

Branitskiy A., Gladysheva P., Desnitsky V, Kotenko I. Implementation and Evaluation of Adaptation and Retraining Methods for the Analysis of Information Objects in Web-Content. – PP. 154–158.

The methods of adaptation and retraining of the system of analysis of information objects on the Internet are considered. As such methods, we consider the method of parallel training of classifiers and methods of compression of the feature space (the principal component analysis, the method of removing the features weakly correlating with the class label). These methods are aimed at reducing the time spent in the process of performing tasks related to the adaptation and retraining of classifiers within the developed system. When implementing a system for analyzing information objects in Web-content, the Python programming language and the scikit-learn machine learning library are used.

Key words: adaptation and retraining methods, Web-documents, information objects, the Internet.

Branitskiy A., Doynikova E., Kotenko I. Technique for Determination of Social Network Users Exposure to Destructiveness. – PP. 159–162.

Currently social networks are a popular environment of youth communication. At the same time, they can be used to disseminate information that has a destructive effect on users. To identify and prevent such impacts, a technique is proposed that involves the detection of signs of de-

structive effects in the information provided by users on a social network. It is based on the assumption that there is a relationship between this information and the user's exposure to destructiveness. To identify this relationship, it is proposed to use an apparatus of artificial neural networks. The experiments were conducted that confirmed the existence of a relationship between the information provided by users on social networks and the psychological characteristics of the person. In the future, it is planned to determine a set of features and conduct experiments to identify the destructive effects in dynamics.
Key words: destructive impact, social network, Ammon's test, neural network, forecasting.

Branitskiy A., Le N. Investigation of the Vulnerability Detection Method in Applications using the JBIG2 Codec. – PP. 162–166.
The JBIG2 codec is used in electronic PDF reader applications (PortableDocumentFormat). The widespread and popularity of documents in this format raises the question of ensuring the security of relevant applications is particularly acute. In the research process, a code review method is used to analyze vulnerabilities. Thus, by analyzing the graph of the control flow of the program and the presence of the relationship between the objects, it becomes possible to identify errors and exploit them.
Key words: JBIG2 codec, vulnerability detection, PDF documents, code review.

Brydchenko A., Gevel M., **Mikhailova M., Telnov N.** Li-Fi. Wireless Optical Technology Data Transfer on Bases Light-Emitting Diodes. – PP. 167–170.
Li-Fi technology is innovative and is still gaining popularity. Its potential in various fields of application needs to be developed for worldwide use. The advantages of Li-Fi are the ability to unload, the most used at the moment, Wi-Fi technology. The study of the principle of operation, technical characteristics and application methods, as well as the assessment of the global market for 2020, will help to assess the relevance of the led-based data transmission system.
Key words: Li-Fi technology, data transmission, LED lighting, wireless data transmission networks, data transmission in the visible spectrum, LEDs, LED lamp, photodetector.

Budyldina N., Yurchenko E. Calculation of Delays for the Fog Net and the Cloud in Networks IoT. – PP. 171–175.
Fog computing is becoming a promising paradigm for performing low latency distributed computing by leveraging the computing resources of end-user devices and cloud servers. However, the dynamic and distributed formation of local fog networks is a very difficult task due to the periodic appearance of neighboring fog nodes. Consequently, the fog node must correctly select a set of neighboring nodes and intelligently transfer its computational tasks in order to achieve transmission and computation with a low delay.
Key words: fog computing, border computing, delay.

Budyldina N., Guseva Yu. Positioning of Wireless Local Area Network by Wi-Fi Technology. – PP. 176–179.
The article considers the impact of the positioning method on the positioning accuracy in Wi-Fi networks. Methods of two-dimensional angular lateration and RSSI measurements applied enable to reach a meter level accuracy of the positioning. The analysis shows that a high density of access points is required.

Key words: positioning, Wi-Fi, two-dimensional angular lateration, RSSI, user equipment trajectory.

Buranova M., Rezyapkina M., Ergasheva D. Jitter Analysis in the General View Queue System. – PP. 180–184.

The total traffic of modern networks is increasing significantly, and existing network resources are limited. Network performance management allows you to choose the most optimal flow management solution. Delay and its jitter are the parameters that are most important for data transmission. The paper compares the analytical results and the results of simulation when evaluating jitter.

Key words: Jitter, delay, quality of service, modeling.

Bushuev S., Pantyukhin O., Parashchuk I., Saenko I. The Tasks of Analysis and Synthesis of Data Access Control Systems in Cloud Infrastructures of Critical Information Objects. – PP. 185–190.

The complex of tasks of analysis and synthesis of systems and mechanisms for restricting access to data in modern cloud infrastructures of critical information objects is considered. This type of information infrastructures is increasingly used in industry and other areas of activity of individuals and the state, therefore data protection in them is a key task. The proposed and described in detail the nature and content of the problems of analysis and synthesis will allow, if successfully solved, to achieve results that can positively affect the reliability and quality of access control policies, which, in turn, will increase the security of elements and content of cloud infrastructures of critical information objects and systems.

Key words: critical information object, system, access control, analysis, synthesis, cloud infrastructure, data, threat, artificial intelligence.

Bylina M. Probe Signals for Time Domain Reflectometry of Cable Communication Lines. – PP. 190–195.

The paper provides a classification of probe signals used for time domain reflectometry. The requirements for probe signals and their characteristics are considered. A comparative analysis of various probe signals is carried out. The advantages of using complementary sequences are shown.

Key words: two-wire communication line, reflectometry, time domain reflectometry, probe signal, pulse signal, voltage drop, pseudo-random sequence, complementary sequences, complementary Golay sequences.

Bylina M., Ivanov O. Experimental Research of Optical Fiber Corning TXF. – PP. 195–200.

The results of experimental studies of innovative optical fiber are presented. TXF with reduced attenuation coefficient and increased mode field area developed by Corning in accordance with ITU-T G.654.

Key words: Corning TXF, single-mode optical fiber, attenuation coefficient, mode field, stimulated Raman scattering.

Bylina M., Fomchenko A. Method for Calculating the Width Band of the Polymeric Multilayer Fiber. – PP. 201–206.

Multimode polymer optical fibers are recommended by international standards for use in local area networks. The maximum length of a network segment built on such a fiber is limited by its intermode dispersion. It is of interest to use polymer fibers with a multistage refractive index profile, which provide a higher broadband than step fibers at a relatively low cost.

Key words: multimode optical fiber, polymer optical fiber, refractive index profile, multilayer optical fiber, multistep refractive index profile, intermode dispersion, width band.

Valieva K., Vitkova L., Smirnov E. Methods for Detecting Malicious Information in the Information Space of Social Networks. – PP. 206–211.

The greatest severity of the problem of detecting malicious information is manifested in attempts to recognize target information channels, content distribution paths, and reduce the negative impact of such information on subjects (individual or collective, for example, a person, family, group, or organization). The paper presents an analysis of some existing systems for processing network content and the possibility of their application in the framework of the method of detecting malicious information. The result of this method is to increase the level of protection of users from malicious information in social networks.

Key words: malicious information; monitoring; network content; processing system; network Analytics services.

Vasyliv N., Kislyakov S. Self-Learning Neural Network Contact Center Load Forecasting Model. – PP. 211–215.

The work is devoted to the study of the neural network model for predicting the number of incoming calls to the contact center. To calculate the optimal parameters of the model we used data of the actual input loads of contact centers. The relevance of the task is determined by the understanding that the incoming load determines the number of operators involved in the work, which in turn determines the cost of operators' pay. To ensure the necessary quality of service with a minimum number of contact center operators, it is necessary to know in advance (or predict with the highest possible accuracy) the number of incoming calls. The present work is devoted to the analysis of the dependence of the quality parameter for predicting a recurrent neural network model on the volume of historical data (incoming calls). Such a seemingly simple statement of the research problem allows us to answer the question: how long does it take for the model to work to achieve the maximum quality of the prediction, and what could be the financial loss (or gain) of the contact center itself.

Key words: call center, operator, neural networks, LSTM, forecasting.

Vasyutkin A., Shvidkiy A. Performance Research of Fault-Tolerant Software-Defined Storage in Hyper-Converged Systems. – PP. 216–220.

The article presents the main properties and functions of Software-defined storage/SDS, describes performance evaluation parameters and identifies SDS bottlenecks. The architecture of SDS - Ceph implementation is considered. Performance test results of Ceph cluster as the main system of virtual machines data storage are given.

Key words: hyper-converged infrastructure, distributed storage system, software-defined storage.

Kirichek R., Kuznetsova E. Network Structure for Testing Augmented Reality Applications. – PP. 220–225.

This paper discusses augmented reality devices and applications in communication networks. Based on existung devices and applications,was developed architecture of the software and hardware complex. Using the developed architecture of the hardware-software complex, a network structure was created for testing augmented reality systems. Based on the developed network, a study was made of the properties of traffic from devices and applications of augmented reality. This network structure can be used to design systems for load testing communication networks for traffic resistance of augmented reality.

Key words: augmented reality, virtual reality, traffic analysis, AR, VR.

Vershinina X., Saltykov A. Application of Quantum Key Distribution in WDM-PON Networks. – PP. 225–230.

Ensuring the users security of passive optical networks (PON) requires the application of advanced technologies, including cryptographic methods. The research is devoted to the possibility of applying the quantum cryptography method – quantum key distribution (QKD) in PON. Quantum cryptography (QC) uses a quantum channel for secure key exchange and protects confidential information from eavesdropper and malicious users. QKD is used for sharing a random secret key by encoding information in quantum states. The article also considers the basic principles of QKD, starting from theorems of quantum mechanics (QM) and ending at the BB84 protocol. The main focus of this research is on the QKD technology integration into the wavelength division multiplexed passive optical networks (WDM PON).

Key words: Quantum Key Distribution (QKD), wavelength division multiplexed passive optical network (WDM PON), Quantum Cryptography (QC), Quantum Mechanics (QM), protocol BB84.

Vikulova A., Volostnykh V., Kononov P. Personal Data Protection in Electronic Document Management Systems. – PP. 230–235.

Currently, various electronic document management systems are used for transmitting documented information. A number of transmitted documents contain information that is personal data. The article considers the proposed procedure for creating an enterprise electronic document management system designed to transmit documents containing confidential information, including personal data. The article describes the main measures to meet the requirements of the legislation on personal data. This article may be useful for specialists of office management services and technical information security departments.

Key words: document management, electronic document management, electronic document management system, personal data protection, information security tools, cryptographic protection of document management information.

Vitkova L. Model and Algorithms for Protecting Against Malicious Information in Social Networks. – PP. 235–240.

In the early 2000s, only system administrators worked with computer networks and the Internet. However, today all people use social networks. However, new types of crimes have also appeared. Software solutions offer users various ways to protect themselves from malicious information. There is no universal model of malicious information yet. In this regard, the development of models and algorithms for protection in social networks is an important and urgent task. The author proposes a model of malicious information and its distributor that differs from

existing ones in that it contains new components: hierarchical relationships between messages with malicious information and its distributor, and also takes into account the information attribute of malicious information, characteristics of links, message types, and discrete attributes of the distributor.
Key words: malicious information, information indicative of the model, the distribution of information, information security, social network analysis.

Vitkova L., Hamidov T., Kovzur M. Development of Mechanisms for Analyzing Unwanted Information in Social Networks – PP. 240–245.
At the beginning of 2020, more than four and a half billion people use the world wide web, and the audience of social networks has passed the mark of 3.8 billion. However, as the number of users in social networks increases, so does the amount of information, and therefore the amount of unwanted content. It is becoming more and more difficult to detect and stop its spread. Every post containing the content, the dissemination of which is prohibited, analyzed and blocked separately. There is no single mechanism for identifying the source of unwanted information. Instagram Facebook, Vkontakte, and other social networks offer an approach to creating a single data model for several social networks. It is assumed that a single data model will allow you to identify the source of the spread of unwanted information in several social networks at the same time.
Key words: social network analysis, SNA, model, data, data models, information, unsolicited information, source, distribution, distribution source.

Vitkova L., Diorditsa V., Kovtsur M., Targonskaya A. Investigation of the Integration Mechanisms of the Agat CU 72XX Telecommunication Platform. – PP. 246–249.
The paper discusses the technical and functional capabilities of Agat CU 72XX, a professional telecommunications platform for providing telephone infrastructure. Mainly the capabilities of the platform are surveyed, what tasks can be solved with its help, as well as integration with third-party systems to improve performance. The analysis of the Agat CU 72XX functional existing at this stage is carried out, with consideration of its possible expansion by using additional options.
Key words: IP-telephony, LDAP, PBX, integration.

Vitkova L., Donskov E. Analysis of Keystroke Recognition Algorithms and Their Performance Indicators. – PP. 249–253.
Many tools are available to identify a person with a high level of confidence. Some of them base their algorithms on keyboard handwriting. Keyboard handwriting is a specific biometric characteristic that provides descriptions of input dynamics, speed, delays, and error rates. However, in order to properly assess the quality of keystroke algorithms, it is necessary to define certain criteria, assessing which one can make a conclusion based on efficiency criteria, as they are called. This work deals with these algorithms as well as performance indicators.
Key words: authentication, identification, password, keyboard handwriting, neural network, perceptron, far, frr.

Vitkova L., Izrailov K., Chechulin A. Classification of Vulnerability of Interfaces Transport Infrastructure of a Smart City – PP. 253–258.
The article considers the task of classifying vulnerabilities of the transport infrastructure interfaces of a smart city. For this, the approach of categorical dividing vulnerabilities is used for the following pairs: Man VS Machine, Inside VS Outward, Algorithm VS Data, Static VS Dynamic, a combination of which allows us to distinguish 16 classes. Also, a conceptual model of the transport infrastructure with interfaces and their vulnerabilities is given.
Key words: interface vulnerabilities, smart city, transport infrastructure, categorical division.

Vitkova L., Spravtseva M. Countering the Spread of Unwanted Information in the Information Space of Social Networks. – PP. 258–261.
Social networks are used for communication, people openly talk about their interests and publish different posts. Ensuring information security in social networks is one of the priorities of the country, because today such networks are also a platform for the dissemination of unwanted information. In the article authors discusses different methods, models, algorithms and services for countering the spread of unwanted information (cyberbullying).
Key words: unwanted information, cyberbullying, counteraction measures, social networks.

Vitkova L., Temchenko V., Chechulin A. Heuristic Traffic Analysis Methods. – PP. 261–266.
Detection of network attacks is currently one of the most acute problems of information security of telecommunication networks. There are various ways to prevent attacks - antivirus, firewall, host-level intrusion prevention systems, etc. However, often such "active" measures are not enough and therefore "passive" mechanisms are used - intrusion detection systems. Moreover, most of these systems work on the basis of signature approaches and methods. Practice shows that the signature approach is not enough to ensure information security of the network. The authors consider heuristic methods for detecting abnormal activity in traffic and explore the possibilities of using such approaches in intrusion detection systems.
Key words: Traffic analysis, anomaly detection methods, heuristic analysis methods, traffic anomalies.

Vladimirov S., Garifullin V. Blockchain-Based Registry Software for Data Storage. – PP. 266–271.
The paper presents a software structure for organizing a decentralized registry based on Blockchain technology. Implementation approaches and construction options for distributed data storage systems are considered. A minimally implemented Blockchain structure is specified. Algorithms for the interaction of system elements and cryptographic methods were selected to ensure safe storage and transmission of data. Implementation of a software user interface for various operating systems, including mobile operating systems, is provided. The task is considered for a general registry with the possibility of final configuration for a specific task.
Key words: blockchain, registry, cryptography, distributed systems.

Vladimirov S., Gutovskiy A., Nemanov I., Fomin A. Development of a Mobile Test Bed for Researching LoRa Technology in Promising Data Transmission Networks. – PP. 271–275.
The paper presents a mobile test bed for researching LoRa technology in promising data transmission networks. The requirements for the technical parameters of the test bed are given.

The hardware configuration of LoRa transceivers and control modules was made taking into account the research features. The user control interface for stationary and mobile computer terminals has been developed. Scenarios of the stand operation during research in the framework of research and development, as well as options for using the test bed in the educational process are presented. Outlined steps for the further development of the test bed.
Key words: test bed, LoRa, measurements in wireless network, IoV.

Vladimirov S., Koshkin S. Hardware Implementation of Galois Field Element Calculator. – PP. 275–279.
The paper presents the hardware implementation of the Galois binary field element calculator designed to support the learning process. Authors select algorithms for performing basic operations on field elements and give requirements for the technical parameters of the developed device. There is completed selection of the hardware configuration of the calculator, taking into account the tasks to be solved and given requirements. Authors propose options for the management interface and hardware user interface. The proposed implementation represents basic model and provides for further development.
Key words: Galois field, MCU, ESP8266, user interface.

Vnuchkova V., Tsvetkov A., Yurchenko M. Development of Web Applications for Accounting the Performance of Students Works in Higher Educational Institutions. – PP. 279–284.
Many educational organizations lack automation of accounting for the implementation of laboratory, practical and term papers and projects. Nowadays, the relevance of the use of electronic document management systems is increasing due to the increase in the volume of documents requiring manual processing and the need for automation following from this. The possibility of introducing a system of accounting for the performance of work is considered, the main problems of introducing this system into the educational process of the department of a higher educational institution are highlighted and possible ways of protecting information on the basis of existing regulatory documents of the Russian Federation are shown.
Key words: Digital signature, electronic document management, web, php.

Volostnykh V., Gvozdev Y., Kononov P. Generalized Model of an Educational Organizations Information System. – PP. 285–289.
The process of activity of an educational organization of higher education is a complex system that covers information processes that occur in interaction with the external environment of the organization and all internal information flows. An organization's information system is a combination of the organization's information infrastructure and information assets. The article considers approaches to the development of a generalized model of the information system of a typical educational organization of higher education of engineering and technical orientation, functioning in the conditions of threats to information security.
Key words: information system, threats to information security, educational organization.

Gabuev A., Korzhik V., Nguyen Z. Detection of Stegosystem with ±LSB Embedding Based on NIST Tests. – PP. 290–295.
There are many methods for detecting stegosystems (SG). This article evaluates the effectiveness of using the new method of stegoanalysis based on the use of NIST tests in relation to an attachment known as ± 1LSB. The principles of embedding and extracting information using the ±1LSB method are explained. The results of stegoanalysis using NIST tests are compared

with the results of stegoanalysis based on a previously known method that uses a two-dimensional Fourier transform.
Key words: stegosystem, stegoanalysis, NIST tests, ±1LSB embedding.

Gabuev A., Krasov A., Oschenkov F., Tarasov N. Security Analysis of Modern Means of Transmitting Information Using a Portable Laboratory Based on the Raspberry Pi Microcomputer. – PP. 295–298.
This article discusses a method for verifying the security of wireless media using a portable security analysis tool based on Raspberry. To analyze the security of the WPA2 authentication protocol, the Raspberry platform with Linux OS and installed software used, which allows checking the security of the Wi-Fi authentication protocol.
Key words: Wi-Fi, Linux, information security, penetration testing, WPA2, Raspberry, DoS.

Gavrilyuk V., Chechulin A. Multi-Step Attack Analysis Algorithm for Assessing Computer Network Security. – PP. 299–302.
Currently, computer networks are used in almost all areas of our lives. Therefore, hacking of such networks can lead to significant financial and reputational losses. This article describes the analysis method. Security of the local network based on modeling the actions of the intruder and possible vulnerabilities in the hardware and software elements of this network. In addition, the article describes the developed software, implementation of this method, as well as experimental results.
Key words: security assessment, attack graphs, computer network, vulnerability.

Gaifulina D. Analysis of Structurally Undefined Network Traffic Payload of Industrial Cyber-physical Systems. – PP. 302–307.
A specific feature of the transmission environment of industrial cyber-physical systems is the frequent use of protocols with unregulated specifications, which may complicate the construction of a network activity profile and monitoring security events in such networks. This paper presents the study of network traffic in the conditions of uncertain specifications of network protocols of cyber-physical systems. We propose an approach to the analysis of the payload of network traffic using lexical recognition of conditionally structured binary data based on the frequency analysis of possible sequences of information units and their combinations. We present the technique of network traffic analysis and the results of experiments confirming the applicability of the proposed approach. The test bench simulates the operation of an industrial cyber-physical system using the MODBUS/TCP protocol. The binary payload for the analysis is the Modbus protocol payload.
Key words: network traffic analysis, ad hoc protocols, industrial cyber-physical systems, cybersecurity, intrusion detection.

Gaifulina D., Kotenko I. Analysis of Deep Learning Methods for Intrusion Detection. – PP. 308–313.
At present, machine learning technologies are widely used to solve many problems of classification, prediction and decision-making in the field of information security. Increasingly, these areas are based on a class of methods called deep learning. This article presents an analysis of the deep learning methods used to detect intrusions in information and communication systems. We propose a general approach to intrusion detection using deep learning. The approach

consists in the implementation of four main processes: analysis of source data, extraction of attributes, pre-processing and classification based on deep learning. We give a comparative description of the considered deep learning methods, indicating the training parameters, network configuration, data sets used and the final quality of work according to experimental estimates.
Key words: deep learning, deep neural networks, cybersecurity, intrusion detection.

Galaktionov M., Okuneva D. Developing of a Mobile Application with the Functions of a Presenter for a Universal Presentation Format. – PP. 313–315.
This article discusses the approaches and software development process for remote presentation management. The development goal is to create software that allows you to manage a presentation without a presenter, using a mobile device (smartphone), and also use a universal PDF presentation format without electronic drives.
Key words: Software, presenter, client-server architecture, slide, Android, java, python.

Gelfand A., Kazantsev A., Krasov A., Orlov G. Assessment of Security Risks and Threats in the Smart Home Environment. – PP. 316–321.
In smart home environment, systems and devices are controlled and interact with each other automatically to provide convenience and efficiency to house residents increasing their quality of life. Nevertheless, concept of concept of a smart home environment and that fact, that it is connected with the whole world through the Internet may cause a lot of problems. The main aims of the research are: to reveal various vulnerabilities of smart house security and o show some of possible risks for house residents.
Key words: IoT, Internet of Things.

Gelfand A., Kazantsev A., Krasov A., Orlov G. Research of a Distributed Security Mechanism for Internet of Things Devices with Limited Resources. – PP. 321–326.
Due to development and extension of Internet of Things (IoT) there are more and more devices connected to the Internet, transmitting private confidential data. This article is devoted to Distributed Security Mechanism for provision of secure data transmission in IoT architecture with class 0 devices without sufficient resources for computation which is required for encryption. The aim of this research is scrutiny of the whole way of data transmission in two segments: device-controller and controller-server.
Key words: IoT, Internet of Things.

Gerling E., Gorlov S., Kirillov D. Ensuring Information Security in the Development of Web Applications. – PP. 326–331.
Web services that are provided to users cover a wide range of human needs and for this reason are so desirable for hackers. When registering for such services, people, entering their personal data, may not be aware that this information can get into attackers. Exploiting vulnerabilities, such as SQL and PHP injections, etc., allows you to gain full control over user data. Ensuring the protection of this information, as well as protecting the web applications themselves, is one of the main tasks that is posed during the development process.
Key words: SQL injections, attacks on web applications, hacking, protection of web applications.

Glukhovsky M., Sakharov D. To SS7 Information Security Questions in the Modern World. – PP. 331–335.
Signaling System No. 7 (SS7) is a nervous system of telecommunication networks based on 2G and 3G technologies. SS7 was previously isolated and protected, but now it has become more vulnerable with the industry switching to IP technology. Attackers use network communications to track subscribers, intercept calls, denial of service, and conduct fraudulent transactions. This article provides an overview of SS7 threats and vulnerabilities.
Key words: SS7, SIGTRAN, signaling protocols, telecommunication security, CN, MAP, SCTP.

Golovlyova Y., Peshkov A. The Protection of Information in the Process of Use of Copyright Objects. – PP. 336–339.
This article addresses the concepts of intellectual property and copyright, issues of protection of copyright in the modern information space, cyber threats of information security in relation to objects of intellectual property rights, as well as technical means of copyright protection and it disadvantages.
Key words: copyright, information security, protection of copyright.

Goldstein A., Terentev D. The Analyze of Application Performance using the Results of Functional Auto-Tests. – PP. 339–344.
In order to speed up the verification process and build an infrastructure for software development based on continuous integration practices, a large number of functional auto-tests are written. The article suggests using the data collected additionally during functional testing to analyze the performance of the developed application. This will help to speed up organization of performance monitoring avoiding additional costs for writing special tests. An example of using this idea in practice to solve a real engineering problem is given. It demonstrates the promise of further methods analysis for mathematical processing of performance data obtained in this way. This article will discuss the main aspects of such approach, the problems and possible solutions.
Key words: QA, performance testing, analyze of tests result.

Goldstein B., Eliseev S. About MVNO Virtual Operators at the Present Stage. – PP. 344–348.
MVNO is one of the current trends in a highly competitive telecommunications market. The share of MVNO in the Russian segment of telecommunications services is about 4 %. The customer base of virtual operators in Russia is growing at a faster pace: at the end of 2019, its increase was recorded by 40 %, while the subscriber base of the entire mobile market was less than 1 %.
Key words: MVNO, MNO, MVNE, MVNA, DCN, Private LTE.

Goldstein B., Kachalov V. Integration of AI and ML in Software Testing. – PP. 349–352.
Progress is going up every moment of life. We creating more and more software. In our time this process is unstoppable. And quality of software is important. Testing is need to make program working without any troubles on the production phase. But automatized testing has some problems. Integration of machine learning and artificial intelligence makes this process better.
Key words: quality assurance, automatized testing, machine learning, artificial intelligence.

Grebenshchikova A., Elagin V. Data Slicing and Traffic Segmentation Algorithm. – PP. 352–357.

Data traffic model in Machine to Machine Communications and data traffic slices model the are considered in this work. The main purpose is to increase the efficiency of using 5G radio resources for the M2M Communications. It is expected that 5G radio resources will be used for each slice separately in the aggregating the data path of several M2M devices. Each slice is isolated from the others and uses resources in M2M devices to increase the spectral effectiveness of the system.

Using this work and simulation methods, it can be predicted the effectiveness of data segmentation in 5G networks.

Key words: Slicing, Machine to Machine Communications, data traffic aggregation, relay node, 5G, Priority Queue, radio resources.

Grebeniuk V., Elagin V. Analysis of Big Data Frameworks for Distributed Streaming Computing. – PP. 358–363.

In July 2016, Russia adopted two draft laws amending federal legislation: No. 374 and No. 375. Regarding the topic of this work, changes in the field of regulation of user traffic storage and the rules for its provision to federal services are of interest. The bill obliges telecom operators to store calls and messages of subscribers for a period determined by the Government of the Russian Federation (but not more than 6 months) in accordance with Article 64 of the Federal Law "About Communications", and information on the facts of reception, transmission, delivery and message and call processing - 3 years. The main problem for the implementation of federal law No. 374 is the large amount of data that must be stored and processed on the operator's network. Given this, standard approaches to working with them as statically stored in spreadsheets or relational databases are of little use.

Saving traffic information and the traffic itself is a dynamic, non-stop process. Based on this, Big Data approaches can be used to work with such a continuously flowing amount of information. In this paper, we consider possible options for using Big Data frameworks for distributed streaming computing for telecom operator tasks. As a result of writing the work, various data storage and processing schemes, possible points of failure, as well as a set of capabilities provided by software systems for data processing and storage were studied.

Key words: Big data, distributed computing, data storage and processing, telecom operator, Apache Spark, Apache Flink, Apache Storm, Apache Samza.

Grigorev M., Davidova S., Krivonosova N. Content Filtering Systems. – PP. 363–368.

Separation content in condition famous and availability resources internet become most important for all categories users. Separation has specific importance in the general education organization inside "parents control", so also job in the internet is necessary and not only educational institution, but and in home conditions.

This point is important because the most of part a new information, which made in the internet has unnecessary and consist from pornographic resources, online casinos, sites about weapons, drugs, Satanism, violence and etc.

Key words: dynamic filtration, static filtration, filtration control system.

Gubaidullin R. Microwave Photonic System for Temperature Control of Accumulator Batteries of Hybrid Vehicles Based on Addressed Fiber Bragg Structures with Two Identical Ultra-narrow-Band Reflection Spectra. – PP. 368–373.
The work presents a schematic diagram of a microwave photonic system for monitoring the state of batteries of hybrid vehicles based on temperature monitoring using an array of addressed fiber Bragg structures with two identical ultra-narrow-band reflection spectra.
Key words: fiber Bragg grating, FBG, temperature sensor, addressed fiber Bragg structures, hybrid vehicle, hybrid car.

Davydova A. Features of the Use of Smart Grid Technologies for the Development of the Subsystem of Continuous Monitoring of the Metro Power Supply Network. – PP. 374–379.
The article provides the rationale for the use of Smart grid technology to develop a subsystem for continuous monitoring of the metro power supply network. The characteristic of the technology of intelligent networks to be applied is presented. The features of the multi-parameter complexes of the metro power supply network are presented. A classification of diagnostic parameters, equipment characteristics and existing systems for subsequent monitoring and calculations has been formed.
Key words: metro power supply network, Smart grid, diagnostic parameters, monitoring.

Danilova U., Egorova A., Shterenberg S. 802.11ax Wireless Network Standard. – PP. 379–383.
The 802.11ax standard is the next evolution of wireless local area network (WLAN) technology. It is reportedly 30% faster than 802.11ac, but speed is not the main advantage advertised by the Wi-Fi Alliance and other industry amenities. Standards also provide less latency, more data delivered simultaneously and increased energy efficiency.
Key words: wireless network, Wi-Fi, standard, transmission speed, access point.

Danshina A., Korzhik V., Nguyen Z. Stegosystem for Image Based on Contour and Detection it Using NIST-tests. – PP. 384–389.
This article presents one of the modern stegosystems, which embedded encrypted message by strong cipher based on contour of image. The procedure of embedding based on image contour provides higher protection from visual detection, as compared to embedding in the "smoothed" areas. The effectiveness of this stegosystem has also been evaluated based on the PSNR parameter. A detection method of this stegosystem based on using NIST-tests is proposed.
Key words: stegosystem, stegoanalysis, contour embedding, NIST-tests.

Desnitsky V., Meleshko A. Modeling Attacks on Self-Organizing Wireless Sensor Networks. – PP. 389–394.
Today wireless self-organizing sensor networks are developing and spreading in various application fields. Such networks are used to collect and aggregate data from physical sensors of devices as well as for their processing and transmission over the network in conditions of time-varying loading characteristics of communication channels, location of devices and their operating modes. Examples of such networks are distributed systems for monitoring the environmental situation of a city or industrial enterprise, transport and logistics systems,

operational management and emergency response systems. The paper presents an approach to modeling and analysis of attacks exploiting self-organization of such systems.
Key words: wireless sensor network, self-organization, security.

Desnitsky V., Parashchuk I. A Generalized Algorithm for Analyzing the Security of Wireless Sensor Networks from Attacking Influences. – PP. 394–398.
The approach to the formulation and substantive assessment of the stages of a generalized algorithm for analyzing the security of wireless sensor networks from attacking influences is considered. The algorithm includes the stages of modeling the processes of functioning of wireless sensor networks and the behavior of an intruder, capable of applying multistep attacking effects of both physical and program-information nature. The algorithm is designed to increase the reliability and speed of security analysis of networks of this class, its key stages use modern principles of processing data and information security events based on Big Data technology and neural networks.
Key words: wireless sensor network, security, impact, data, threat, analysis, modeling, intruder, resource.

Jafarova E., Ibrahimov B., Ismaylova S. Analysis Complex Indicators Multiservice Telecommunication Networks Based on Architectural Concepts FN. – PP. 399–404.
In this work, the subject research is a network multiservice infrastructure using innovative technologies of the next and future generations, supporting a wide range multimedia services and applications. The complex indicators multiservice telecommunication networks (MTS) based on the architectural concepts future networks FN (FN, Future Networks) are analyzed. Based on the study, a method for calculating the complex indicators MTS based on the architectural concept FN is proposed. Analytical expressions have been obtained to evaluate the performance indicators and the quality of the operation public communication networks, information security, the quality of service QoS (Quality of Services) heterogeneous traffic and the structural reliability of the system in providing multimedia services.
Key words: performance, SDN, multiservice telecommunications network, FN, network performance, multimedia services, NFV, Future networks, resources.

Diorditsa V., Krasov A., Targonskaya A. Research of Modern Methods of Network Steganography. – PP. 404–409.
Currently, the relevance of the use of steganography has greatly increased due to the rapid development of the information sphere. Modern steganography finds its application in various areas of the information sphere, making it possible to solve a wide range of problems: from creating digital fingerprints confirming authorship and protecting the exclusive right to an activity product, ending with covert data transmission, the use of which in a compartment using reliable cryptographic protection ensures maximum security data. In the framework of this work, various methods and algorithms for stegging into network packets (WLAN, LACK) will be considered, each of the considered methods will be evaluated based on various parameters and system stability criteria.
Key words: network steganography, data hiding, wlan, lack, hiccups, sip, mac.

Doynikova E., Dudkina O., Saenko I. Decisions Support to Increase Protection Against Information Security Incidents Using Mitre Att&ck Database. – PP. 409–414.
The task of automating the decision-making process for responding to information security incidents is complex and urgent. A problem in this area is the standardization of possible response measures and the automatic mapping of these measures to different types of incidents. This paper discusses one of the solutions in this field – the database of attacks and mitigations – Mitre Att&ck. It also examines how it can be used to support decisions to increase the security of information systems.
Key words: information security, incident, decision-making, MITRE ATT&CK.

Doynikova E., Novikova E. Forecasting Attacker Behavior using Intelligent Data Analysis. – PP. 415–418.
The early detection of security incidents and the correct prediction of their development in the analyzed system is the basis for an effective and timely response. The development of an attack depends on the attack steps, as well as his/her goals and the profile that determines the behavior of the attacker in the system. Under the profile of the attacker we understand a set of his/her characteristics, both internal, such as motives or qualifications, and external, such as financial capabilities or tools used. Determining the characteristics of the attacker will allow one to determine the type of attackers who are attracted by the analyzed system, and the complexity of the protective measures that need to be implemented. The purpose of the work is to analyze the existing methods for determining the behavior of the attacker, the profile of the attacker and its application to forecast further steps and goals of the attack. Based on the analysis, the classes of the existing approaches are defined, as well as the challenges and possible options for overcoming them existing in this area. An approach to forecasting attacker behavior based on intelligent data analysis is proposed.
Key words: security incident, attacker, forecasting, attacker profile, attributes, attack goals.

Doynikova E., Polubaryeva A. Analysis of the Problems, Their Possible Solutions and Existing Prospects of Information Security Issues of Wireless Medical Devices. – PP. 419–424.
The article dedicated to the significance of information security for wireless medical devices. The research of the vulnerabilities of medical devices was performed; standards and requirements in this industry were analyzed. The study highlighted the existing and predicted problems facing medical institutions intending to ensure information security when transmitting data over the network, and manufacturers of wireless medical devices. The solutions of the selected problems are given. The objective of the study is to show the "Internet of vulnerable things", in particular, wireless medical devices operating in cyberphysical systems during the transition to the Industry 4.0 standard, as well as the negative consequences of information security breaches in this area for an individual, society and the state as a whole.
Key words: information security, Industry 4.0, smart medicine, internet of things, wireless devices.

Dokshin A., Kiseleva A., Yurkin D. Actual Security Mechanisms of Wireless Networks. – PP. 424–429.
One of the fastest growing modern telecommunications is the wireless computing network. Moreover, for these networks, the issue of security and protection of transmitted data is very relevant. Technologies created in this area initially had a low degree of protection. The IEEE 802.11 wireless network communication group has undergone many changes since its inception

and up to now, including improvements to security mechanisms. The article conducted a study affecting the latest changes in the security section, describes the principles for building security in the Wi-Fi Protected Access 2 and 3 mechanisms. The article systematizes data on the security of wireless networks and will be useful for quickly getting acquainted with modern mechanisms.
Key words: wireless network, network security mechanisms, Wi-Fi, IEEE 802.11, WPA2, WPA3.

Dolgomer A., Muthanna A. Testing Methodology for SDN – Controller Based on 5G Network Models. – PP. 429–433.
5G / IMT-2020 communication network technologies is a relatively new and promising paradigm in the development of global network architecture. Due to the development and implementation of the IoT, the use of 5G communication network technologies completely changes the existing networking architectures and services that are available to users today. Paper provides an overview of architectures for organizing 5G network services and existing software (utilities) for testing a model network that is in the public domain. The work evaluates the functionality of the testing tools, as well as the effectiveness of their use to study different characteristics of the assembled model network and its components. The results will allow you to choose the appropriate software for model network testing and its elements when planning communication networks of different levels and with different requirements.
Key words: model network, SDN, testing, controller, 5G.

Dolgun V., Revenko Y. Development of Models of Automation of Business Processes on the Basis of Electronic Document System of Turnover SPbGUT. – PP. 433–438.
This article describes the problems and features of automating the business processes of the 1C: Document Management System using the example of SPbSUT. Automation of business processes of a document management system consists of certain stages: conducting a domain research, preparing an infrastructure, setting up an EDMS (electronic document management system), developing models, conducting acceptance tests, training employees, and conducting pilot operations. The purpose of the implementation is to increase the efficiency of activities through improved paperwork.
Key words: 1C: Document management, automation, 1C, EDMS.

Dotsenko S. Research of Processes of Distribution of Pulses of a Gaussian and Rectangular form in a Single-Mode Optical Fiber Without Attenuation Taking Into Account Linear and Nonlinear Effects. – PP. 439–444.
In single-mode optical fibers, propagation processes are affected by linear chromatic dispersion and attenuation, as well as nonlinear phase self-modulation. It is known that in lossless single-mode optical fibers with anomalous chromatic dispersion, optical pulses having the form of a hyperbolic secant (fundamental solitons) with a certain ratio of duration and peak power can propagate without distortion to infinitely large distances. The properties of solitons are explained by the complete compensation of the chromatic dispersion due to self-phase modulation. In this paper, we consider the possibilities of compensating for the chromatic dispersion due to self-phase modulation for Gaussian and rectangular pulses. Theoretical calculations were compared with the results of simulation of the propagation of pulses along single-mode optical fibers.
Key words: fiber-optic communication systems, single-mode optical fiber, chromatic dispersion, phase self-modulation, Gaussian and rectangular pulses.

Elagin V., Istomin D. Analysis of the Application of LBS Technologies in Mobile Applications. – PP. 444–450.
In the modern world, it is difficult to overestimate the importance of determining the user's location. Thanks to the rapid development of LBS (Location Based Service), new opportunities are opening up for people. Situations where you need to quickly and accurately determine the location of a person are constantly occurring. Modern people cannot imagine their life without using a Navigator, digital maps with information about buildings and companies located in them, and many other mobile programs that require a location detection function. However, applications have different requirements for geolocation recognition services. Some programs require more precise location detection, while others may sacrifice accuracy for speed and performance savings. This article analyzes LBS technologies, compares them, and applies them to mobile applications.
Key words: LBS (Location Based Servise), positioning, indoor-navigation.

Elagin V., Lobanova L. Analysis of Updated Requirements of Laws and Their Implementation in Systems of Legal Interception. – PP. 450–455.
Currently, there is a problem in SORM with the implementation of requirements in accordance with amendments to federal law No.374. This article discusses the new requirements for the development of SORM software. As well as consideration of the architecture of one embodiment of the requirements and the necessary calculations for the implementation of software.
Key words: SOSM, Spring Law, lawful interception, data storage.

Esalov K., Pomogalova A., Rodionov S. A New Paradigm for the Provision of Infocommunication Services Based on the Blockchain Platform. – PP. 455–459.
Today there are many different ways and means of providing infocommunication services. But, as with any such services and systems, the most pressing issue is the security and convenience of service delivery. One solution to this problem is the possibility of using blockchain technology. In this paper, a blockchain platform is considered, which makes it possible to provide infocommunication services safely, keeping information about the actions performed in the blockchain network. The architecture of this solution is also discussed, and the focus is on the review of smart contracts that are responsible for automation and security of the services provided, as part of the interaction with the Ethereum blockchain network.
Key words: Blockchain, Singularity, distributed ledger, smart contracts, Ethereum, artificial intelligence.

Zhernova K., Kolomeets M. Virtual Reality in Visual Analysis of Graphs. – PP. 460–462.
Analysis of graph data structures is a common task in many areas of computer science: analysis of social networks, computer networks, file systems, service dependencies, etc. This work is devoted to visual analysis of graph structures using virtual reality. The question of the efficiency of information perception by the operator in the analysis of graphs with varying degrees of connectivity and size is investigated. At the same time, effectiveness is evaluated by objective indicators (speed of decision making and accuracy of task performance in visual analysis) and subjective indicators (ease of use of virtual reality in visual analytics). The assessment is done by a double randomized method in comparison with the use of a computer screen, keyboard and mouse.
Key words: Virtual reality, information security, user interfaces, data visualization, performance evaluation.

Zhernova K., Kolomeets M. Review of Methods for Evaluating the Efficiency of Visual Analytics Systems. – PP. 463–466.
Modern computer security tools use a variety of visualization models. These models can vary in level of complexity, and for this reason, the development of models of human-computer interaction that are most suitable for each specific visualization model is required. However, the complexity of the model should not reduce the effectiveness of interaction with this model. This report proposes a methodology for experimental evaluation of the effectiveness of human-computer interaction with computer security applications.
Key words: human-computer interaction, information security, user interfaces, data visualization, efficiency evaluation.

Zhernova K., Komashinskiy N., Kotenko I. Models of Visual Human-Computer Interaction with the Network of Devices in the Internet of Things. – PP. 466–470.
Internet of Things technology is constantly evolving, with the number of devices connected to the Internet of things increasing over time. To manage such a network with a large number of devices and monitor its status, complex visualization models are used, for example, graphs. So, as the network becomes more complex, it becomes necessary to develop new, more efficient models of human-computer interaction with the visualization of the Internet of things network. This paper presents possible solutions for human-computer interaction with a network of devices.
Key words: human-computer interaction, information security, user interfaces, data visualization, Internet of things, touch screens.

Zadorozhnyaya A., Kirichek R., Reutova D. Development of Models and Methods of Interaction Between Self-Driving Vehicles and Network Infrastructure. – PP. 470–473.
Technologies for implementing self-driving vehicles are rapidly developing and will become an integral part of human life in the near future. However, for the convenience of using such technologies, it is necessary to develop a new structure for interaction between self-driving vehicles and the network infrastructure based on the first generation of self-driving vehicles. This is the so-called "concept of the second generation of unmanned vehicles", which is currently being actively studied, and in this regard, the scientific community faces a number of tasks, including the creation of architecture and development of requirements for building a network infrastructure of the self-driving vehicles.
Key words: self-driving vehicle, network infrastructure, sensors, lidars, radar scanners.

Zalesova P., Saenko I. Neural Networks for Monitoring and Countering Unwanted Information on the Internet. – PP. 474–478.
The problem of countering the spread of unwanted information in General, and cyberbullying in particular, on the Internet is acute for modern society. Modern Internet monitoring systems are increasingly being developed using deep learning algorithms for neural networks. The paper explores methods, models and algorithms of deep learning, offers possible implementations and approaches aimed at direct analysis of information. A separate classification of measures to counter the spread of unwanted information is proposed, based on the distribution of responsibility zones among distributors.
Key words: unwanted information, cyberbullying, counteraction, Internet, social networks, neural networks.

Zakharov M., Kirichek R. Analysis of Medicinal Products Based on Public Communication Network Using Methods of Infrared Microspectroscopy. – PP. 478–481.
Currently, the task of analyzing the chemical composition of medicines in order to check their quality is becoming more and more urgent. Often, such analysis is required to be performed in a short time and in the "field", which eliminates the possibility of using traditional methods of laboratory analysis of medicines. To conduct a rapid analysis of the composition of medicines, the authors suggest using a portable infrared microspectrometer connected to a public communication network. Connecting to the SSOP not only provides the ability to transfer the results of molecular analysis to the destination or perform remote analysis on request, but also the ability to remotely process and store analysis data using Cloud Computing and Edge Computing.
Key words: microspectrometer, molecular analysis, public communication network, Cloud Computing, Edge Computing.

Zelenov V., Kirichek R., Shustov N. Development of Methods for Remote Testing of Network Parameters on the Basis of Itu-t Recording q.3056 with Use of Software Probes. – PP. 481–486.
The constant increase in the number of Internet users creates an increasing burden on the network equipment of operators providing access services, which subsequently entails a decrease in the quality of service. This may affect the quality of network access for certain users or organizations that use this service. There is currently no standardized method for measuring such indicators. In this regard, it is advisable to implement a method for remote testing of network parameters based on ITU-T recommendation Q.3056 using software probes, which will allow us to constantly collect and store information on network service quality indicators in real time.
Key words: quality of service, QoS, carrier's network measurement, Draft Recommendation Q.3056 ITU-T, client-server.

Zelenov V., Kirichek R., Shustov N. Development of Methods for Measuring Internet Speed on Fixed and Mobile Communication Networks. – PP. 486–491.
Today, the work of many organizations directly depends on the quality of the Internet connection. Using the method of measuring the speed of the Internet based on Output draft ITU-T Q.3961 will allow us to control the quality of the services provided. There are solutions for measuring the bandwidth of Internet connection such as Speedtest, 2ip, Fast, but they are not based on a standard or recommendation. Therefore, measurements of these systems cannot be considered trusted. Thus, in order to control the quality of the Internet connection using a trusted source, we need the trusted method, which is discussed in this article.
Key words: throughput, quality of network, Output draft ITU-T Q.3961.

Zuyev I., Karelskii P., Kovzur M., Yurkin D. Development of Testing Methodology for IPS Modules. – PP. 492–496.
The protecting of confidential information and its processing processes in a local area network is a priority for any organization falling under federal regulation. One of the common methods for managing information flows which interact with public networks, including the Internet, is to install a firewall at the edge of the local computer network. However, modern approaches to ensuring the security of interworking require the installation of intrusion detection and prevention tools (IPS systems) together with firewalls. The work is devoted to the review of IPS

systems, the development of a test bench for testing and its verification by testing one of the solutions for detection and prevention of intrusions.
Key words: IDS, IPS, corporate network, intrusion prevention, network perimeter protection.

Ivanov V., Savitskiy A. Advantages and Disadvantages of Application of PLC Technologies for Establishing Communications Node Control Using an Automated Communications Node Control System. – PP. 497–501.
Much attention is paid to establishing control and duty shift running at the communications nodes. To achieve these goals, a large number of different types of terminal devices are used at communications nodes. The article analyzes the application of PLC technologies as part of the universal terminal device for intercom and control called "Terminal".
Key words: control, communication node, communications, PLC.

Ivanov V., Savitskiy A. System for Monitoring the Parameters of Equipment and Services of Communication Nodes using a Universal Terminal Intercom Device. – PP. 501–505.
Much attention is paid to establishing control and duty shift running at the communications nodes. The article discusses ways of organization of management at the present stage of development of network process management tools. The main directions/tendencies in the development of the control system and the possibilities of using modern edge software management tools are shown.
Key words: control, communication node, SNMP.

Ivanov V., Reznikov B., Sergeev A. Estimation of the Dispersion Run-Up Length of Optical Signals in Glasses with Different Chemical Compositions. – PP. 505–509.
Due to the increase in speed and the widespread introduction of systems with spectral channel separation, new optical fibers with different chemical compositions are appearing. In this case, there are new influencing factors that can not be ignored in the engineering calculations of the projected or reconstructed communication line. When performing calculations, it is necessary to take into account, in addition to traditional factors, the speed of propagation of different wavelengths, which determines the ability of the system to transmit the largest possible streams of information. In this regard, there is a need to know about the maximum divergence of individual optical channels when light passes through an optical fiber, taking into account the chemical composition of the glass from which the fiber core is made. This will optimize the transmission system both in terms of speed and the maximum length of an elementary cable section or optical path.
Key words: dispersion, transmission rate, chemical composition of glasses, spectral channel separation, phase velocity.

Ivanov N., Radzievskaya T. The Photonics and Radioelectronics Technologies Convergence on High-Speed Data Transmission Buses Fabrication. – PP. 510–514.
High-speed data transmission over a distance between blocks or modules can be achieved by optical methods. The article is focused on polymeric optical wave guides in combination with micro optical devices of interface to connect wave guides with laser- and photodiodes. Production of such optical digital bus based on multiple additive technologies close to 3D MID is suggested.
Key words: polymer planar optical waveguide, additive technologies.

Ivanov S., Sapchenko E., Smirnov I. Application of Field Optical Cables in Robotic Complexes. – PP. 515–519.
The issues of field optical cables application in robotic complexes are considered in this article. The disadvantages of using an optical cable based on quartz optical fibers for controlling robotic complexes are given. The application of polymer optical fiber in field optical cables is justified. The analysis of polymer optical fibers of domestic and foreign producers is given.
Key words: field optical cable, optical fiber, robotic complex, communication lines.

Ivko V., Lapko A. Configuring the Samba File Server in the Operating System Astra Linux Special Edition. – PP. 519–524.
The article is devoted to networking in heterogeneous networks based on Windows and Linux operating systems. The reasonable choice of the Samba file server for the task solution is presented. The Samba file server configuration variants in the Astra Linux SE operating system are presented. The interface and basic functionality of the Samba application are described. The procedure for configuring access to network resources using this application is noted. The structure and parameters of the configuration file are highlighted, an example of its filling is given.
Key words: networking, heterogeneous network, the operating system Astra Linux Special Edition, the Samba file server, the configuration file smb.conf, configuration options.

Kabardov M., Romanova U. Research Key Sharing Protocol for Public Constant Channels. – PP. 525–530
Key distribution protocol: "A protocol for distributing keys over publicly accessible, silent channels, performed without cryptographic assumptions." The protocol itself is based on the calculation of legitimate participants in a session of eigenvalues of randomly generated matrices. In this paper, we obtain the results of studies of the dependence of probabilities on the number of errors with a decrease in the accuracy of intermediate records. An important element when using the protocol is the calculation of the required traffic for its implementation. This work also provides an accurate calculation of this parameter.
Key words: EVSKey scheme, key sharing protocol, protocol of key distribution.

Kalyashov E., Saveleva A., Tarlykov A. Inspection of Custom Network Protocol Packets with Use of Kernel Level Netfilter Module. – PP. 530–535.
The article describes a way to custom ipv6 based network protocol packets' inspection. Netfilter subsystem approaches are provided – module architecture, compilation and installation. Parts of key code fragments are provided. Performance results with fixed hardware are given.
Key words: protocol, packets' filtering, netfilter, kernel module, linux.

Kalyashov E., Saveleva A., Tarlykov A. Custom IP Packets Reception in Java Using Jni to Access System Network Stack. – PP. 536–539.
The article describes a method to receive ip packets of custom type in Java without use of network support in standard Java library. Questions like Java native interface integration and usage of Java direct buffers with it are reviewed. Examples of key code fragments are also provided.
Key words: transport network layer, custom ip packets, java, jni.

Kalyashov E., Tarlykov A. Performance Comparison of Various Queue Implementations with Use of Producer – Consumer Integration Pattern. – PP. 540–544.
The article investigates performance of various producer – consumer pattern topologies in network packets' processing problem. Scenarios for different queue implementations in various tasks are reviewed. System metrics in various modes are also provided.
Key words: producer-consumer pattern, java, queues, threads.

Kalyashov E., Tarlykov A. Binding of Java Execution Threads to Hardware Cpu Cores for Execution Optimization in Linux. – PP. 544–548.
The article describes a way to bind a thread of Java application program to a specific cpu cores. Provided code examples of key fragments based on jni toolkit. Results of application of such technique in network packets' processing task are provided.
Key words: threads, affinity, java.

Kalyashov E., Tarlykov A., Shvidkiy A. Overhead Reduction for Network Packets' Receive in Java With Use of Multiple Reception and Extra Copy Elimination. – PP. 549–553.
The article is dedicated to optimization of network packets' reception in Java without use of standard library. Integration with multiple message reception system call for performance improvement is reviewed. Examples for key code fragments are also provided.
Key words: transport layer, java, jni.

Kalyashov E., Tarlykov A., Shvidkiy A. Recording of Tracks with Use of Location Api and Sensor Framework in Android. – PP. 553–557.
The article reviews possibilities of nowadays smartphones' sensors in object's' motion recording task. Data accuracy of typical hardware sensors is given. Examples for location api and sensor framework integration are provided. Measurements' fusion from multiple sensors for common track accuracy improvements is reviewed.
Key words: track, android, location api, sensor framework.

Kandziouba E. Method for Calculating the Maximum Cable Length of a "Long" Ethernet Cable. – PP. 558–563.
The method of calculating the maximum length of the cable path of the "long" Ethernet based on the regulatory parameters of existing standards is considered. The possibility of calculating the characteristics of a cable intended for broadband transmission of a digital signal based on calculations for one frequency is shown. The determining frequency for the trapezoidal signal described in the ANSI X3.263-1995 standard is 31.25 MHz.
Key words: cable tract, Long Ethernet, crosstalk, signal level, network interface.

Katasonov A., Tcvetkov A. Analysis of Access Restriction Mechanisms in Special Purpose Systems. – PP. 563–568.
Nowadays, the issue of ensuring information security is one of the most acute. It is important not only for each individual user, but also concerns issues of national importance. This article describes the problem of ensuring data security in special-purpose operating systems. An analysis is made of the PARSEC security module used in the Astra Linux special-purpose system.
Key words: Operating Networks, Security, Astra Linux, PARSEC, Administration.

Katina T., Kovtsur M. Algorithm for Detecting Attacks on the N2 5G Network Interface. – PP. 569–573.
This article is devoted to the security problems of 5G networks and the Internet of things. The relevance of the article is due to the fact that the security of 5G networks is an insufficiently studied problem, especially given the critical nature of the possible consequences of a security breach in IoT networks. The article analyzes the security of the NGAP signaling protocol. Based on the analysis of abnormal behavior in 5G networks in the context of the NGAP protocol when conducting a DDoS attack on the subscriber ID, an algorithm for detecting attacks is proposed.
Key words: 5G networks, NG-RAN, DDoS attack, NGAP Protocol, Internet of things.

Kirichek R., Storozhuk M. Development of Models and Methods of Testing Communications Networks 2030. – PP. 574–578.
With the development of the Internet of Things technology, modern networks are under great pressure. For many areas, the quality of the channels through which information is transmitted is very important. Failure to maintain the parameters of these channels can lead to negative consequences. Such networks need continuous monitoring and control. To ensure the fulfillment of the given parameters, new methods for estimating the parameters of networks and equipment capable of performing them are needed.
Key words: 2030 networks, the Internet of things, packet switching technology, parameter measurement.

Kiseleva P., Kislyakov S. Possible Directions of Application of Methods of the Intellectual Data Analysis for Dynamic Management of Autonomous Communication Networks. – PP. 579–583.
Service providers around the world are currently in the process of digitization towards 5G networks. 5G/M2M technologies allow to revise approaches towards "Plug&Play", i.e. developing the concept of Autonomous Networks. The purpose of this article is to reflect the results of research to identify possible areas of application of methods of intellectual data analysis in relation to autonomous networks.
Key words: Autonomous Networks, 5G/M2M, TM Forum, Artificial Intelligence (AI).

Kleverov D., Kotenko I. Adaptation of Bio-Inspired Algorithms for Computer Security Analysis to Big Data Technologies. – PP. 583–588.
With the advent of big data technologies and the increasing complexity of attacks, existing network traffic analysis algorithms require serious revision. The article presents the current state of the art in the field of intrusion detection based on bio-inspired algorithms and suggests various approaches to the adaptation of such algorithms for the analysis of big volume of traffic.
Key words: bio-inspired algorithms, intrusion detection, big data, genetic algorithms, artificial immune system.

Kleverov M., Kotenko I. Big Data Feature Selection using Biclustering Algorithms for the Problem of Cyber-Attack Detection. – PP. 588–592.
Currently, the need to work with big data is one of the key problems in the field of attack detection. To solve this problem, many authors use various methods for selecting important features. The report demonstrated an approach that uses biclustering and allows you to select the most

important data attributes for attack detection based on an analysis of the results of other algorithms. Biclustering algorithms are known for their ability to provide an interpreted result, which makes the proposed approach promising for finding ways to combine various algorithms
Key words: feature selection, machine learning, ensemble classification, biclustering.

Kovalev I., Pashchenko V. Organization Backup and Recovery of Information in Local Computing Networks of Special Purpose Management Systems. – PP. 593–597.
Issues of existing methods of backup and recovery of information are considered. Options for backup and restoring information on the local computing network are offered.
Key words: backup and recovery of information; file backup copy; incremental, differential, full copying.

Kovtsur M., Minyaev A., Potemkin P., Hamza D. Provision Information Security for Web Applications Using Machine Learning. – PP. 597–601.
Most companies use information systems for storing and processing data. With the increase in the use of various web applications, the number of all kinds of attacks increases in order to obtain classified information, starting from all kinds of malicious programs (viruses, worms, etc.) and ending with social engineering. Therefore, the use of machine learning will improve the tracking and forecasting of various types of attacks, which ultimately will make any information system more secure. This article describes the security mechanisms of web applications using machine learning, as well as examples of the successful use of neural networks in the framework of database security.
Key words: machine learning, database, web application, monitoring, threats, tracking, supervised learning.

Kovtsur M., Kozmyan A., Malinin N., Tverdohlebova Y. Experimental Analysis of the Probability and Time of RADIUS Authorization for IP-TV Services. – PP. 601–606.
The study examines client authorizations for accessing the IP-TV service using a RADIUS server. The main parameters of the communication channel that affect the time of access to the service are determined. Charts are constructed that demonstrate the dependence of the access time to the IP-TV service on the parameters of the communication channel, as well as probabilistic dependencies. The results of a practical experiment carried out with the aim of proving the formed mathematical model are presented. A comparison is made of the results of a practical experiment and theoretical calculation, based on which conclusions are drawn.
Key words: authorization, IP-TV, graph, IGMP, multicast, RADIUS.

Kolomeets M., Kotenko I., Chechulin A. Architecture and Implementation of Visual Interfaces for Identification and Opposition of Unwanted, Doubtful and Harmful Information. – PP. 606–609.
Systems for countering unwanted, doubtful and malicious information include expert decision making, which is supported by visual analytics. The paper presents the architecture and an example of the implementation of a hardware-software visualization stand for solving problems of countering information. The system interface is designed to confirm the operation of the classifier of web resources. The operator's interface includes a preview of the resource, statistics on the compliance of a site with a certain category, navigation tools on the database, as well as distribution of the number of resources by category.

Key words: countering information, information security, user interfaces, data visualization, visual analytics.

Komashinsky N., Kotenko I. Methods for Detecting Computer Attacks in High-Load Networks. – PP. 609–614.
The problem of building modern systems for detecting attacks in networks with a large volume of traffic is considered. The main methods for detecting attacks and anomalies in networks with a large volume of circulating traffic are described. The methods used and the composition of intrusion detection systems are analyzed in accordance with the main groups identified. We propose an approach to handling security events to identify cyber attacks in networks with high load through the use of big data technologies. It is based on the use of the Spark Structured Streaming system, load balancers, and Snort detection components.
Key words: computer networks, information system, malicious software, Snort, big data.

Konovalova V., Shterenberg S. Study of the Implementation Policy of the LCD Keypad Shield for the Arduino Microcontrol System. – PP. 614–619.
This article will focus on studying the purpose of an unknown device, how to use it, finding its pros and cons, as well as providing its own example of its use. The main feature is the study of the device at the level of an ordinary user.
Key words: Arduino, LCD Keypad Shield, microcontroller, LiquidCrystal, LCD 1602.

Kotenko I., Pronichev A. Modeling Query Processing Processes in Distributed Big Data Storage Systems. – PP. 620–624.
In big data storage systems, information is distributed across multiple nodes to ensure performance, scalability, availability and integrity. Designing a scalable distributed storage system is a complex and resource-intensive task. Therefore, when designing such systems, modeling is used to preliminary assess the overall performance and identify deficiencies. The report presents the features of modeling the process of processing client requests in the storage system and the main factors affecting the speed of processing requests between system nodes and between the system and the client. An approach to modeling the query processing process is proposed. This approach allows us to measure the efficiency of processing both client requests and the interaction between the modules of the distributed storage system. This approach is supposed to be used to process large volumes of traffic to solve intrusion detection tasks.
Key words: wireless sensor network, self-organizing networks, self-organizing network security.

Kotenko I., Tynymbayev B. Model and Architecture of UEBA System for Cloud Service Provider. – PP. 624–629.
The paper describes the model and architecture of the developed UEBA (User and Entity Behavior Analytics) system, designed to protect the information resources of the cloud service provider. The interaction scheme of the system with sources of information security events is considered. The paper presents an example of using the system to address the security challenges of cloud service provider.
Key words: cybersecurity analytics, user behavior, information security, UEBA.

Kotenko I., Tynymbayev B. Comparative Analysis of Solutions for building UBA and UEBA prospective Systems. – PP. 629–634.
The paper examines current practical solutions for building systems and components of User Behavior Analytics (UBA) and User and Entity Behavior Analytics (UEBA). The paper also provides an overview of scientific research on user behavior analytics. Information on the use of mathematical models in UBA and UEBA systems is systematized.
Key words: cybersecurity analytics, user behavior, information security, UEBA.

Kotenko I., Ushakov I. Big Data Representation Model about Insider Attacks in NoSQL Format. – PP. 634–639.
The article discusses the developing of a Big Data representation model about insider attacks in NoSQL format for detecting insiders in the Computer Networks. The task is to collect the maximum amount of data from the system, create user behavior profiles with their help, and determine from this collected information the behavior of which users differs from normal behavior. Further, based on this information, it is possible to identify insiders and how they can carry out unauthorized actions.
Key words: information security, insider attacks, computer networks, NoSQL, Big Data representation model.

Kotenko I., Ushakov I. Detection of Insiders in Computer Networks Based on Expert Rules and Machine Learning Methods. – PP. 639–643.
The article discusses approaches to detecting insiders in a computer network based on expert rules and machine learning methods.
Key words: information security, insider attacks, computer networks, expert rules, machine learning methods.

Kotenko I., Khinenzon A. Analysis of Algorithms for Detecting Suspicious Behavior in Social Networks. – PP. 644–648.
The issue of ensuring information security in the social networks area is a number one objective in the modern world. Machine learning algorithms and deep data analysis may be possible ways to solve this problem with the rapid development of information technologies. The authors explore machine learning models, methods, and algorithms, as well as statistical data analysis used to detect suspicious behavior in social networks. The paper considers existing approaches, forms sets of signs of suspicious behavior, and offers a classification of accounts based on them.
Key words: machine learning, social networks, suspicious behavior, information security.

Krasov A., Krylov A., Ushakov I. Designing a Network Segment of the APK "Safe city" and Researching Methods to Ensure Protection from Outsider Threats. – PP. 649–653.
Modern cities must meet the increasing information needs of citizens and autonomously ensure their security. To do this, the networks that unite the APK in a single structure are being improved and expanded, new opportunities are emerging and the level of security of such networks is growing. Cities, in the near future, will become more convenient and safer for everyone, thanks to the introduction of APK everywhere.
Key words: security, APK "Safe city", a segment of the city-level network, the introduction of a security system, methods of protection against outsider attacks.

Krayushkin A., Kryukov O., Romanov D., Ulyanov I. Algorithm for Preliminary Identification of the Parameters of the Logic Channel Model of the Multiservice Communication Network. – PP. 653–659.
The problem of preliminary identification of the parameters of the logical channel model of a multiservice communication network using the resource of a communication operator under conditions of non-stationary measured values of the quality of service indicators is considered.
Key words: multiservice communication network, logical channel, quality of service (QoS), hidden Markov model.

Kuznetsov V., Mikutavichaite D. Research into the Influence of Multi-Wave Pumping on the Spectral Range of EDFA's Amplification. – PP. 659–664.
One the most important tasks in the field of infocommunication is to achieve sufficient output signal level in the entire EDFA's gain spectral range. Using of multi-wave pumping allow appreciably reduce the requirements for the pump sources. This article discusses the using of several pump sources with wavelengths different from the effective one – 980 nm. The influence of the amplifier's parameters with multi-wave pumping on input signal's gain with different power levels are considered in the simulation program. The obtained results can be used as a recommendation for amplifier developers and communication line designers.
Key words: erbium optical amplifiers, spectral range, offset, channel compaction.

Kuznetsov E., Pantyukhin O., Ryabov G., Solodukhin B. Features of the Approach to Creation Information Systems in the Interests of Management of Technical Support of Special Purpose. – PP. 664–667.
Significant progress in the field of software and computer technology is currently causing a significant increase in the size and complexity of information systems developed, implemented and applied in various fields of activity of organizations.
A feature of the development of special-purpose information systems is not only the need for strict adherence to state standards in the field of software quality and the development of special-purpose systems, but also the dependence of the structure of the information system on the current structure of governing bodies and their interaction.
Key words: information systems, technical support management.

Kuznetsov K., Muthanna A. S. The Tactile Internet for Industries. – PP. 667–672.
Tactile Internet represents communication networks that allow real-time control, touch transmit, information from sensors and actuators. Such networks should be sufficiently reliable, intelligent and responsive. The article examines the role of the Tactile Internet in modern and future industrial systems, which will allow us to reconsider our views on existing implementations and make it possible to secure human labor, grow up productivity with an increase in quality, make training productive, exciting, etc. A huge number of sensors, information from which can be collected in real time, provide unprecedented accuracy of decisions. It also gives an idea of the 3GPP developments in the field of creating ultra-reliable networks and low latencies – 5G / IMT2020.
Key words: Tactile Internet, 5G, IIoT.

Larionov N., Khodanovich A. Analysis of the Application of Ray Tracing for Conversion of 3D Objects into a Raster Image. – PP. 672–679.
The relevance of ray tracing technology for converting 3D objects into a raster image is substantiated. The perspective directions of development of technologies for 3D visualization of objects in the form of a raster image, the mathematical support of technologies for 3D visualization of objects in the form of a raster image are analyzed, the disadvantages and advantages of existing methods are identified, the analysis of the direction of development of technologies for 3D visualization of objects in the form of a raster image is analyzed, well-known formalizations for technology research are analyzed 3D visualization of objects in the form of a raster image.
Key words: ray tracing, visualization, rendering.

Levshun D. An Attacker Model for a Modern Cyber-Physical System. – PP. 679–682.
The typical model of an attacker involves the classification of an attacker by the level of his knowledge, the resources available to him and the type of access that he has to the target system. So, for example, if one evaluates the knowledge and resources available to the attacker from 1 to 3, then 1 will correspond to the minimum resources and surface knowledge, while 3 will correspond to almost unlimited resources and knowledge sufficient to detect and exploit previously unknown vulnerabilities. The type of access from 1 to 5 shows the system interfaces accessible to the attacker: from (1) access to web services via the Internet to (5) the internal interfaces of individual devices. In the framework of this work, the construction of an attacker model for a modern cyber-physical system is presented. This model takes into account the attacker's possible intentions, including violation of confidentiality and integrity of information, as well as violation of device accessibility and interception of their management. Thus, the solution presented will allow us to answer not only the question "who is attacking?" but also "why?".
Key words: attacker model, cyber-physical system, attack action, intent analysis.

Lepeshkin O., Permyakov A., Shuravin A. Analysis of the Intruder's Ability to Control Traffic in the Infotelecommunication Network. – PP. 683–688.
This article presents a comparative characteristic of software designed to intercept and analyze traffic in a telecommunications network. The author focuses on the architectural features of the tools, analyzes their main advantages and disadvantages in terms of functionality. The analysis of opportunities for extracting route information from traffic by the violator is also performed. Recommendations are formulated to reduce the availability of information that can reveal the structure of the infotelecommunication network.
Key words: traffic analysis, telecommunications network, sniffer, traffic interception.

Lobastova M., Matyukhin A. Model for Assessing the Reliability of the Network of Functioning of Clock Network Synchronization. – PP. 688–692.
The development of modern digital transmission systems cannot be imagined without a well-organized network of clock network synchronization, the main task of which is the coordinated work of network elements. One of the indicators of the TSS is its reliability. To assess the reliability of a network, its model is considered, which reflects the main operating modes of a clock synchronization network, and can be applied to a source of a synchronization signal of any level. In addition, the assessment of network reliability indicators is considered. The methods

under consideration are based on matrix theory, graph theory, probability theory, and reliability theory.
Key words: clock network synchronization, network reliability, network synchronization modes, matrix theory, graph theory.

Makolkina M., Sharlaeva M. Use of the Otsu Method to Calculate the Adaptive Segmentation Threshold. – PP. 693–697.
This article discusses the work of the Otsu method, presents the results of applying the global and adaptive threshold for image segmentation. The method of window filtering of the original image is presented. A comparison is made of the use of the method for calculating the Otsu threshold in cases of the original image with noise and after applying a window filter.
Key words: computer vision, image processing, Otsu method, global threshold, adaptive threshold, image segmentation.

Makolkina M., Sharlaeva M. Application of Threshold Transformation for Image Segmentation. – PP. 697–702.
This article presents development of the concept of "Internet of Things" in the field of healthcare as the emergence of a new idea - "Internet of Medical Things". Existing medical image analyzers and software solutions in the field of artificial intelligence for the diagnosis of diseases are presented. The classification of medical images, methods and phases of their processing are described. A comparative result of the operation of segmentation methods based on threshold transformation implemented using machine learning libraries is presented. Examples of the application of threshold conversion in medical research are considered.
Key words: medical images, artificial intelligence, segmentation, threshold methods, binarization, binary conversion threshold.

Mamashev Z., Muthanna A. S. Research on Object Recognition Methods for Organizing the Movement of Unmanned Vehicles. – PP. 702–707.
Today there is a revolution in the automotive industry. Cars become unmanned, equipped with advanced sensors, cameras and recognition algorithms. Algorithms and scenarios are evolving and improving every day, however, it is too early for unmanned vehicles to enter public roads. The operation of detection algorithms is far from ideal. For the correct and synchronized operation of all elements of an unmanned vehicle, a person needs to transfer all his intellectual experience to artificial intelligence algorithms. This article discusses methods for recognizing various objects by the computer vision system and problems in this area, and also analyzes various options for implementing complex systems of unmanned vehicles.
Key words: unmanned vehicles, computer vision, neural networks, artificial intelligence, object recognition.

Marykov M., Roslyakov A. Technologies for Realizing the NaaS Model. – PP. 707–711.
XaaS is a general, collective term that refers to the delivery of anything as a service. It recognizes the vast number of services. The most promising and developing model of XaaS in telecommunications is NaaS - Network as a Service. In the article technologies for realizing the NaaS model are described: SDN (Software Defined Networking), NFV (Network Function

Virtualization), VON (Virtualized Overlay Networks). In addition, the article considers protocols and solution of the NaaS. In conclusion, we described the advantages and development prospects of the Naas model.
Key words: XaaS, NaaS, Virtualization, Future Networks, SDN, NFV, VONs, telecommunications

Maslakov M. Experimental Check of Single-Tone HF Data Modem Based on ARINC 635 Standard Signals. – PP. 712–716.
The results of real simulation of a single-tone HF data modem model are presented. The main technological designs are considered. The analysis of the performance indicators of a single-tone HF radio line based on the signals of the aviation standard ARINC 635 is carried out.
Key words: data modem, single-toe modem, aviation communication, ARINC 635.

Minyaev A. The Efficiency Evaluation Method of the ISPd Protection System. – PP. 716–719.
The article is reviewed the problem of The efficiency evaluation method of the ISPd protection system. As evaluation criteria, it is proposed to use the project documentation for standard information security systems for distributed information systems. Considered and proposed the method of certification of systems. The obtained results can be used to assess the effectiveness of information protection systems of distributed information systems in accordance with existing legislation.
Key words: information security (IS); certification of the informatization objects (IO); the efficiency evaluation method of the ISPd protection system; the criteria of efficiency evaluation.

Muthanna A. S., Nikitin D. Edge Computing Enabled Smart Cities. – PP. 720–724.
Today there is a significant increase in the population of cities, as well as an increase in the data generated by various devices, such as smartphones, global positioning systems, smart cameras. In recent years, a significant proliferation of computationally demanding applications has been discovered in smart cities. Such applications should provide latency-aware computing capabilities While edge computing is a good technology for resolving issues related to delays, they pose new problems. This article provides a general overview of smart cities and the role of edge computing in them and analyzes the requirements for edge computing enabled smart cities.
Key words: Smart city, MEC, 5G.

Muthanna A. S., Tagandurdyyev N. Analysis of Methods for Building Unmanned Vehicles using Network Support. – PP. 725–729.
The rapid growth of computing power and the emergence of new advanced services and applications leads to a huge increase in network traffic around the world. This phenomenon has not spared the transport industry. Every year, more and more modern applications for cars appear, designed to solve road safety problems, eliminate traffic jams and provide a comfortable transport environment. Along with this, the problem arises of meeting the requirements for communications and computing. MEC and SDN technologies are designed to solve these problems, which will give impetus to the development of the concept of smart car networks. MEC is an in-place computing technology where computing devices are located in close proximity to a source of information, thereby offloading the communications infrastructure. SDN

as well as MEC will remove the main load from computing devices by dividing the control and transmission planes, as well as give more flexibility and scalability to the network.
This article analyzes the construction of an automotive network based on the MEC / SDN architecture. The method of the most effective implementation of these technologies for the deployment of IoT applications and services is considered. This article illustrates the functional features of the transport network architecture of the future. Also shown are the features of the interaction of vehicles with network infrastructure.
Key words: SDN, Edge Computing, 5G, vehicular network, IoT.

Muthanna A. S., Khakimov A., Sharofidinov F. Analysis of Methods and Solutions for the Use of the Internet of Things in the Agricultural Industry. – PP. 730–735.
Due to the Internet of things, new optimal methods of soil cultivation have been discovered using inexpensive equipment (sensors/actuators) and infocommunication technologies (Internet). Remote management and control, crop monitoring, as well as Analytics for predicting the weather, the state of crops in the future, or smart logistics and crop storage are some examples of the new opportunities that the Internet of things opens up. Surely, farmers are experts in agriculture, but, nevertheless, not every one of them has worked with the Internet of things devices. This is why researchers who work with IoT should participate in the development, improving integration and their use in the industry. This article reviews and analyzes solutions and methods of using the Internet of things in the agricultural industry, analyzes new technological solutions that allow you to optimize the production process in agriculture.
Key words: Internet of things, precision agriculture, edge and fog computing.

Nugzarov D., Pantyukhin O., Ryabov G., Shvetsov K. Modeling the Efficiency of the Data Processing Center with the Database Server. – PP. 735–739.
The article discusses the possibilities of modeling the speed of query execution for a data center with a database server. Modeling is a method that allows you to describe processes as they would actually happen. Modeling is used in various fields, in particular, to test the performance characteristics of components of automated systems, such as computers, data transmission channels, computer networks, and data centers.
Key words: data center, automated system, simulation.

Objedkov S., Panteleeva O., Savelyev D., Savelyev S. Analysis of the Application of Software-defined Networks SDN in Condition of the Transition to a Digital Economy. – PP. 740–743.
Software-defined networks, as a platform for providing network services, are becoming increasingly popular in the transition to a digital economy due to the fact, that they allow operators and enterprises to receive unprecedented programming, automation and control, which allows to create scalable, flexible networks that do not require separate configuration of each specific devices and easily adapts to customer requiremants.
Key words: Software-defined networks, digital economy.

Ovechkin G., Seksembayeva M., Tashatov N. The Effect of Fading in Multipath Communication Channel. – PP. 744–749.
This article discusses the mechanism of small-scale fading formation and their description using Nakagami, rice, and Rayleigh distributions.

Key words: multipath channel, digital communication channel model, small-scale fading.

Ozhiganov I., Tatarenkov D. Development of a Software Package for Online Broadcasting. – PP. 749–754.
High-quality online broadcasts of mass events require the use of several television cameras, which creates a need for software that allows switching video signals from cameras. This paper presents software for mobile TV studios. The functionality of this software package includes: switching input signals from TV cameras, capturing images from the speaker's computer (presentations), drawing titles, and running commercials. Broadcast control in this system is possible both with the help of a mixing console and without it.
Key words: TV, broadcasting, software.

Panteleeva O., Savelyev D., Savelyev S. Analysis of the Directions of Increasing the Information Efficiency of Fixed Broadband Subscriber Access Technologies. – PP. 754–759.
In the modern segment of the infocommunication market, various services are in demand, approaching in terms of speed indicators to 1 Gbit/s, and in the near future from 10 to 100 Gbit/s. In connection with these requirements, fixed broadband subscriber access technologies based on the use of fiber-optic cable are becoming increasingly popular. However, the use of symmetrical copper and coaxial subscriber communication lines, both separately and in combination, can also provide high-speed performance sufficient for provision of services to the consumer and commercial segments of the market.
Key words: fixed widescreen subscriber access systems, digital carriers, information efficiency, software-defined networks.

Parashchuk I., Chechulin A. The Essence and Content of the Task of Searching for Interface Vulnerabilities in the Interests of the Safe Control of Unmanned Vehicles of the «Smart City». – PP. 759–763.
Unmanned vehicles are becoming increasingly popular, especially as part of the «smart city» concept. One of the main problems with their application is safety. An important element that affects security is interaction interfaces. The approach to the formulation of the essence and content of the task of searching for vulnerabilities of interfaces such as «man – artificial intelligence» in the interests of the safe control of unmanned vehicles of the «smart city» is considered. The list of tasks includes both the modeling of threats and the functioning processes of unmanned vehicles, and the tasks of intelligent data processing. The solution to these problems will increase the security of unmanned vehicle control systems.
Key words: unmanned vehicles, smart city, interface, vulnerability, threat, data, artificial intelligence.

Pozdnyak I., Filippov T. Ways to Protect From Mobile Code. – PP. 764–767.
Currently, mobile code is a rather serious threat to the information system. Due to the automatic launch due to user negligence, it is difficult to defend against malicious code. In this paper, we consider the general principles of mobile code and possible measures to protect network resources from its harmful effects through the introduction of various control mechanisms that ensure the prevention, detection and removal of malicious code.
Key words: mobile code, security tools, JavaScript, ActiveX.

Polyakova E. Development of a Laboratory Module for the Study of Prismatic Systems on the Element Base of an Optical Designer. – PP. 767–771.
Due to the fact that the set of parts of the optical designer is quite diverse, it is possible to conduct experiments with optical prisms included in it, as well as to create a laboratory layout for visual demonstration of the laws of geometric optics based on optical prismatic systems. Understanding the action of refractive prisms will allow them to be used correctly in optical instrumentation.
Key words: optical prism, optical prismatic system, optical constructor/

Reznikov B. Application of Interference Filters in Optical Communication Systems. – PP. 771–775.
The article describes the scope of optical filters based on multilayer thin-film structures. The use of filters in multiplexers for systems for separating the spectral resource of an optical fiber is considered. The filtering structure of WDM multiplexers is described. The transmission characteristics of filters with a different number of layers are considered.
Key words: Filter, optical communications, DWDM, CWDM, WDM, TFF, thin films.

Reznikov B., Stepanenkov G., Urvantsev G. Overview of Programmable Logic Devices with Optical Interfaces. – PP. 775–779.
The article provides a comparative analysis of programmable logic integrated circuits having optical interfaces. The trends in the application of programmable logic integrated circuits on transport networks and subscriber access networks, as well as data centers implemented on optical transmission media, are examined. The concept of Softly Defined Network, SDNet.
Key words: FPGA, programmable logic, optical communications, systems on a chip, SoC, SDNet, PLD.

Ryzhkov A., Tsvetkov A. Development of a Software Package for Device Audit in Networks. – PP. 779–782.
The rapid growth of computer networks leads to frequent errors in their performance. To ensure efficient operation of the entire system, you need a management platform with integrated tools. This system allows you to quickly get information about the state of equipment and services and quickly respond to failures. This software package can collect, analyze and store incoming information. The introduction of the system significantly reduces the time to find the causes of errors and eliminate them.
Key words: audit, computer networks, ping, ICMP, SNMP, syslog, NTP, operating system.

Sakharov D., Shashkin V. System of Countering the Dissemination of Harmful Information on Social Networks. – PP. 783–787.
Any event causes a public reaction, a public outcry. The information war actively uses this phenomenon, and at the moment, false information has become one of the most popular actions of teams conducting psychological operations. And not only professionals, but also amateurs. Modern media technologies, primarily the Internet, provide enormous opportunities for applying the practice of false information.
Key words: information security, social networks, information wars, information attack, information security threat, social engineering.

Seryozhin E., Yakovlev V. Analysis of the Protocol for Anonymous Calculation user Points of Interest Based on Map Segmentation. – PP. 787–792.
The analysis of the protocol of hidden location of points of interest (POI) of a mobile user is carried out taking into account the type of POI, using homomorphic Paillier and Rabin cryptosystems. The option is considered when the map of the area has a large size and contains a lot of POI. As a result, the server may receive a large number of requests, which will result in a large amount of information being exchanged between users and the server. In order to reduce the computational load on the server and reduce the response time from the server, a protocol modification is proposed by segmenting the binding map and applying a two-stage query, which reduces the amount of information transmitted from the server to the user. Quantitative characteristics of the Protocol's effectiveness are given.
Key words: anonymous calculation, points of interest, geomaps, homomorphic encryption.

Sizova J., Yakovlev V. Analysis of the Security of Protocol Key's Formation Based on using Avispa Program. – PP. 792–797.
At article discusses the characteristics and capabilities of the of Automated Validation of Internet Security Protocols and Applications (AVISPA) program for analysis of the security cryptographic protocols. On based of this program an analysis of the Diffie-Hellman key generation protocol and the "MagPairing" key authenication protocol was performed. Namely the protocol codes was analyzed by the programm, all vulnerabilities were found and attacks on the protocols were reproduced by the application "Security Protocol Animator". It is mportant to include the using of the AVISPA program in the educational process in the study the discipline "Cryptographic Protocols".
Key words: authentication, AVISPA program, security analysis, cryptographic protocols, Diffie-Hellman, MagPairing.

Tarlykov A. Receive of Network Packets in Java with Help of Data Link Layer's Ring Buffer. – PP. 797–802.
The article describes a way improve incoming network packets' processing in Java with help of such Linux capabilities as packet sockets and memory mapped ring buffers. Format of 3rd version of ring buffer is described and approaches of its direct usage in Java are proposed. Performance benefits of this technique in real use case are provided.
Key words: network packets, ring buffer, linux, java.

Khvorova I., Yakovlev V. Key Authentication Distributed Based on the EVSkey Scheme and the using of Physically Unclonable Functions. – PP. 802–807.
The system of key generation between two correspondents through open communication channels, which is based on a modified EVSkey scheme, is considered.
The attacker can control communication channels between correspondents and channels between correspondents and the trusted center and conduct active attacks on them, including a man-in-the-middle attack. A protocol authentication of key generated by correspondents based on the exchange of challenge-response signals between a trusted center and correspondents using physically unclonable functions that each correspondent has, is proposed.
Key words: key generation, key authentication, physically unclonable functions, hash functions.

Shustova E. Provision of Technical Protection of Information in Fiber Optical Transmission Systems. – PP. 807–811.

Development of a monitoring system for fiber-optic communication lines and ensuring technical protection of information circulating in telecommunication systems and automated process control systems for various purposes, with limited data transmission via fiber-optic communication lines that go beyond controlled areas.

Key words: fiber-optic transmission systems, optical time-domain reflectometer, monitoring system.

АВТОРЫ СТАТЕЙ

АБИЛОВ Альберт Винерович — кандидат технических наук, доцент кафедры сети связи и телекоммуникационные системы Ижевского государственного технического университета им. М. Т. Калашникова, albert.abilov@gmail.com

АБРАМОВ Сергей Степанович — доктор технических наук, доцент, профессор кафедры радиотехнических устройств Сибирского государственного университета телекоммуникации и информатики, abramov@sibsutis.ru

АБРАМОВА Евгения Сергеевна — кандидат технических наук, доцент, доцент кафедры радиотехнических устройств Сибирского государственного университета телекоммуникации и информатики, evgenka_252@mail.ru

АВДЕЕВА Маргарита Леонидовна — студентка группы ИКТЗ-63 Санкт-Петербургского государственного университета телекоммуникаций им. проф. М. А. Бонч-Бруевича, avdeeva18marg@gmail.com

АГЕЕВ Сергей Александрович — кандидат технических наук, доцент, ведущий научный сотрудник Санкт-Петербургского института информатики и автоматизации Российской академии наук, ageev_sa@mail.ru

АГЕЕВА Анастасия Дмитриевна — студент группы ИКТМ-82м Санкт-Петербургского государственного университета телекоммуникаций им. проф. М. А. Бонч-Бруевича, iageevanastya@mail.ru

АЛЗАГИР Аббас Али Хасан — аспирант кафедры сетей связи и передачи данных Санкт-Петербургского государственного университета телекоммуникаций им. проф. М. А. Бонч-Бруевича, abbasaltamimi89@gmail.com

АЛЬШАЕВ Виктор Алексеевич — студент группы ИКТЗ-64 Санкт-Петербургского государственного университета телекоммуникаций им. проф. М. А. Бонч-Бруевича; ООО «НГКМ», младший инженер технической поддержки, alshaev2011@yandex.ru

АНДРЕЕВ Дмитрий Павлович — сотрудник ООО «НПП «ИТС», dmitrij-andreev-2000@inbox.ru

АНДРЕЕВ Владимир Александрович — доктор технических наук, профессор, президент Поволжского государственного университета телекоммуникаций и информатики, andreev@psati.ru

АНДРЕЕВА Елена Ивановна — кандидат физико-математических наук, доцент кафедры фотоники и линий связи Санкт-Петербургского государственного университета телекоммуникаций им. проф. М. А. Бонч-Бруевича, andreeva.elena@sut.ru

АНДРИАНОВ Владимир Игоревич — кандидат технических наук, доцент кафедры защищенных систем связи Санкт-Петербургского государственного университета телекоммуникаций им. проф. М. А. Бонч-Бруевича, vladimir.i.andrianov@gmail.com

АНИСИМОВ Антон Сергеевич — студент группы ИКТГ-48м Санкт-Петербургского государственного университета телекоммуникаций им. проф. М. А. Бонч-Бруевича, Oki1515@gmail.com

АНИСИМОВ Даниил Густавович — студент группы ИКТУ-68 Санкт-Петербургского государственного университета телекоммуникаций им. проф. М. А. Бонч-Бруевича, anisimovdd@outlook.com

АНУФРЕНКО Александр Викторович — кандидат технических наук, научный сотрудник научно-исследовательского центра Военной академии связи им. Маршала Советского Союза С. М. Будённого, leroi88@mail.ru

АПТРИЕВА Елизавета Алексеевна — студентка группы ИКТК-66 Санкт-Петербургского государственного университета телекоммуникаций им. проф. М. А. Бонч-Бруевича, lizok.5757@gmail.com

АХРАМЕЕВА Ксения Андреевна — кандидат технических наук, доцент кафедры защищенные системы связи Санкт-Петербургского государственного университета телекоммуникаций им. проф. М. А. Бонч-Бруевича, cbor.mail@gmail.com

БАТЕНКОВ Кирилл Александрович — доктор технических наук, доцент, сотрудник Академии Федеральной службы охраны Российской Федерации, pustur@yandex.ru

БАХТИН Дмитрий Витальевич — студент группы ИКТБ-88м Санкт-Петербургского государственного университета телекоммуникаций им. проф. М. А. Бонч-Бруевича, drivan289@gmail.com

БАХТИН Юрий Евгеньевич — младший научный сотрудник Санкт-Петербургского института информатики и автоматизации Российской академии наук (СПИИРАН), лаборатория проблем компьютерной безопасности, bakhtin@comsec.spb.ru

БЕЗУГЛОВ Михаил Юрьевич — студент Санкт-Петербургского государственного университета телекоммуникаций им. проф. М. А. Бонч-Бруевича, bezuglov61@mail.ru

БЕЛОВ Станислав Михайлович — магистрант кафедры автоматизации предприятий связи Санкт-Петербургского государственного университета телекоммуникаций им. проф. М. А. Бонч-Бруевича, madl@inbox.ru

БЕРЕЗИНА Елизавета Олеговна — студент группы ИКТБ-97М Санкт-Петербургского государственного университета телекоммуникаций им. проф. М. А. Бонч-Бруевича, berezinaelizaveta@icloud.com

БИРЮКОВА Наталья Владимировна — студент группы ИКТС-83м Санкт-Петербургского государственного университета телекоммуникаций им. проф. М. А. Бонч-Бруевича, natabir316@gmail.com

БОБРОВА Ксения Борисовна — старший техник отдела перспективных сетевых технологий научно-исследовательского центра ОАО «Радиоавионика», студентка Петербургского государственного университета путей сообщения Императора Александра I, atorina141@yandex.ru

БОГДАНОВА Любовь Николаевна — студентка группы ИКТБ-97М Санкт-Петербургского государственного университета телекоммуникаций им. проф. М.А. Бонч-Бруевича, lyubogdanova1996@yandex.ru

БОЙКО Алексей Павлович — кандидат технических наук, старший преподаватель кафедры военных систем многоканальной электропроводной и оптической связи Военной академии связи имени Маршала Советского Союза С. М. Буденного, varenyxa007@rambler.ru

БОРОДИНА Полина Евгеньевна — студент группы ИКВТ-61 Санкт-Петербургского государственного университета телекоммуникаций им. проф. М. А. Бонч-Бруевича, p.borodina@yandex.ru

БРАНИЦКИЙ Александр Александрович — кандидат технических наук, старший научный сотрудник Санкт-Петербургского института информатики и автоматизации Российской академии наук, доцент кафедры защищенных систем связи Санкт-Петербургского государственного университета телекоммуникаций им. проф. М. А. Бонч-Бруевича, branitskiy@comsec.spb.ru

БРЫДЧЕНКО Александр Владимирович — кандидат технических наук, преподаватель Военного учебного центра Санкт-Петербургского государственного университета телекоммуникаций им. проф. М. А. Бонч-Бруевича, baw1979@mail.ru

БУДЫЛДИНА Надежда Вениаминовна — кандидат технических наук, доцент кафедры общепрофессиональных дисциплин технических специальностей Уральского технического института связи и информатики (филиал) ФГБОУ ВО «Сибирский государственный университет телекоммуникаций и информатики» в г. Екатеринбурге, 20bnv@mail.ru

БУРАНОВА Марина Анатольевна — кандидат технических наук, доцент кафедры информационной безопасности Поволжского государственного университета телекоммуникаций и информатики, mburanova@yandex.ru

БУРДИН Антон Владимирович — доктор технических наук, профессор, профессор кафедры линии связи и измерения в технике связи Поволжского государственного университета телекоммуникаций и информатики, bourdine@psuti.ru

БУРДИН Владимир Александрович — доктор технических наук, профессор, заведующий кафедрой линии связи и измерения в технике связи Поволжского государственного университета телекоммуникаций и информатики, burdin@psati.ru

БУШУЕВ Сергей Николаевич — доктор технических наук, профессор, заместитель генерального директора ЗАО «НПП ТЕЛДА», г. Санкт-Петербург, bsn@telda.ru

БЫЛИНА Мария Сергеевна — кандидат технических наук, доцент, заведующий кафедрой фотоники и линий связи Санкт-Петербургского государственного университета телекоммуникаций им. проф. М. А. Бонч-Бруевича, BylinaMaria@mail.ru

ВАЛИЕВА Кристина Альбертовна — студентка группы ИКТБ-97М Санкт-Петербургского государственного университета телекоммуникаций им. проф. М. А. Бонч-Бруевича, kristinavalievaa@gmail.com

ВАЛЮХОВ Владимир Петрович — доктор технических наук, профессор Института физики, нанотехнологий и телекоммуникаций Санкт-Петербургского политехнического университета Петра Великого, valyukhov@yandex.ru

ВАСИЛЬЕВ Данил Сергеевич — кандидат технических наук, доцент кафедры сети связи и телекоммуникационные системы Ижевского государственного технического университета имени М. Т. Калашникова, selaan@gmail.com

ВАСЫЛИВ Назар Иванович — студент группы ИКТС-83м Санкт-Петербургского государственного университета телекоммуникаций им М. А. Бонч-Бруевича, nazarvasyliv1@gmail.com

ВАСЮТКИН Артём Васильевич — студент группы ИКВТ-61 Санкт-Петербургского государственного университета телекоммуникаций им. проф. М. А. Бонч-Бруевича, artemcoman98@gmail.com

ВЕРШИНИНА Ксения Витальевна — студентка группы ИКТО-61 Санкт-Петербургского государственного университета телекоммуникаций им. проф. М. А. Бонч-Бруевича, xenia.vershinina@mail.ru

ВИКУЛОВА Александра Юрьевна — главный специалист информационной службы Санкт-Петербургского государственного университета телекоммуникаций им. проф. М.А. Бонч-Бруевича, aleksandra_kokur@mail.ru

ВИТКОВА Лидия Андреевна — старший преподаватель кафедры защищенных систем связи Санкт-Петербургский государственный университет телекоммуникаций им. проф. М. А. Бонч-Бруевича, vitkova@comsec.spb.ru

ВЛАДИМИРОВ Сергей Александрович — старший преподаватель кафедры сети связи и передача данных Санкт-Петербургского государственного университета телекоммуникаций им. проф. М. А. Бонч-Бруевича, vlsa.vlcom@yandex.ru

ВЛАДИМИРОВ Сергей Сергеевич — кандидат технических наук, доцент кафедры сетей связи и передачи данных Санкт-Петербургского государственного университета телекоммуникаций им. проф. М. А. Бонч-Бруевича, vladimirov.opds@gmail.com

ВНУЧКОВА Варвара Дмитриевна — студентка группы ИКТЗ-64 Санкт-Петербургского государственного университета телекоммуникаций им. проф. М. А. Бонч-Бруевича, k1rilovanatasha@yandex.ru

ВОЛОСТНЫХ Виктор Анатольевич — кандидат военных наук, руководитель информационной службы Санкт-Петербургского государственного университета телекоммуникаций им. проф. М. А. Бонч-Бруевича, ra1alo@mail.ru

ГАБУЕВ Арсен Георгиевич — студент группы ИКБ-72 Санкт-Петербургского государственного университета телекоммуникаций им. проф. М. А. Бонч-Бруевича, GoldenTiger1337@yandex.ru

ГАВРИЛЮК Владимир Андреевич — студент группы ИКТБ-87М Санкт-Петербургского государственного университета телекоммуникаций им. проф. М. А. Бонч-Бруевича, vladgavr96@gmail.com

ГАЙФУЛИНА Диана Альбертовна — младший научный сотрудник лаборатории проблем компьютерной безопасности Санкт-Петербургского института информатики и автоматизации Российской академии наук (СПИИРАН), diana-lina95@yandex.ru

ГАЛАКТИОНОВ Михаил Алексеевич — студент группы ИКПИ-61 Санкт-Петербургского государственного университета телекоммуникаций им. проф. М. А. Бонч-Бруевича, mgalaktionov4@gmail.com

ГАМИДОВ Тимур Октаевич — магистрант кафедры защищенных систем связи Санкт-Петербургского государственного университета телекоммуникаций им. проф. М. А. Бонч-Бруевича, dakota4126@gmail.com

ГАРИФУЛЛИН Валерий Флоритович — студент группы ИКВТ-62 Санкт-Петербургского государственного университета телекоммуникаций им. проф. М. А. Бонч-Бруевича, gval98@gmail.com

ГВОЗДЕВ Юрий Васильевич — старший преподаватель кафедры защищенных систем связи Санкт-Петербургского государственного университета телекоммуникаций им. проф. М. А. Бонч-Бруевича, caraim@yandex.ru

ГЕВЕЛЬ Марина Дмитриевна — студентка группы ИКТВ-63 Санкт-Петербургского государственного университета телекоммуникаций им. проф. М. А. Бонч-Бруевича, marinagevel@gmail.com

ГЕЛЬФАНД Артем Максимович — ассистент кафедры защищенных систем связи Санкт-Петербургского государственного университета телекоммуникаций им. проф. М. А. Бонч-Бруевича, amgelfand@mail.ru

ГЕРАСИМОВИЧ Александр Сергеевич — аспирант кафедры защищенных систем связи Санкт-Петербургского государственного университета телекоммуникаций им. проф. М. А. Бонч-Бруевича, Alexgera93@gmail.com

ГЕРЛИНГ Екатерина Юрьевна — кандидат технических наук, доцент кафедры безопасности информационных систем Санкт-Петербургского государственного университета телекоммуникаций им. проф. М. А. Бонч-Бруевича, gerlingeu@gmail.com

ГЛАДЫШЕВА Полина Алексеевна — студентка кафедры защищенных систем связи Санкт-Петербургского государственного университета телекоммуникаций им. проф. М. А. Бонч-Бруевича, polina9810@mail.ru

ГЛУХОВСКИЙ Михаил Дмитриевич — студент группы ИКТЗ-81М Санкт-Петербургского государственного университета телекоммуникаций им. проф. М. А. Бонч-Бруевича, mikhail-glukhovsky@yandex.ru

ГОЛОВЛЁВА Юлия Андреевна — студент группы ИКТЗ-88м Санкт-Петербургского государственного университета телекоммуникаций им. проф. М. А. Бонч-Бруевича, golovlyova96@mail.ru

ГОЛЬДШТЕЙН Александр Борисович — кандидат технических наук, доцент кафедры инфокоммуникационных систем Санкт-Петербургского государственного университета телекоммуникаций им. проф. М. А. Бонч-Бруевича, agold@niits.ru

ГОЛЬДШТЕЙН Борис Соломонович — доктор технических наук, профессор кафедры инфокоммуникационных систем Санкт-Петербургского государственного университета телекоммуникаций им. проф. М. А. Бонч-Бруевича, bgold@sut.ru

ГОРЛОВ Сергей Евгеньевич — студент группы ИКТЗ-64 Санкт-Петербургского государственного университета телекоммуникаций им. проф. М. А. Бонч-Бруевича, s.gorlov123@gmail.com

ГРЕБЕНЩИКОВА Александра Андреевна — студентка группы ИКТМ-82М Санкт-Петербургского государственного университета телекоммуникаций им. проф. М. А. Бонч-Бруевича, sgreben1@mail.ru

ГРЕБЕНЮК Владислав Петрович — студент группы ИКТС-83М Санкт-Петербургского государственного университета телекоммуникаций им. проф. М. А. Бонч-Бруевича, vladg2e@gmail.com

ГРИГОРЬЕВ Максим Дмитриевич — студент группы К-580 Санкт-Петербургского колледжа телекоммуникаций, maximkagrig@gmail.com

ГУБАЙДУЛЛИН Роберт Радикович — аспирант, ассистент кафедры радиофотонники и микроволновых технологий Казанского национального исследовательского технического университета им. А. Н. Туполева – КАИ, diablogrr@gmail.com

ГУСЕВА Юлия Олеговна — студентка магистратуры Уральского технического института связи и информатики (филиал) ФГБОУ ВО «Сибирский государственный университет телекоммуникаций и информатики» в г. Екатеринбурге, guyulo@mail.ru

ГУТОВСКИЙ Алексей Сергеевич — студент группы ИКВТ-61 Санкт-Петербургского государственного университета телекоммуникаций им. проф. М. А. Бонч-Бруевича, lesha.gutovsky@yandex.ru

ДАВЫДОВА София Алексеевна — студентка группы К-580 Санкт-Петербургского колледжа телекоммуникаций, sofia.davidova999@gmail.com

ДАВЫДОВА Анастасия Валентиновна — аспирант кафедры электрической тяги Петербургского государственный университета путей сообщения Императора Александра I, opras26an@yandex.ru

ДАНИЛОВА Юлия Сергеевна — студентка группы ИКБ-71 Санкт-Петербургского государственного университета телекоммуникаций им. проф. М. А. Бонч-Бруевича, danilovajulia123@gmail.com

ДАНЬШИНА Арина Викторовна — студентка группы ИКТЗ-64 Санкт-Петербургского государственного университета телекоммуникаций им. проф. М. А. Бонч-Бруевича, arina_danshina1999@mail.ru

ДЕСНИЦКИЙ Василий Алексеевич — кандидат технических наук, доцент, старший научный сотрудник лаборатории проблем компьютерной безопасности Санкт-Петербургского института информатики и автоматизации Российской академии наук; доцент кафедры защищенных систем связи Санкт-Петербургского государственного университета телекоммуникаций им. проф. М. А. Бонч-Бруевича, vasily.desnitsky@mail.ru

ДЖАФАРОВА Эльнаре Миртаги кызы — диссертант кафедры телекоммуникаций и информационной безопасности Азербайджанского технического университета, elnara.axadova@mail.ru

ДИОРДИЦА Вячеслав Николаевич — студент группы ИКТБ-98м Санкт-Петербургского государственного университета телекоммуникаций им. проф. М. А. Бонч-Бруевича, dior.slavik@gmail.com

ДОЙНИКОВА Елена Владимировна — кандидат технических наук, старший научный сотрудник лаборатории проблем компьютерной безопасности Санкт-Петербургского института информатики и автоматизации Российской академии наук; доцент кафедры защищенных систем связи Санкт-Петербургского государственного университета телекоммуникаций им. проф. М. А. Бонч-Бруевича, doynikova@comsec.spb.ru

ДОКШИН Александр Денисович — студент группы ИКТЗ-64 Санкт-Петербургского государственного университета телекоммуникаций им. проф. М. А. Бонч-Бруевича, a.dokshin007@gmail.com

ДОЛГОМЕР Ася Андреевна — студентка группы ИКТВ-52 Санкт-Петербургского государственного университета телекоммуникаций им. проф. М. А. Бонч-Бруевича, Dolgomer@mail.ru

ДОЛГУН Владислав Олегович — аспирант кафедры информационных управляющих систем Санкт-Петербургского государственного университета телекоммуникаций им. проф. М. А. Бонч-Бруевича, Dolgun@spbgut.ru

ДОНСКОВ Евгений Андреевич — магистрант кафедры защищенных систем связи Санкт-Петербургского государственного университета телекоммуникаций им. проф. М. А. Бонч-Бруевича, radion2002@gmail.com

ДОЦЕНКО Сергей Эдуардович — инженер кафедры фотоники и линий связи Санкт-Петербургского государственного университета телекоммуникаций им. проф. М. А. Бонч-Бруевича, 0472895@gmail.com

ДУДКИНА Ольга Сергеевна — студент группы ИКТБ-87м Санкт-Петербургского государственного университета телекоммуникаций им. проф. М.А. Бонч-Бруевича, dudkinaole4ka.ru@mail.ru

ДУНАЙЦЕВ Роман Альбертович — кандидат технических наук, доцент кафедры сетей связи и передачи данных Санкт-Петербургского государственного университета телекоммуникаций им. проф. М. А. Бонч-Бруевича, roman.dunaytsev@spbgut.ru

ЕГОРОВА Анастасия Леонидовна — студентка группы ИКБ-71 Санкт-Петербургского государственного университета телекоммуникаций им. проф. М. А. Бонч-Бруевича, egorovaucheba@gmail.com

ЕЛАГИН Василий Сергеевич — кандидат технических наук, доцент кафедры инфокоммуникационных систем Санкт-Петербургского государственного университета телекоммуникаций им. проф. М. А. Бонч-Бруевича, elagin.vas@gmail.com

ЕЛИСЕЕВ Сергей Михайлович — студент группы ИКТМ-82М Санкт-Петербургского государственного университета телекоммуникаций им. проф. М. А. Бонч-Бруевича, serdgio96@list.ru

ЕСАЛОВ Кирилл Эдуардович — начальник научно-образовательного центра «Инфокоммуникационных технологий и нейрокогнитивных архитектур» Санкт-Петербургского государственного университета телекоммуникаций им. проф. М. А. Бонч-Бруевича, yk@bonch-ikt.ru

ЖЕРНОВА Ксения Николаевна — аспирант, младший научный сотрудник лаборатории проблем компьютерной безопасности Санкт-Петербургского института информатики и автоматизации Российской академии наук, zhernova@comsec.spb.ru

ЗАДОРОЖНЯЯ Алина Александровна — аспирант кафедры сетей связи и передачи данных Санкт-Петербургского государственного университета телекоммуникаций им. проф. М. А. Бонч-Бруевича, alina27812@mail.ru

ЗАЛЕСОВА Полина Михайловна — студентка группы ИКТЗ-64 Санкт-Петербургского государственного университета телекоммуникаций им. проф. М. А. Бонч-Бруевича, p.zalesova@mail.ru

ЗАХАРОВ Максим Валерьевич — аспирант кафедры сетей связи и передачи данных Санкт-Петербургского государственного университета телекоммуникаций им. проф. М. А. Бонч-Бруевича, zaharov.spbgut@gmail.com

ЗЕЛЕНОВ Василий Васильевич — студент группы ИКТИ-85м Санкт-Петербургского государственного университета телекоммуникаций им. проф. М. А. Бонч-Бруевича, разработчик web-приложений ООО «НТЦ АРГУС», ze_vs@outlook.com

ЗУЕВ Игорь Павлович — студент группы ИКТБ-88м Санкт-Петербургского государственного университета телекоммуникаций им. проф. М. А. Бонч-Бруевича, zuyev.i.p@mail.ru

ИБРАГИМОВ Байрам Ганимат оглы — доктор технических наук, профессор кафедры телекоммуникаций и информационной безопасности Азербайджанского технического университета, i.bayram@mail.ru

ИВАНОВ Александр Юрьевич — научный сотрудник Санкт-Петербургского института информатики и автоматизации Российской академии наук, лаборатория проблем компьютерной безопасности, vniira@yandex.ru

ИВАНОВ Олег Андреевич — студент группы ИКТФ-86м Санкт-Петербургского государственного университета телекоммуникаций им. проф. М. А. Бонч-Бруевича, ioleg0210@gmail.com

ИВАНОВ Василий Геннадьевич — кандидат военных наук, доцент кафедры боевого применения войск связи Военной академии связи им. Маршала Советского союза С. М. Буденного, wasj2006@yandex.ru

ИВАНОВ Владимир Степанович — кандидат технических наук, доцент кафедры фотоники и линий связи Санкт-Петербургского государственного университета телекоммуникаций им. проф. М. А. Бонч-Бруевича, vsivanovspb@yandex.ru

ИВАНОВ Николай Николаевич — доктор технических наук, заместитель директора института магистратуры по научной работе Санкт-Петербургского государственного университета телекоммуникаций им. проф. М. А. Бонч-Бруевича, ivanov.2nik@ya.ru

ИВАНОВ Сергей Александрович — кандидат технических наук, докторант Военной академии связи им. Маршала Советского союза С. М. Буденного, sa-ivanov@inbox.ru

ИВКО Вадим Игоревич — студент Академии Федеральной службы охраны Российской Федерации, ivadi@bk.ru

ИЗРАИЛОВ Константин Евгеньевич — кандидат технических наук, доцент кафедры защищенных систем связи Санкт-Петербургского государственного университета телекоммуникаций им. проф. М. А. Бонч-Бруевича, Konstantin.Izrailov@mail.ru

ИСМАЙЛОВА Севиндж Рамиз кызы — кандидат технических наук, старший преподаватель кафедры информационных технологий и программирования Азербайджанского технического университета, sevinc_ism@hotmail.com

ИСТОМИН Дмитрий Андреевич — студент группы ИКТК-65 Санкт-Петербургского государственного университета телекоммуникаций им. проф. М. А. Бонч-Бруевича, dimanbras71@gmail.com

КАБАРДОВ Муаед Мусович — кандидат физико-математических наук, доцент кафедры высшей математики Санкт-Петербургского государственного университета телекоммуникаций им. проф. М. А. Бонч-Бруевича, kabardov@bk.ru

КАЗАНЦЕВ Алексей Анатольевич — инженер кафедры защищенных систем связи Санкт-Петербургского государственного университета телекоммуникаций им. проф. М. А. Бонч-Бруевича, Farvest.ax@yandex.ru

КАЙСИНА Ирина Алексеевна — аспирант кафедры радиотехника Ижевского государственного технического университета имени М. Т. Калашникова, irinakaysina25@gmail.com

КАЛЯШОВ Евгений Владимирович — инженер-программист научно-образовательного центра «Лаборатория программирования» Санкт-Петербургского государственного университета телекоммуникаций им. проф. М. А. Бонч-Бруевича, ekalyshov@gmail.com

КАНАЕВ Андрей Константинович — доктор технических наук, профессор, заведующий кафедрой «Электрическая связь» Петербургского государственного университета путей сообщения Императора Александра I, kanaev@pgups.ru

КАНДЗЮБА Евгений Владимирович — аспирант Московского технического университета связи и информатики, ekandziouba@gmail.com

КАРЕЛЬСКИЙ Павел Владимирович — студент группы ИКТБ-88м Санкт-Петербургского государственного университета телекоммуникаций им. проф. М. А. Бонч-Бруевича, pasha.karelscky@yandex.ru

КАТАСОНОВ Александр Игоревич — студент группы ИКБ-61 Санкт-Петербургского государственного университета телекоммуникаций им. проф. М. А. Бонч-Бруевича, ksasha716@yandex.ru

КАТИНА Татьяна Владимировна — студентка группы ИКТБ-97м Санкт-Петербургского государственного университета телекоммуникаций им. М. А. Бонч-Бруевича, katina.tanya.net@gmail.com

КАЧАЛОВ Владислав Алексеевич — студент группы ИКТС-83М Санкт-Петербургского государственного университета телекоммуникаций им. проф. М.А. Бонч-Бруевича, kachalov.vladislav@gmail.com

КИРИЛЛОВ Даниил Игоревич — старший преподаватель кафедры защищенных систем связи Санкт-Петербургского государственного университета телекоммуникаций им. проф. М. А. Бонч-Бруевича, daniil.kirillov@gmail.com

КИРИЧЁК Руслан Валентинович — доктор технических наук, профессор кафедры сетей связи и передачи данных Санкт-Петербургского государственного университета телекоммуникаций им. проф. М. А. Бонч-Бруевича, kirichek@sut.ru

КИСЕЛЕВА Алена Андреевна — студент группы ИКТБ-98М Санкт-Петербургского государственного университета телекоммуникаций им. проф. М. А. Бонч-Бруевича, kiseleva.a27@mail.ru

КИСЕЛЕВА Полина Владимировна — студентка группы ИКТК-66 Санкт-Петербургского государственного университета телекоммуникаций им. проф. М. А. Бонч-Бруевича, appolinarey@gmail.com

КИСЛЯКОВ Сергей Викторович — кандидат технических наук, доцент кафедры инфокоммуникационных систем Санкт-Петербургского государственного университета телекоммуникаций им. проф. М. А. Бонч-Бруевича, бизнес-аналитик ООО «НТЦ Аргус», s.v.kislyakov@gmail.com

КЛЕВЕРОВ Денис Анатольевич — аспирант, младший научный сотрудник лаборатории проблем компьютерной безопасности Санкт-Петербургского института информатики и автоматизации Российской академии наук, denklewer@gmail.com

КЛЕВЕРОВ Максим Анатольевич — аспирант Санкт-Петербургского института информатики и автоматизации Российской академии наук, klevermx@gmail.com

КОБЗЕВ Кирилл Олегович — студент группы ИКТС-83С Санкт-Петербургского государственного университета телекоммуникаций им. проф. М. А. Бонч-Бруевича, noxis-96@yandex.ru

КОВАЛЕВ Игорь Станиславович — кандидат военных наук, доцент, преподаватель кафедры Военной академии связи им. Маршала Советского Союза С. М. Буденного, iskova@yandex.ru

КОВЦУР Максим Михайлович — кандидат технических наук, доцент кафедры защищенных систем связи Санкт-Петербургского государственного университета телекоммуникаций им. проф. М. А. Бонч-Бруевича, maxkovzur@mail.ru

КОЗЬМЯН Александр Владимирович — студент Санкт-Петербургского государственного университета телекоммуникаций им. проф. М. А. Бонч-Бруевича, avk96@list.ru

КОЛОМЕЕЦ Максим Вадимович — аспирант Санкт-Петербургского национального исследовательского университета информационных технологий, механики и оптики; младший научный сотрудник лаборатории проблем компьютерной безопасности Санкт-Петербургского института информатики и автоматизации Российской академии наук, kolomeec@comsec.spb.ru

КОМАШИНСКИЙ Владимир Ильич — доктор технических наук, профессор, доцент кафедры беспроводных телекоммуникаций Национального исследовательского университета информатики механики и оптики», kama54@rambler.ru

КОМАШИНСКИЙ Николай Александрович — аспирант лаборатории проблем компьютерной безопасности Санкт-Петербургского института информатики и автоматизации Российской академии наук, komashinsky@comsec.spb.ru

КОНОВАЛОВА Виктория Вадимовна — студентка группы ИКБ-72 Санкт-Петербургского государственного университета телекоммуникаций им. проф. М. А. Бонч-Бруевича, konovalova.viktoriuya.99@mail.ru

КОНОНОВ Павел Александрович — начальник отдела технической защиты информации Санкт-Петербургского государственного университета телекоммуникаций им. проф. М. А. Бонч-Бруевича, kononov.pa@spbgut.ru

КОПАЛИН Константин Русланович — студент Санкт-Петербургского государственного университета телекоммуникаций им. проф. М. А. Бонч-Бруевича, andreeva.elena@sut.ru

КОРЖИК Валерий Иванович — доктор технических наук, почётный профессор кафедры защищенных систем связи Санкт-Петербургского государственного университета телекоммуникаций им. проф. М. А. Бонч-Бруевича, val-korzhik@yandex.ru

КОРОЛЕВ Александр Васильевич — кандидат технических наук, доцент, сотрудник Академии Федеральной службы охраны Российской Федерации, pustur@yandex.ru

КОТЕНКО Игорь Витальевич — доктор технических наук, профессор, заведующий лабораторией проблем компьютерной безопасности Санкт-Петербургского института информатики и автоматизации Российской академии наук, ivkote@comsec.spb.ru

КОШКИН Станислав Сергеевич — студент группы ИКВТ-61 Санкт-Петербургского государственного университета телекоммуникаций им. проф. М. А. Бонч-Бруевича, stasevich1010@gmail.com

КРАСОВ Андрей Владимирович — кандидат технических наук, доцент, заведующий кафедрой защищенных систем связи Санкт-Петербургского государственного университета телекоммуникаций им. проф. М. А. Бонч-Бруевича, krasov@inbox.ru

КРАЮШКИН Андрей Романович — сотрудник Академии Федеральной службы охраны Российской Федерации, ilya@academ.msk.rsnet.ru

КРИВОНОСОВА Наталья Викторовна — преподаватель Санкт-Петербургского колледжа телекоммуникаций, nvkrivonosowa@mail.ru

КРЫЛОВ Алексей Вадимович — студент группы ИКТЗ-63 Санкт-Петербургского государственного университета телекоммуникаций им. проф. М. А. Бонч-Бруевича, Krylov180497@yandex.ru

КРЮКОВ Олег Витальевич — кандидат технических наук, доцент, сотрудник Академии Федеральной службы охраны Российской Федерации, ilya@academ.msk.rsnet.ru

КУЗНЕЦОВ Вячеслав Сергеевич — преподаватель, аспирант кафедры фотоники и линий связи Санкт-Петербургского государственного университета телекоммуникаций им. проф. М. А. Бонч-Бруевича, slava_kuznetsov@inbox.ru

КУЗНЕЦОВ Константин Алексеевич — студент Санкт-Петербургского государственного университета телекоммуникаций им. проф. М. А. Бонч-Бруевича, kuznetsov.sut@gmail.com

КУЗНЕЦОВ Евгений Михайлович — слушатель Военной академии связи имени Маршала Советского Союза С. М. Буденного, Kuznetsov52EM@yandex.ru

КУЗНЕЦОВА Екатерина Александровна — студентка группы ИКТИ-95 Санкт-Петербургского государственного университета телекоммуникаций им. проф. М. А. Бонч-Бруевича, cotti31@gmail.com

КУКУНИН Дмитрий Сергеевич — кандидат технических наук, доцент кафедры систем связи и передачи данных Санкт-Петербургского государственного университета телекоммуникаций им. проф. М. А. Бонч-Бруевича, coux@yandex.ru

КУПЦОВ Владимир Дмитриевич — кандидат технических наук, доцент Института физики, нанотехнологий и телекоммуникаций Санкт-Петербургского политехнического университета Петра Великого, vdkuptsov@yandex.ru

ЛАПКО Александр Николаевич — кандидат технических наук, сотрудник Академии Федеральной службы охраны Российской Федерации, lan46@mail.ru

ЛАРИОНОВ Никита Юрьевич — магистрант кафедры информационных управляющих систем Санкт-Петербургского государственного университета телекоммуникаций им. проф. М. А. Бонч-Бруевича, larionov.nu@gmail.com

ЛЕ Нгуен-Нам — студент Санкт-Петербургского государственного университета телекоммуникаций им. проф. М. А. Бонч-Бруевича, lenguyennam1710@gmail.com

ЛЕВШУН Дмитрий Сергеевич — младший научный сотрудник Санкт-Петербургского института информатики и автоматизации Российской академии наук, levshun@comsec.spb.ru

ЛЕПЕШКИН Олег Михайлович — доктор технических наук, доцент кафедры безопасности инфокоммуникационных систем специального назначения Военной академии связи им. Маршала Советского Союза С. М. Буденного, lepechkin1@ya.ru

ЛОБАНОВА Любовь Михайловна — студентка группы ИКТМ-82м Санкт-Петербургского государственного университета телекоммуникаций им. проф. М. А. Бонч-Бруевича, lobanova@protei.ru

ЛОБАСТОВА Мария Викторовна — старший преподаватель, аспирант кафедры сетей связи и передачи данных Санкт-Петербургского государственного университета телекоммуникаций им. проф. М. А. Бонч-Бруевича, mlobastovabk1@rambler.ru

МАКАРОВ Леонид Михайлович — кандидат технических наук, доцент, доцент кафедры автоматизации предприятий связи Санкт-Петербургского государственного университета телекоммуникаций им. проф. М. А. Бонч-Бруевича, biopet@mail.ru

МАКОЛКИНА Мария Александровна — кандидат технических наук, доцент кафедры сетей связи и передачи данных Санкт-Петербургского государственного университета телекоммуникаций им. проф. М. А. Бонч-Бруевича, makolkina@list.ru

МАЛИНИН Никита Игоревич — студент Санкт-Петербургского государственного университета телекоммуникаций им. проф. М. А. Бонч-Бруевича, hawalo1@yandex.ru

МАМАШЕВ Завур Бекболатгаджиевич — студент группы ИКВТ-61 Санкт-Петербургского государственного университета телекоммуникаций им. проф. М. А. Бонч-Бруевича, zavur.mamashev@mail.ru

МАРЫКОВ Михаил Валерьевич — аспирант кафедры сетей и систем связи Поволжского государственного университета телекоммуникаций и информатики, mikhail.marykov@gmail.com

МАСЛАКОВ Михаил Леонидович — кандидат технических наук, научный сотрудник АО «Российский институт мощного радиостроения» maslakovml@gmail.com

МАТЮХИН Александр Юрьевич — кандидат технических наук, доцент кафедры сетей связи и передачи данных Санкт-Петербургского государственного университета телекоммуникаций им. проф. М. А. Бонч-Бруевича, Matukhin@list.ru

МЕЛЕШКО Алексей Викторович — младший научный сотрудник лаборатории проблем компьютерной безопасности, аспирант Санкт-Петербургского института информатики и автоматизации Российской академии наук, meleshko.a@iias.spb.su

МИКУТАВИЧАЙТЕ Диана Сергеевна — студент Санкт-Петербургского государственного университета телекоммуникаций им. проф. М. А. Бонч-Бруевича, mikutavichaite@bk.ru

МИНЯЕВ Андрей Анатольевич — старший преподаватель кафедры защищенных систем связи Санкт-Петербургского государственного университета телекоммуникаций им. проф. М. А. Бонч-Бруевича, minyaev.a@gmail.com

МИРОНОВ Александр Егорович — кандидат технических наук, доцент, сотрудник Академии Федеральной службы охраны Российской Федерации, pustur@yandex.ru

МИХАЙЛОВА Анастасия Валерьевна — студентка группы ИКТЗ-64 Санкт-Петербургского государственного университета телекоммуникаций им. проф. М. А. Бонч-Бруевича, ova.007@yandex.ru

МИХАЙЛОВА Мария Александровна — студентка группы ИКТВ-63 Санкт-Петербургского государственного университета телекоммуникаций им. проф. М. А. Бонч-Бруевича, mariamihajlova99@gmail.com

МУТХАННА Аммар Салех Али — кандидат технических наук, доцент кафедры сетей связи и передачи данных Санкт-Петербургского государственного университета телекоммуникаций им. проф. М. А. Бонч-Бруевича, ammarexpress@gmail.com

МЫШКИН Вячеслав Федорович — доктор физико-математических наук, профессор, профессор инженерной школы ядерных технологий Национального исследовательского Томского политехнического университета, gos100@tpu.ru

НГУЕН Зуи Кыонг — аспирант кафедры защищенных систем связи Санкт-Петербургского государственного университета телекоммуникаций им. проф. М. А. Бонч-Бруевича, cuong0111@gmail.com

НЕМАНОВ Иван Дмитриевич — студент группы ИКВТ-61 Санкт-Петербургского государственного университета телекоммуникаций им. проф. М. А. Бонч-Бруевича, tcmchw@gmail.com

НИЖГОРОДОВ Антон Олегович — аспирант кафедры линии связи и измерения в технике связи Поволжского государственного университета телекоммуникаций и информатики, anton.socol2017@yandex.ru

НИКИТИН Даниил Витальевич — студент группы ИКВТ-62 Санкт-Петербургского государственного университета телекоммуникаций им. проф. М. А. Бонч-Бруевича, dn-nikitin98@yandex.ru

НОВИКОВА Евгения Сергеевна — кандидат технических наук, старший научный сотрудник лаборатории проблем компьютерной безопасности Санкт-Петербургского института информатики и автоматизации Российской академии наук, novikova@comsec.spb.ru

НУГЗАРОВ Давид Эльбрусович — магистрант Санкт-Петербургского государственного университета телекоммуникаций им. М. А. Бонч-Бруевича, p_oleg99@mail.ru

ОБЪЕДКОВ Семен Алексеевич — сотрудник Академии Федеральной службы охраны Российской Федерации, s_savelyev@mail.ru

ОВЕЧКИН Геннадий Владимирович — доктор технических наук, профессор кафедры «Вычислительная и прикладная математика» Рязанского государственного радиотехнического университета, g_ovechkin@mail.ru

ОЖИГАНОВ Игорь Васильевич — студент группы Р-91м Санкт-Петербургского государственного университета телекоммуникаций имени профессора М. А. Бонч-Бруевича, confirmedancient@mail.ru

ОКУНЕВА Дарина Владимировна — кандидат технических наук, доцент кафедры программной инженерии и вычислительной техники Санкт-Петербургского государственного университета телекоммуникаций им. проф. М. А. Бонч-Бруевича, darina_okuneva@mail.ru

ОЛИМПИЕВ Алексей Александрович — кандидат технических наук, инженер отдела разработки конструкторской документации акционерного общества «Научно-исследовательский институт «Рубин», aao_82@mail.ru

ОРЕШИН Андрей Николаевич — кандидат технических наук, доцент, сотрудник Академии Федеральной службы охраны Российской Федерации, pustur@yandex.ru

ОРЛОВ Григорий Александрович — техник кафедры защищенных систем связи Санкт-Петербургского государственного университета телекоммуникаций им. проф. М. А. Бонч-Бруевича, grigory.a.orlov@gmail.com

ОЩЕНКОВ Филипп Дмитриевич — студент группы ИКБ-72 Санкт-Петербургского государственного университета телекоммуникаций им. проф. М. А. Бонч-Бруевича, shepard990@yandex.ru

ПАВЛОВ Иван Иванович — кандидат технических наук, доцент, доцент кафедры техносферной безопасности Сибирского государственного университета телекоммуникации и информатики, iipavlov02@mail.ru

ПАВЛОВА Мария Сергеевна — ассистент кафедры радиотехнических устройств Сибирского государственного университета телекоммуникации и информатики, mspavlova@ngs.ru

ПАНТЕЛЕЕВА Оксана Николаевна — кандидат педагогических наук, сотрудник Академии Федеральной службы охраны Российской Федерации, s_savelyev@mail.ru

ПАНТЮХИН Олег Игоревич — кандидат технических наук, доцент, доцент кафедры сетей связи и передачи данных Санкт-Петербургского государственного университета телекоммуникаций им. проф. М. А. Бонч-Бруевича; доцент кафедры Военной академии связи им. Маршала Советского Союза С. М. Буденного, p_oleg99@mail.ru

ПАРАЩУК Игорь Борисович — доктор технических наук, профессор, Заслуженный изобретатель РФ, ведущий научный сотрудник Санкт-Петербургского института информатики и автоматизации Российской академии наук, инженер лаборатории Санкт-Петербургского национального исследовательского университета информационных технологий, механики и оптики, shchuk@rambler.ru

ПАЩЕНКО Василий Владимирович — кандидат технических наук, старший преподаватель кафедры Военной академии связи им. Маршала Советского Союза С. М. Буденного, iskova@yandex.ru

ПЕРМЯКОВ Александр Сергеевич — адъюнкт кафедры безопасности инфокоммуникационных систем специального назначения Военной академии связи им. Маршала Советского Союза С. М. Буденного, permyak.as@ya.ru

ПЕШКОВ Андрей Иванович — кандидат философских наук, доцент кафедры защищенных систем связи Санкт-Петербургского государственного университета телекоммуникаций им. проф. М. А. Бонч-Бруевича, ap2000@yandex.ru

ПОЗДНЯК Ирина Сергеевна — кандидат технических наук, доцент кафедры информационной безопасности Поволжского государственного университета телекоммуникаций и информатики, vis_517@mail.ru

ПОЛУБАРЬЕВА Анна Николаевна — студентка группы n41512c Национального исследовательского университета информационных технологий, механики и оптики, anna.polubaryeva@gmail.com

ПОЛЯКОВА Елена Валериевна — старший преподаватель кафедры фотоники и линий связи Санкт-Петербургского государственного университета телекоммуникаций им. проф. М.А. Бонч-Бруевича, e.v@inbox.ru

ПОМОГАЛОВА Альбина Владимировна — ассистент, инженер-программист кафедры программной инженерии и вычислительной техники Санкт-Петербургского государственного университета телекоммуникаций им. проф. М. А. Бонч-Бруевича, a.l.b.i.n.a@bk.ru

ПОТЕМКИН Павел Андреевич — студент магистрант кафедры защищенных систем связи Санкт-Петербургского государственного университета телекоммуникаций им. проф. М. А. Бонч-Бруевича, potiomkinpa98@gmail.com

ПРОНИЧЕВ Алексей Петрович — младший научный сотрудник лаборатории проблем компьютерной безопасности, аспирант Санкт-Петербургского института информатики и автоматизации Российской академии наук, pronichevAP@gmail.com

РАДЗИЕВСКАЯ Тамара Александровна — аспирант кафедры фотоники Санкт-Петербургского государственного электротехнического университета «ЛЭТИ» им. В. И. Ульянова (Ленина), tamaramanvelova239@mail.ru

РЕВЕНКО Юлия Павловна — студентка группы ИКТК-65 кафедры инфокоммуникационных систем Санкт-Петербургского государственного университета телекоммуникаций им. проф. М. А. Бонч-Бруевича, revenko.up@spbgut.ru

РЕЗНИКОВ Богдан Константинович — студент группы ИКТФ-96м, ассистент кафедры фотоники и линий связи Санкт-Петербургского государственного университета телекоммуникаций им. проф. М. А. Бонч-Бруевича, rznkff@gmail.com

РЕЗЯПКИНА Магдалина Игоревна — магистрант кафедры информационной безопасности Поволжского государственного университета телекоммуникаций и информатики, m.rezyapkina@psuti.ru

РЕУТОВА Дарья Олеговна — студентка группы ИКТМ-92М Санкт-Петербургского государственного университета телекоммуникаций им. проф. М. А. Бонч-Бруевича, doreutova@gmail.com

РОДИОНОВ Сергей Алексеевич — кандидат технических наук, инженер-исследователь в области искусственного интеллекта в SingularityNET, astroseger@gmail.com

РОМАНОВ Даниил Владиславович — сотрудник Академии Федеральной службы охраны Российской Федерации, ilya@academ.msk.rsnet.ru

РОМАНОВА Ульяна Михайловна — студент группы ИКТЗ-64 Санкт-Петербургского государственного университета телекоммуникаций им. проф. М. А. Бонч-Бруевича, mur.kataleya@mail.ru

РОСЛЯКОВ Александр Владимирович — доктор технических наук, профессор, заведующий кафедрой сетей и систем связи Поволжского государственного университета телекоммуникаций и информатики, arosl@mail.ru

РУСИН Иван Сергеевич — оператор научной роты Военной академии связи им. Маршала Советского Союза С. М. Будённого, aokruan@gmail.com

РЫЖКОВ Андрей Александрович — студент группы ИКТЗ-64 Санкт-Петербургского государственного университета телекоммуникаций им. проф. М. А. Бонч-Бруевича, ryzhkov.a.a11@gmail.com

РЯБОВ Геннадий Анатольевич — преподаватель Военной академии связи им. Маршала Советского Союза С. М. Буденного, Kuznetsov52EM@yandex.ru

САВЕЛЬЕВ Сергей Николаевич — кандидат технических наук, доцент, сотрудник Академии Федеральной службы охраны Российской Федерации, s_savelyev@mail.ru

САВЕЛЬЕВ Дмитрий Сергеевич — сотрудник Академии Федеральной службы охраны Российской Федерации, s_savelyev@mail.ru

САВЕЛЬЕВА Анастасия Андреевна — аспирант кафедры инфокоммуникационных систем Санкт-Петербургского государственного университета телекоммуникаций им. проф. М. А. Бонч-Бруевича, saa@spbgut.ru

САВИЦКИЙ Алексей Юрьевич — слушатель Военной академии связи им. Маршала Советского союза С. М. Буденного, savialexey7@mail.ru

САЕНКО Игорь Борисович — доктор технических наук, профессор, ведущий научный сотрудник Санкт-Петербургского института информатики и автоматизации Российской академии наук, инженер Санкт-Петербургского национального исследовательского университета информационных технологий, механики и оптики, ibsaen@comsec.spb.ru

САЛТЫКОВ Антон Радиевич — старший преподаватель кафедры фотоники и линий связи Санкт-Петербургского государственного университета телекоммуникаций им. проф. М. А. Бонч-Бруевича, anton.saltykov@gmail.com

САПЧЕНКО Елена Сергеевна — техник научно-исследовательского центра Военной академии связи им. Маршала Советского союза С. М. Буденного, sensemile.nic@mail.ru

САХАРОВ Дмитрий Владимирович — кандидат технических наук, доцент кафедры защищенных систем связи Санкт-Петербургского государственного университета телекоммуникаций им. проф. М. А. Бонч-Бруевича, d.sakharov@rkn.gov.ru

САХАРОВА Мария Александровна — кандидат технических наук, заместитель начальника отдела по разработке систем связи ЗАО «Институт телекоммуникаций»; доцент кафедры «Электрическая связь» Петербургского государственного университета путей сообщения Императора Александра I, zuvakamariya@mail.ru

СЕКСЕМБАЕВА Манара Ануаровна — докторант кафедры «Вычислительная техника» Евразийского национального университета имени Л. Н. Гумилева, sexembayeva_ma_1@edu.enu.kz

СЕРГЕЕВ Алексей Николаевич — старший преподаватель кафедры фотоники и линий связи Санкт-Петербургского государственного университета телекоммуникаций им. проф. М. А. Бонч-Бруевича, a32@bk.ru

СЕРЁЖИН Евгений Антонович — студент группы ИКТБ-98М Санкт-Петербургского государственного университета телекоммуникаций им. проф. М. А. Бонч-Бруевича, se271196@yandex.ru

СИЗОВА Юлия Дмитриевна — студент группы ИКБ-63 Санкт-Петербургского государственного университета телекоммуникаций им. проф. М. А. Бонч-Бруевича, sizovajulya@bk.ru

СМИРНОВ Евгений Витальевич — студент группы ИКТЗ-91М Санкт-Петербургского государственного университета телекоммуникаций им. проф. М. А. Бонч-Бруевича, john.1.9.98@mail.ru

СМИРНОВ Иван Юрьевич — старший научный сотрудник научно-исследовательского центра Военной академии связи им. Маршала Советского союза С. М. Буденного, sensemile.nic@mail.ru

СОЛОДУХИН Борис Владимирович — кандидат военных наук, доцент, преподаватель кафедры Военной академии связи им. Маршала Советского Союза С. М. Буденного, Kuznetsov52EM@yandex.ru

СПИРИДОНОВ Сергей Олегович — студент Санкт-Петербургского государственного университета телекоммуникаций им. проф. М. А. Бонч-Бруевича, andreeva.elena@sut.ru

СПИРКИНА Анастасия Валентиновна — аспирант кафедры инфокоммуникационных систем Санкт-Петербургского государственного университета телекоммуникаций им. проф. М. А. Бонч-Бруевича, anastasia.4991@mail.ru

СПРАВЦЕВА Марина Александровна — студентка группы ИКТЗ-64 Санкт-Петербургского государственного университета телекоммуникаций им. проф. М. А. Бонч-Бруевича, spravtseva.2611@gmail.com

СТАРОСТИН Владимир Сергеевич — кандидат физико-математических наук, доцент кафедры высшей математики Санкт-Петербургского государственного университета телекоммуникаций им. проф. М. А. Бонч-Бруевича, star_vs_47@mail.ru

СТАСЮК Владислав Валерьевич — студент группы ИКТБ-88м Санкт-Петербургского государственного университета телекоммуникаций им. проф. М. А. Бонч-Бруевича, vlad030397@gmail.com

СТЕПАНЕНКОВ Григорий Викторович — студент Санкт-Петербургского государственного университета телекоммуникаций им. проф. М. А. Бонч-Бруевича, stepanenkovgv@mail.com

СТОРОЖУК Максим Николаевич — аспирант кафедры сетей связи и передачи данных Санкт-Петербургского государственного университета телекоммуникаций им. М. А. Бонч-Бруевича, Maxtor@bk.ru

СУМКИН Владимир Радомирович — генеральный директор ООО «НПП «ИТС», sumkinv@mail.ru

ТАГАНДУРДЫЕВ Нурмурад — студент группы ИКТК-66 Санкт-Петербургского государственного университета телекоммуникаций им. проф. М. А. Бонч-Бруевича, nuriktagan@gmail.com

ТАРАНОВ Максим Андреевич — соискатель кафедры военных систем многоканальной электропроводной и оптической связи Военной академии связи им. Маршала Советского Союза С. М. Буденного, taranixm11@gmail.com

ТАРАСОВ Никита Максимович — студент группы ИКБ-72 Санкт-Петербургского государственного университета телекоммуникаций им. проф. М. А. Бонч-Бруевича, nik_tarasov_99@mail.ru

ТАРГОНСКАЯ Алина Игоревна — студентка группы ИКТБ-98М Санкт-Петербургского государственного университета телекоммуникаций им. проф. М. А. Бонч-Бруевича, targonskaya.ai@gmail.com

ТАРЛЫКОВ Алексей Владимирович — начальник научно-образовательного центра «Лаборатория программирования» Санкт-Петербургского государственного университета телекоммуникаций им. проф. М. А. Бонч-Бруевича, atarlykov@gmail.com

ТАТАРЕНКОВ Дмитрий Александрович — старший преподаватель, аспирант кафедры телевидения и метрологии Санкт-Петербургского государственного университета телекоммуникаций им. проф. М. А. Бонч-Бруевича, duferob@gmail.com

ТАШАТОВ Нурлан Нуркенович — кандидат физико-математических наук, доцент кафедры «Вычислительная техника» Евразийского национального университета имени Л. Н. Гумилева, tash.nur@mail.ru

ТВЕРДОХЛЕБОВА Юлия Владимировна — студентка Санкт-Петербургского государственного университета телекоммуникаций им. проф. М. А. Бонч-Бруевича, yulia.tverdohlebova@yandex.ru

ТЕЛЬНОВ Никита Андреевич — студент группы ИКТВ-61 Санкт-Петербургского государственного университета телекоммуникаций им. проф. М. А. Бонч-Бруевича, Nikit.telnov2@yandex.ru

ТЕМЧЕНКО Владислав Игоревич — студент группы ИКТБ-97М Санкт-Петербургского государственного университета телекоммуникаций им. проф. М. А. Бонч-Бруевича, sspman2603@gmail.com

ТЕРЕНТЬЕВ Денис Александрович — студент группы ИКТС-93М Санкт-Петербургского государственного университета телекоммуникаций им. проф. М. А. Бонч-Бруевича, terentyevdenis7@gmail.com

ТЫНЫМБАЕВ Болат Айткожинович — докторант механико-математического факультета Евразийского национального университета Республики Казахстан, tynymbaevba@gmail.com

УЛЬЯНОВ Илья Владимирович — сотрудник Академии Федеральной службы охраны Российской Федерации, ilya@academ.msk.rsnet.ru

УРВАНЦЕВ Георгий Александрович — студент Санкт-Петербургского государственного университета телекоммуникаций им. проф. М. А. Бонч-Бруевича, minehaka@yandex.ru

УШАКОВ Игорь Александрович — старший преподаватель кафедры защищенных систем связи Санкт-Петербургского государственного университета телекоммуникаций им. проф. М. А. Бонч-Бруевича, ushakovia@gmail.com

ФИЛИППОВ Артём Александрович — студент группы ИКТЗ-63 Санкт-Петербургского государственного университета телекоммуникаций им. проф. М. А. Бонч-Бруевича, artm.filippov98@mail.ru

ФИЛИППОВА Татьяна Вячеславовна — студентка группы ИБТС-51 Поволжского государственного университета телекоммуникаций и информатики, filippovatv97@mail.ru

ФОКИН Александр Борисович — сотрудник Академии Федеральной службы охраны Российской Федерации, tatarin57ru@mail.ru

ФОМИН Артем Игоревич — студент группы ИКВТ-61 Санкт-Петербургского государственного университета телекоммуникаций им. проф. М. А. Бонч-Бруевича, artem.fomin633@gmail.com

ФОМЧЕНКО Александра Николаевна — студентка группы ИКТФ-86м Санкт-Петербургского государственного университета телекоммуникаций им. проф. М. А. Бонч-Бруевича, fomc.sasha@gmail.com

ХАКИМОВ Абдукодир Абдукаримович — аспирант кафедры сетей связи и передачи данных Санкт-Петербургского государственного университета телекоммуникаций им. проф. М. А. Бонч-Бруевича, khakimov.a@sdnlab.ru

ХАМЗА Дириех Дарар — магистрант кафедры защищенных систем связи Санкт-Петербургского государственного университета телекоммуникаций им. проф. М. А. Бонч-Бруевича, hamzadirieh1@gmail.com

ХВОРОВА Ирина Олеговна — студентка группы ИКБ-63 Санкт-Петербургского государственного университета телекоммуникаций им. проф. М. А. Бонч-Бруевича, khvorova.irina12@gmail.com

ХИНЕНЗОН Александра Витальевна — студент группы ИКТБ-98М Санкт-Петербургского государственного университета телекоммуникаций им. проф. М. А. Бонч-Бруевича, khinenzon.av@gmail.com

ХОДАНОВИЧ Александр Иванович — доктор педагогических наук, профессор кафедры информационных управляющих систем Санкт-Петербургского государственного университета телекоммуникаций им. проф. М. А. Бонч-Бруевича, akhodanovich@yandex.ru

ЦВЕТКОВ Александр Юрьевич — старший преподаватель кафедры защищенных систем связи Санкт-Петербургского государственного университета телекоммуникаций им. проф. М. А. Бонч-Бруевича, alexander.tsvetkov89@gmail.com

ЧЕЧУЛИН Андрей Алексеевич — кандидат технических наук, ведущий научный сотрудник лаборатории проблем компьютерной безопасности Санкт-Петербургского института информатики и автоматизации Российской академии наук; доцент кафедры защищенные системы связи Санкт-Петербургского государственного университета телекоммуникаций им. проф. М. А. Бонч-Бруевича, chechulin@comsec.spb.ru

ШАРЛАЕВА Мария Владимировна — студентка группы ИКТИ-95м Санкт-Петербургского государственного университета телекоммуникаций им. проф. М. А. Бонч-Бруевича, masha110.97@mail.ru

ШАРОФИДИНОВ Фатхуллоходжа Шукриллоевич — студент группы ИКТК-65 Санкт-Петербургского государственного университета телекоммуникаций им. проф. М. А. Бонч-Бруевича, Fatkhullo0998@gmail.com

ШАШКИН Владислав Сергеевич — аспирант кафедры защищенных систем связи Санкт-Петербургского государственного университета телекоммуникаций им. проф. М. А. Бонч-Бруевича, vlad_shash@mail.ru

ШВЕЦОВ Кирилл Михайлович — магистрант Санкт-Петербургского государственного университета телекоммуникаций им. М. А. Бонч-Бруевича, p_oleg99@mail.ru

ШВИДКИЙ Артем Александрович — начальник научно-образовательного центра «Программно-определяемых систем» Санкт-Петербургского государственного университета телекоммуникаций им. проф. М. А. Бонч-Бруевича, shvidkiy@sut.ru

ШТЕРЕНБЕРГ Станислав Игоревич — кандидат технических наук, ассистент кафедры защищенных систем связи Санкт-Петербургского государственного университета телекоммуникаций им. проф. М. А. Бонч-Бруевича, shterenberg.stanislaw@yandex.ru

ШУРАВИН Андрей Сергеевич — адъюнкт кафедры безопасности инфокоммуникационных систем специального назначения Военной академии связи им. Маршала Советского Союза С. М. Буденного, and.shuravin@ya.ru

ШУСТОВ Никита Игоревич — студент группы ИКТИ-85м Санкт-Петербургского государственного университета телекоммуникаций им. проф. М. А. Бонч-Бруевича, инженер-программист ООО «НТЦ СевенТест», niiiksh@outlook.com

ШУСТОВА Екатерина Валерьевна — начальник отдела разработки средств защиты информации и программного обеспечения ООО «Техцентр», shustova@tc-secur.ru

ЩУКИН Андрей Владимирович — научный сотрудник научно-исследовательского центра Военной академии связи им. Маршала Советского Союза С. М. Будённого, your_friend83@mail.ru

ЭРГАШЕВА Динара Рашидовна — аспирант кафедры информационной безопасности Поволжского государственного университета телекоммуникаций и информатики, dinara.ergasheva95@mail.ru

ЮРКИН Дмитрий Валерьевич — кандидат технических наук, доцент кафедры защищенных систем связи Санкт-Петербургского государственного университета телекоммуникаций им. проф. М. А. Бонч-Бруевича, dvyurkin@yandex.ru

ЮРЧЕНКО Евгения Владимировна — аспирант кафедры общепрофессиональных дисциплин технических специальностей Уральского технического института связи и информатики (филиал) ФГБОУ ВО «Сибирский государственный университет телекоммуникаций и информатики» в г. Екатеринбурге, jena23@mail.ru

ЮРЧЕНКО Михаил Андреевич — студент группы ИКТБ-98М Санкт-Петербургского государственного университета телекоммуникаций им. проф. М. А. Бонч-Бруевича, polsit@yandex.ru

ЯКОВЛЕВ Виктор Алексеевич — доктор технических наук, профессор кафедры защищенных систем связи Санкт-Петербургского государственного университета телекоммуникаций им. проф. М. А. Бонч-Бруевича, viyak@bk.ru

АВТОРСКИЙ УКАЗАТЕЛЬ