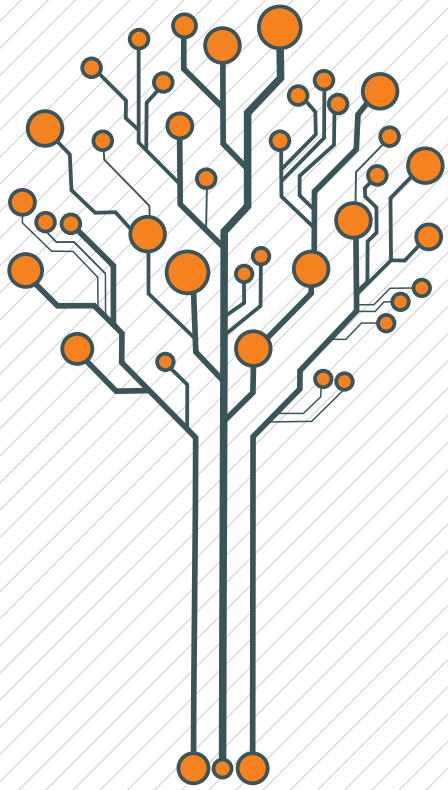
V МЕЖДУНАРОДНАЯ НАУЧНО-ТЕХНИЧЕСКАЯ И НАУЧНО-МЕТОДИЧЕСКАЯ КОНФЕРЕНЦИЯ

АКТУАЛЬНЫЕ ПРОБЛЕМЫ ИНФОТЕЛЕКОММУНИКАЦИЙ В НАУКЕ И ОБРАЗОВАНИИ

АПИНО-2016

СБОРНИК НАУЧНЫХ СТАТЕЙ

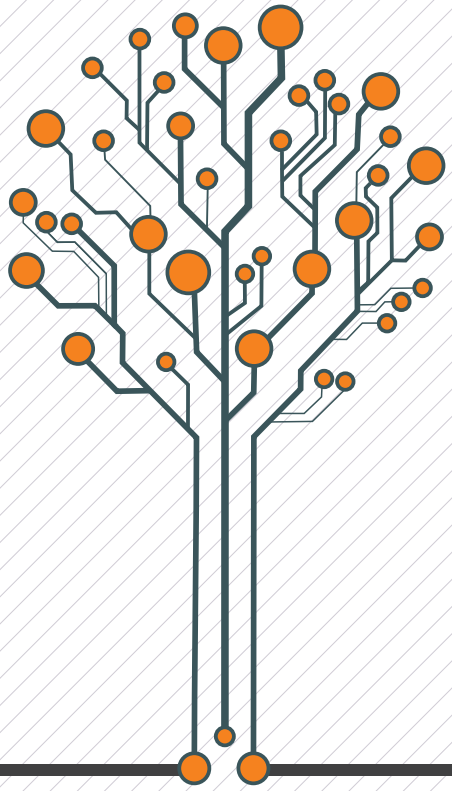


СПбГУТ
10-11.03.2016

COLLECTION OF SCIENTIFIC PAPERS

ICAIT 2016

5th INTERNATIONAL CONFERENCE ON ADVANCED INFOTELECOMMUNICATION



СПбГУТ SPbSUT

АПИНО-2016

СБОРНИК НАУЧНЫХ СТАТЕЙ

ТОМ 1 ▪ VOL. 1

COLLECTION OF SCIENTIFIC PAPERS

ICAIT 2016

С.-ПЕТЕРБУРГ ■ 10-11.03.2016 ■ ST. PETERSBURG

УДК 001:061.3(082)
ББК 74.58
А43

А43 **Актуальные** проблемы инфотелекоммуникаций в науке и образовании. V Международная научно-техническая и научно-методическая конференция: сб. науч. ст. в 3 т.; Т. 1 / под. ред. С. В. Бачевского, сост. А. Г. Владыко, Е. А. Аникевич, Л. М. Минаков. – СПб. : Санкт-Петербургский государственный университет телекоммуникаций им. проф. М. А. Бонч-Бруевича, 2016. – 600 с.

ISBN 978-5-89160-143-7

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.

УДК 001:061.3(082)
ББК 74.58

Научное издание

V Международная научно-техническая и научно-методическая конференция
«Актуальные проблемы инфотелекоммуникаций в науке и образовании»

Сборник научных статей конференции

Том 1

Под редакцией
доктора технических наук, профессора С. В. Бачевского

Составители А. Г. Владыко, Е. А. Аникевич, Л. М. Минаков
Литературное редактирование, корректура Е. А. Аникевич
Оформление Л. М. Минаков
Верстка Е. М. Аникевич

Подписано в печать 01.06.2016. Вышло в свет 30.06.2016.
Формат 60x90 1/8. Усл. печ. л. 37,5 Заказ № 021-ИТТ-2016.
Россия, 193232, Санкт-Петербург, пр. Большевиков, д. 22, корп. 1.

ПРОГРАММНЫЙ КОМИТЕТ

V Международной научно-технической и научно-методической конференции
АКТУАЛЬНЫЕ ПРОБЛЕМЫ ИНФОТЕЛЕКОММУНИКАЦИЙ
В НАУКЕ И ОБРАЗОВАНИИ

Председатель

Бачевский С. В. – доктор технических наук, профессор,
ректор СПбГУТ (Россия)

Заместители председателя

Дукельский К. В. – кандидат технических наук, доцент,
проректор по научной работе СПбГУТ (Россия)

Алексеенко И. А. – кандидат педагогических наук, проректор по воспитательной работе и связям с общественностью СПбГУТ (Россия)

Ответственный секретарь

Владыко А. Г. – кандидат технических наук, member IEEE, СПбГУТ (Россия)

Члены программного комитета

Yevgeni Koucheryavy – professor, Ph. D., Senior member IEEE, Department of Electronics and Communication Engineering Tampere University of Technology (Finland)

Tina Tsou – Liaison rapporteur Huawei Technologies, editor positions in ITU-T, IETF and ETSI, Huawei (China)

Matthias Schnöll – professor, Ph. D., Fachbereich Elektrotechnik, Anhalt University of Applied Sciences (Germany)

Hyeong Ho Lee – Ph. D. in Electrical Engineering, Vice President of IEEK (Institute of Electronics Engineers of Korea), ETRI (Korea)

Edison Pignaton de Freitas – profesor adjunto, Ph. D., Federal University of Rio Grande do Sul (Brasil)

Andrej Kos – professor, Ph. D., University of Ljubljana (Slovenia)

Janusz Pieczerak – M. Sc., Orange Labs (Poland)

Сеилов Ш. Ж. – доктор экономических наук,
президент Казахской Академии Инфокоммуникации (Казахстан)

Воробьев О. В. – кандидат технических наук, профессор,
декан факультета радиотехнологий связи СПбГУТ (Россия)

Бузюков Л. Б. – кандидат технических наук, профессор, декан факультета инфокоммуникационных сетей и систем СПбГУТ (Россия)

Коротин В. Е. – кандидат технических наук, доцент, декан факультета информационных систем и технологий СПбГУТ (Россия)

Колгатин С. Н. – доктор технических наук, профессор,
декан факультета фундаментальной подготовки СПбГУТ (Россия)

Арзуманян Ю. В. – кандидат технических наук, доцент,
декан факультета экономики и управления СПбГУТ (Россия)

Лосев С. А. – кандидат исторических наук, профессор,
декан гуманитарного факультета СПбГУТ (Россия)

Лубянников А. А. – кандидат педагогических наук, доцент,
директор Института военного образования СПбГУТ (Россия)

СОДЕРЖАНИЕ

УДК 621.391

ТАКТИЛЬНЫЙ ИНТЕРНЕТ

А. Е. Кучерявый, А. И. Выборнова

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

В статье рассматривается история развития сетей связи общего пользования и перспективы создания новых сетей на базе технологий Тактильного Интернета, предназначенных для предоставления услуг по передаче тактильных ощущений. Анализируются требования по задержкам и скорости передачи информации для таких сетей, имеющих также название сетей связи со сверхмалыми задержками. Предлагаются подходы к построению таких сетей в условиях одновременного внедрения технологий гетерогенных сверхплотных сетей связи.

тактильный Интернет, сверхмалые задержки, сверхплотные сети, тороидальная сеть.

В последние годы центральное место в развитии сетей связи занимала концепция Интернета Вещей [1, 2]. Данная концепция предполагает, что клиентская база сетей связи создается, в первую очередь, на основе вещей, которые включают в себя физические вещи, в том числе и биомассы, и виртуальные вещи, например, контент. При этом вещью в данной концепции признается любая физическая и виртуальная вещь, имеющая адрес в сети и интерфейс с сетью [3, 4]. Концепция Интернета Вещей существенно изменяет требования к сетям связи. Действительно, очень большое число вещей приводит к необходимости создания самоорганизующихся сетей [5], в сетях появляются новые виды трафика [6, 7, 8], трафик может приобретать антиперсистентные свойства [9], одним из основных методов построения сети становится кластеризация [10, 11, 12]. Однако такая фундаментальная характеристика сети как величина задержки до последнего времени даже в концепции Интернета Вещей оставалась незыблемой.

История развития сетей связи и величина задержки

Выше мы назвали задержку фундаментальной характеристикой сетей связи. Действительно, требования к задержкам в сети связи изменяются даже реже, чем технологии, используемые для построения систем и сетей связи. Преобразование сети связи из аналоговой [13] в цифровую [14] в 90-е годы прошлого века практически не изменило требования к задерж-

ке сигнала «Ответ станции» при снятии абонентом телефонной трубки, которое составляло единицы секунд. Переход от сети с коммутацией каналов к сети с коммутацией пакетов потребовал передачи речи в пакетной форме [15], что привело к существенному изменению требований по задержкам.

Требование о том, чтобы качество передачи речи в сети с коммутацией пакетов было, по крайней мере, не хуже, чем в сети с коммутацией каналов, привело к необходимости нормирования задержки в передаче речи величиной в 100 мс.

Как уже отмечалось выше, в настоящее время основой развития сети в среднесрочной и долгосрочной перспективе является концепция Интернета Вещей. Однако при всех новшествах для сетей связи, привносимых концепцией Интернета Вещей, до последнего времени существенных требований по изменению задержек не выдвигалось. Появление же предложений по услугам Тактильного Интернета как еще одного приложения Интернета Вещей предусматривает для реализации этих услуг наличие требования по величине задержки в 1 мс [15].

Сети со сверхмалыми задержками

Формула для исчисления задержки в сетях связи выглядит следующим образом [16]:

$$T = R \times \tau + \Theta, \quad (1)$$

где R – расстояние, τ – задержка, связанна с физическими ограничениями по передаче информации (5 мкс на километр), Θ – задержка, вносимая техническими средствами сети.

В последние годы появились приложения, которые потребовали меньших задержек, чем задержки при передаче речи. Речь идет, в первую очередь, о приложениях медицинских сетей, где для услуг реального времени требования по задержке определяют ее величину в 10 мс. Такие сети были названы сетями с малыми задержками и их детальное изучение приведено в работе [17]. Важнейшим при этом является даже не то, что потребовались существенно большие скорости на доступе, а то, что в формуле (1) определяющую роль с точки зрения построения сети стало играть первое слагаемое. Это приводит к требованию по децентрализации услуг, которые должны предоставляться на сети связи общего пользования, что в свою очередь должно изменить и структуру построения сети.

Тактильный Интернет предполагает возможность передачи тактильных ощущений человека, что требует задержки в передаче информации по сети величиной в 1 мс. По аналогии с сетями связи с малыми задержками в [17] эти сети назвали сетями со сверхмалыми задержками. В сетях со сверхмалыми задержками происходит дальнейшая децентрализация предоставления услуг. При этом можно считать, что Θ в формуле (1)

за счет требования по использованию сверхскоростных систем на доступе будет стремиться к нулю по сравнению со значением $R \times \tau$.

В [18] предложена архитектура сети со сверхмалыми задержками для реализации услуг Тактильного Интернета. Эта архитектура предполагает децентрализацию облачных вычислений в сетях Тактильного Интернета и проиллюстрирована на рисунках 1 и 2. На рисунке 1 представлена традиционная архитектура сетей Интернета Вещей, где несколько полей устройств Интернета Вещей связаны с облаками, в данном случае индивидуальными для каждого из полей.

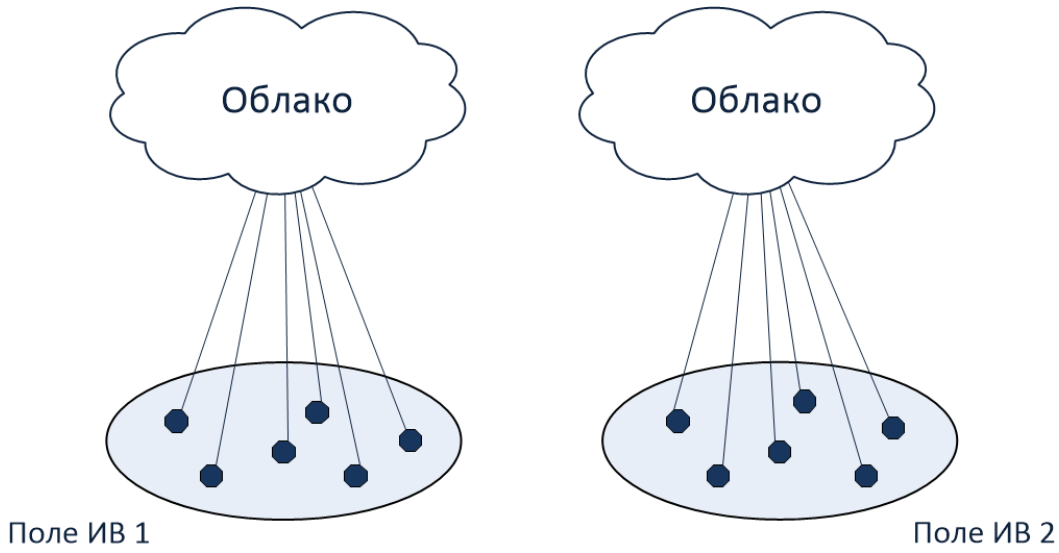


Рис. 1. Традиционная архитектура сетей Интернета Вещей

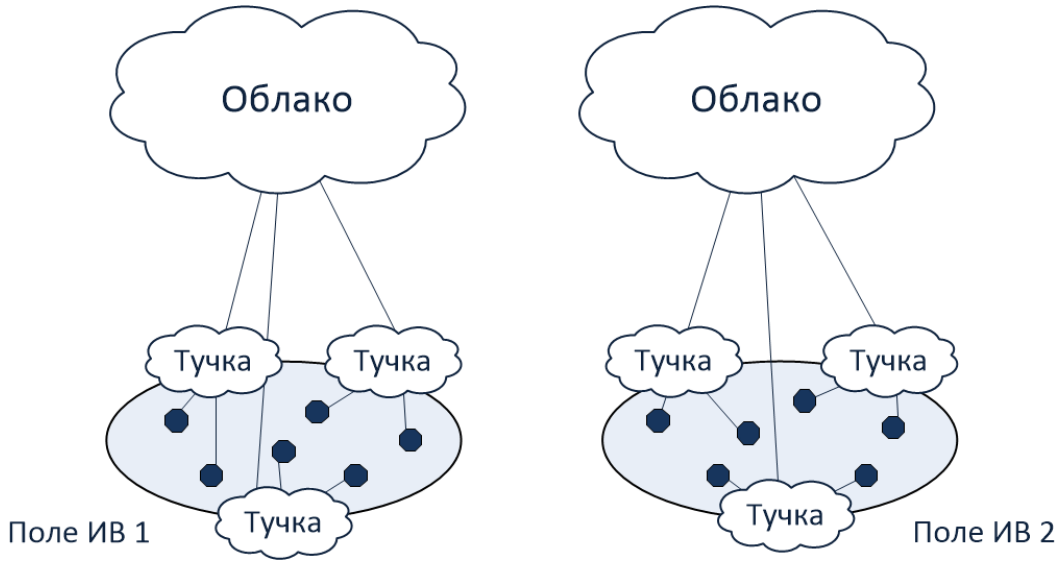


Рис. 2. Децентрализованная архитектура для реализации услуг Тактильного Интернета

В традиционной архитектуре при реализации услуг Тактильного Интернета задержки при передаче информации между интернет вещью и об-

лаком, как правило, будут слишком велики для обеспечения необходимого качества предоставления услуги Тактильного Интернета.

В децентрализованной же архитектуре использование ресурсов распределенных по полям устройств Интернета Вещей «тучек» (*cloudlet*) позволит избежать излишних задержек при оказании услуг Тактильного Интернета, оставляя возможность как централизованного предоставления иных услуг Интернета Вещей, не столь критичных к задержкам, так и возможность поддержки ресурсов «тучек» со стороны основного облака.

Сверхплотные сети и рои

Одновременно с появлением сетей со сверхмалыми задержками происходит процесс создания гетерогенных сетей [19], в которых базовые станции сетей сотовой подвижной связи обслуживают как собственно терминалы пользователей, так и интернет вещи, например, сенсорные узлы. При этом, плотность устройств в такой зоне обслуживания существенно выше, чем в традиционной. Соответственно такие сети получили название сверхплотных гетерогенных сетей.

Для сверхплотных сетей использование существующих методов планирования и расчета, например, показателей качества, вряд ли принесут хорошие результаты. Действительно, эти методы основаны на представлении сети как ячеистой структуры (*mesh*), что вполне приемлемо для сотен узлов в одной зоне. Для сверхплотных же гетерогенных сетей более адекватным представляется использования для целей планирования и расчета методов, применяемых в роевом интеллекте. Даже выбор геометрической структуры роя может оказывать существенное влияние на величину задержки, что критично для услуг Тактильного Интернета. Работы в этом направлении уже начинают появляться. Так в [20] приведены результаты исследований для сетей в форме куба и шара, а в [21] – для цилиндрических сетей. Безусловно, только этими геометрическими фигурами рои устройств в сверхплотных сетях со сверхмалыми задержками не ограничиваются. На рисунке 3 приведена перспективная сверхплотная сеть со сверхмалыми задержками в здании Санкт-Петербургского государственного университета телекоммуникаций им. проф. М. А. Бонч-Бруевича (СПбГУТ), которая в соответствии с формой здания имеет форму тора. Тороидальная сеть еще требует исследования своих параметров, но уже сегодня понятно, что такие сети найдут широкое применение в городских условиях.

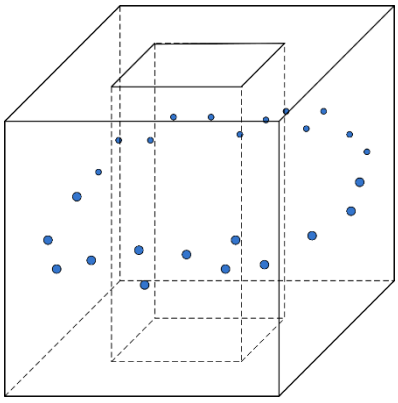


Рис. 3. Тороидальная сеть СПбГУТ в 2020 году

Список используемых источников

1. Кучерявый А. Е., Прокопьев А. В., Кучерявый Е. А. Самоорганизующиеся сети. СПб. : Любавич, 2011. 311 с.

2. Кучерявый А. Е. Интернет Вещей // Электросвязь. 2013. N 1. С. 21–24.

3. Recommendation Y.2060. Overview of Internet of Things. ITU-T, Geneva, 2012. 22 p.

4. Recommendation Y.2069. Terms and Definitions for the Internet of Things. ITU-T, Geneva, 2012. 14 p.

5. Кучерявый А. Е. Самоорганизующиеся сети и новые услуги // Электросвязь. 2009. N 1. С. 19–23.

6. Koucheryavy A., Prokopiev A. Ubiquitous Sensor Networks Traffic Models for Telemetry Applications // 11th NEW2AN, Saint-Petersburg, August 23–25, 2011. Proceedings by Springer, LNCS 6869, 2011. PP. 287–294.

7. Vybornova A., Koucheryavy A. Traffic Analysis in Target Tracking Ubiquitous Sensor Networks // 14th NEW2AN, Saint-Petersburg, August 27–29, 2014. Proceedings by Springer, LNCS 6869, 2014. PP. 389–398.

8. Koucheryavy A. State of Art and Research Challenges for USN Traffic Flow Models // 16th International Conference on Advanced Communication Technology, February 16–19, 2014, Korea. Proceedings of the conference, 2014. PP. 336–340.

9. Paramonov A., Koucheryavy A. M2M Traffic Models and Flow Types in Case of Mass Event Detection // 14th NEW2AN, Saint-Petersburg, August 27–29, 2014. Proceedings by Springer, LNCS 6869, 2014. PP. 294–300.

10. Koucheryavy A., Salim A. Prediction-based Clustering Algorithm for Mobile Wireless Sensor Networks // 12th International Conference on Advanced Communication Technology, February 7–10, 2010, Korea. Proceedings of the conference, 2010. PP. 1209–1215.

11. Abakumov P., Koucheryavy A. The Cluster Head Selection Algorithm in the 3D USN. Proceedings, International Conference on Advanced Communication Technology, 2014. ICACT 2014. Phoenix Park, Korea. PP. 462–466.

12. Кучерявый А. Е., Аль-Кадами Н. А. Адаптивный алгоритм кластеризации для беспроводных сенсорных сетей с мобильными узлами // Электросвязь. 2015. N 3. С. 22–26.

13. Куташов П. Д., Лившиц Б. С., Пошерстник А. Л., Ханин Г. Б. Городские координатные АТС типа АТСК. М. : Связь, 1970. 304 с.

14. Голубев А. Н., Кучерявый А. Е., Миков А. С. Системы коммутации в конце XX – начале XXI века // Проблемы разработки, внедрения и эксплуатации цифровых систем коммутации. Семинар РНТОРЭС, Пермь, 21–23 апреля, 1997. С. 3–5.

15. The Tactile Internet. Technology Watch report. ITU-T, Geneva, 2014. 24 p.

16. Кучерявый А. Е., Маколкина М. А., Киричек Р. В. Тактильный Интернет. Сети связи со сверхмалыми задержками // Электросвязь. 2016. N 1. С. 44–46.

17. Кучерявый А. Е., Парамонов А. И., Аль-Наггар Я. М. Сети связи с малыми задержками // Электросвязь. 2013. N 12. С. 15–19.

18. Maier M., Choudhury M., Riwal B. P., Van D. P. The Tactile Internet: Vision, Recent Progress, and Open Challenges // IEEE Communications Magazine. May 2016. PP. 2–9.

19. Pyttaev A., Johnsson K., Andreev S., Koucheryavy Y. Communications Challenges in High-Density Deploymentsof wearable Wireless Devices // IEEE Wireless Communications. 2015. V. 22, № 1. PP. 12.

20. Dao N., Koucheryavy A., Paramonov A. Analysis of Routes in the Network Based on a Swarrm of UAVS // Lecture Notes in Electrical Engineering. 2016. V. 376. PP. 1261–1271.

21. Vybornova A., Paramonov A., Koucheryavy A. Analysis of the Packet Path Lengths in the Swarms for Flying Ubiquitous Sensor Networks // Distributed Computer and Communication Networks – 2016, Moscow, November 21–25, 2016 (accepted).

УДК 621.372.8.082.5

ТЕНДЕНЦИИ РАЗВИТИЯ КОГЕРЕНТНЫХ СИСТЕМ ДАЛЬНЕЙ СВЯЗИ

А. В. Леонов, О. Е. Наний, В. Н. Трещиков

Компания Т8

В статье рассмотрены основные тенденции развития современных телекоммуникационных DWDM-систем: переход к более сложным форматам модуляции, увеличение символьной скорости, применение суперканалов и гибкого управления спектром (FlexGrid), развитие систем усиления и новых типов оптических волокон. Показано, что существующие технологии теоретически позволяют достичь пропускной способности порядка 100 Тбит/с по одному волокну; дальнейшее увеличение пропускной способности требует задействования новых спектральных диапазонов или пространственного мультиплексирования с применением маломодовых и многосердцевинных волокон.

DWDM, когерентные системы, спектральная эффективность, формат модуляции, символьная скорость, FlexGrid, суперканал, маломодовые волокна, многосердцевинные волокна.

Потребности в скорости передачи информации растут быстрее пропускной способности опорных сетей связи [1, 2]. Единственное отступление от этого правила случилось в «нулевых» годах, когда в связи с появлением коммерческих DWDM-систем с канальной скоростью 40 Гбит/с (~2002 г.) ёмкость магистральных каналов связи на некоторое время превысила потребности пользователей. Однако, уже к 2010 г. ёмкость этих систем была практически исчерпана, и потребовалось очередное обновление оптической инфраструктуры. В 2013–2014 гг. ведущие мировые операторы связи массово внедрили на своих сетях когерентные системы с канальной скоростью 100 Гбит/с, что позволило на какое-то время удовлетворить потребности пользователей [3]. В 2015 г. были представлены коммерческие системы со скоростью 200 Гбит/с по длине волны, в 2017 г. ожидается коммерческая доступность систем со скоростью 400 Гбит/с по длине волны. Дальнейшее увеличение скорости по одной длине волны возможно, но ведёт к радикальному снижению дальности передачи; возможности увеличения количества каналов в существующих системах также практически исчерпаны. При этом каких-либо пределов постоянному росту по-

требностей в передаче трафика пока не наблюдается. Поэтому для продолжения устойчивого развития оптических систем дальней связи жизненно необходим поиск новых физических идей и принципов, с использованием которых будут созданы прорывные технологии следующего поколения.

По существующим оценкам, канал 400 Гбит/с может быть передан в полосе 50 ГГц (спектральная эффективность 8 бит/с/Гц), что теоретически позволит достичь ёмкости 100 Тбит/с в одном волокне в C+L-диапазоне (270 каналов). Однако дальнейшее увеличение ёмкости DWDM-систем по существующей оптической инфраструктуре затруднительно, что мотивирует исследование новых типов усилителей, которые позволят расширить рабочий спектральный диапазон, и новых типов оптических волокон с возможностью одновременной передачи информации по нескольким сердцевинам или модам. Соответственно, можно выделить три основных направления, по которым идёт развитие современных систем дальней связи: 1) совершенствование когерентных систем связи, 2) совершенствование систем усиления, и 3) разработка новых типов оптических волокон.

Совершенствование когерентных систем связи

Когерентные системы связи позволяют использовать все степени свободы электромагнитного поля: амплитуду, фазу и поляризацию (рис. 1).

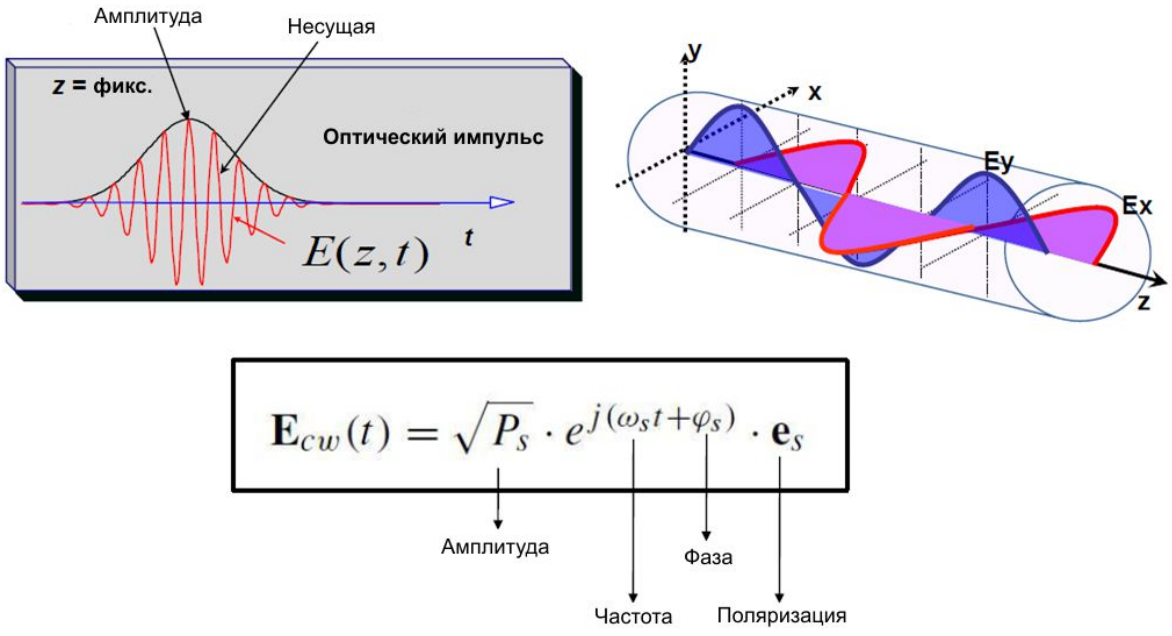


Рис. 1. Параметры светового сигнала, которые могут быть использованы для модуляции и мультиплексирования. В современных системах связи для модуляции используются амплитуда и фаза, а частота и поляризация используются для мультиплексирования

Повышение скорости передачи информации возможно за счет использования большего количества возможных состояний амплитуды и фа-

зы [4], (рис. 2). Например, в системах со скоростью 100 Гбит/с использует формат DP-QPSK (т. е. QPSK в каждой из двух поляризаций), при этом каждый символ QPSK несёт 2 бита информации. В системах со скоростью 200 Гбит/с и 400 Гбит/с по одной длине волны используются форматы DP-16QAM (4 бита в каждой из 2 поляризаций) и DP-64QAM (6 бит в каждой из 2 поляризаций).

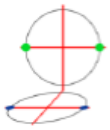
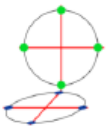
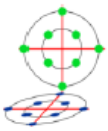
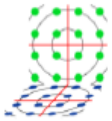
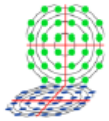
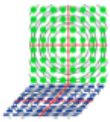
Формат модуляции	DP-DPSK	DP-QPSK	DP-8QAM	DP-16QAM	DP-32QAM	DP-64QAM
бит/символ	2x1	2x2	2x3	2x4	2x5	2x6
Сигнальное созвездие						
Штраф по OSNR, дБ	0	0	2	4	6	8,5

Рис. 2. Символьная эффективность различных форматов модуляции

Однако повышение символьной эффективности (количество бит на 1 символ) ведёт к существенному снижению дальности передачи сигнала [5, 6]. Тем не менее, исследования все более сложных форматов интенсивно проводятся многими компаниями. Сообщается о ведущихся экспериментах с форматами 128QAM и даже 256QAM. Такие форматы дают заметный выигрыш в скорости передачи информации для коротких линий при фиксированной полосе. Можно прогнозировать внедрение систем 200G и 400G в городских сетях с использованием форматов DP-16QAM уже в ближайшее время.

Помимо перехода к более сложным форматам модуляции, для повышения спектральной эффективности (и соответственно ёмкости) в современных системах связи широко применяются методы спектральной инженерии: уплотнение каналов за счет придания им прямоугольного спектра модуляции (Найквист-WDM). Это позволяет до 1,5 раз повысить спектральную эффективность (например, за счет передачи канала 100 Гбит/с в полосе не 50 ГГц, а 33 ГГц), однако за счет некоторого снижения дальности передачи.

Увеличение ёмкости – т. е. суммарной скорости передачи информации – основное, но не единственное направление развития когерентных систем. Активно ведутся исследования по повышению экономичности таких систем, развитию их функциональности и увеличению удобства эксплуатации.

В частности, значительные усилия направлены на увеличение символьной скорости DWDM-систем. Чем больше символьная скорость, тем меньшее число компонентов используется в транспондерах и, следовательно, реализуется потенциально более экономичное решение. Кроме то-

го, увеличение битовой скорости необходимо для дальнейшего увеличения канальной скорости, что является требованием потребителей. К настоящему времени, скорость клиентских интерфейсов впервые сравнялась с канальной скоростью транспортных сетей, а вскоре вероятно превысит её (рис. 3). Это требует от производителей повышения канальной скорости, чего сложно достичь одним лишь усложнением формата модуляции (т. к. при этом существенно падает дальность). В современных и перспективных системах, для повышения канальной скорости используется одновременно увеличение символьной скорости и переход к более сложной модуляции.

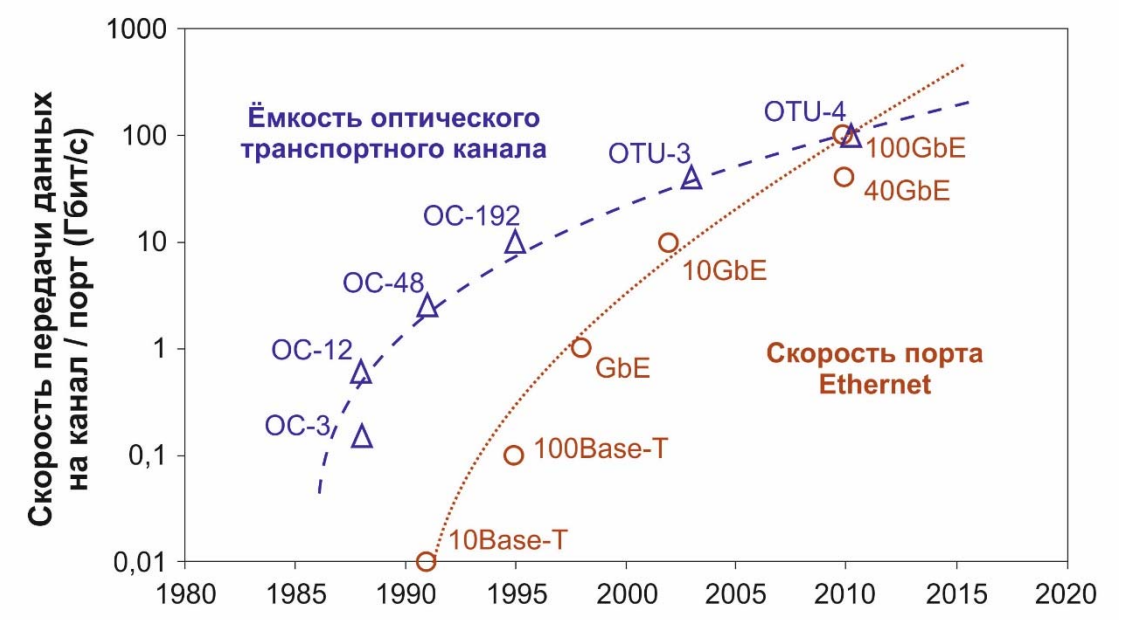


Рис. 3. Рост канальной скорости, регламентируемой стандартами транспортных систем связи, и рост скорости Ethernet-портов [7]

В современных транспондерах используются скорости 30–45 Гбод, следующим шагом может стать 60 Гбод [8]. Этот шаг позволит достигнуть скорости передачи информации 400 Гбит/с с использованием одной несущей в полосе 100 ГГц (например, при использовании формата DP-16QAM и символьной скорости 60 Гбод). Основное препятствие на пути повышения символьной скорости – ограниченное быстродействие электроники. Его можно преодолеть, используя оптические технологии, в частности, технологию «спектрального склеивания» [9] или оптического временного мультиплексирования (технология OTDM) [10, 11]. С использованием технологии OTDM достигнуты символьные скорости, значительно превышающие 100 Гбод, которые пока не доступны при использовании электронных методов. Однако по своим экономическим характеристикам такие оптические методы пока что проигрывают электронным технологиям.

Активно развивается использование суперканалов (рис. 4). При этом для передачи высокоскоростного клиентского потока данных (например, перспективных форматов 400 *Gigabit Ethernet* или 1 *Terabit Ethernet*) используется несколько оптических длин волн (поднесущих) [12, 13, 14]. При передаче по опорной сети связи, эта группа поднесущих на оптическом уровне управляется как единое целое – суперканал. Использование суперканалов позволяет предоставить клиенту любую необходимую скорость на клиентском интерфейсе.

а) б)

Рис. 4. Спектры суперканалов: а) 300 Гбит/с (3x100G в общей полосе 100 ГГц); б) 1 Тбит/с (10x100G, по 33 ГГц на канал – составлен из 4 суперканалов 300G, две крайние поднесущие не используются). ООО «Т8»

Важным направлением развития является гибкое использование доступного спектра (*FlexGrid*) за счёт управления оптическими поднесущими. В технологии Flexgrid рабочий спектр делится на узкие спектральные полосы – слоты (обычно 12,5 ГГц), расположенные вплотную друг к другу. Эти слоты могут объединяться для формирования спектральных блоков нужного размера [15, 16]. Таким образом, шириной спектральной полосы, занимаемой каналом, можно управлять в зависимости от требуемой скорости передачи (например, в зависимости от времени суток). Возможность применения технологии Flexgrid в коммерческих системах появилась только после создания и начала массового производства перестраиваемых спектрально селективных переключателей WSS (*Wavelength Selective Switch*), использующих технологию LCoS (*Liquid Crystal on Silicon*) [17].

Для снижения размеров и энергопотребления приёмо-передающей аппаратуры всё шире применяются фотонные интегральные схемы. При этом на одном фотонном интегральном устройстве (PLC) могут объединяться различные компоненты: делители пучков (*beam splitters*), решетки (*gratings*), соединители (*couplers*), поляризаторы (*polarizers*), интерферометры (*interferometers*), источники излучения, усилители и детекторы. Создание компактных фотонных устройств позволяет снизить себестоимость производимой продукции и энергетические затраты [18, 19, 20].

Наивысший уровень интеграции достигается при монолитной интеграции, когда все оптические элементы, включая источники света, устройства управления светом, детекторы и электронные компоненты расположены на одной подложке. Наиболее перспективными материалами для монолитной интеграции являются полупроводниковые материалы, в частности, для диапазона 1550 нм – кремний (*Si*) и фосфат индия (*InP*).

Активно развиваются методы цифровой обработки сигналов в когерентных системах связи (DSP, *Digital Signal Processing*). В частности, в коммерческих приемниках когерентных систем связи реализованы электронные методы компенсации хроматической дисперсии и поляризационной модовой дисперсии, ведётся их адаптация для высоких символьных скоростей и многоуровневых форматов модуляции, а также разработка методов компенсации нелинейных искажений [21, 22] и развитие алгоритмов коррекции ошибок (*Forward Error Correction*, FEC) [23, 24].

Совершенствование систем усиления

Для снижения уровня шума и, соответственно, повышения качества передаваемого сигнала, желательно обеспечить такой режим распространения сигнала по линии связи, когда мощность сигнала вдоль линии изменяется минимально. Простой путь решения этой задачи – расположение усилителей на все меньшем расстоянии друг от друга – неприемлем по экономическим соображениям. Поэтому широким фронтом ведутся исследования эффективности использования распределенных рамановских усилителей [25]. Применение распределенных усилителей и усилителей с удаленной накачкой позволяет существенно увеличить дальность работы однопролетных и многопролетных ВОЛС [26, 27, 28, 29, 30].

Иногда возникают задачи передать информацию на расстояние 300–400 км без использования промежуточных усилителей, т. е. по однопролетной линии. Для решения таких задач применяются одновременно рамановские усилители и оптические усилители с удалённой накачкой. Например, в России компанией «Т8» создан комплект оборудования, обеспечивающий дальность передачи по однопролетной линии протяжённостью более 500 км с суммарной скоростью 1 Тбит/с [27].

Важным направлением развития систем усиления является расширение их спектрального диапазона, что позволит передавать в DWDM-системе больше каналов. Современные DWDM-сети дальней связи используют почти исключительно С-диапазон оптического волокна в окрестности длины волны 1,55 микрометра. Ширина *С*-диапазона – примерно 35 нм, или 4,4 ТГц. В то же время, спектральная область, которая потенциально могла бы быть использована для передачи информации в волокне (с оптическими потерями, не превышающими 0,4 дБ/км), простирается от 1300 нм до 1700 нм (рис. 5).

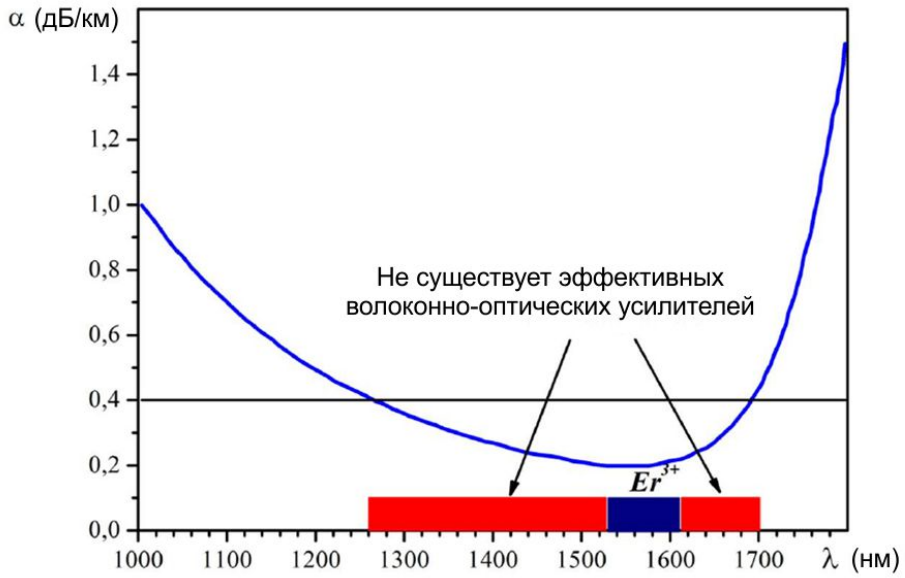


Рис. 5. Спектральные диапазоны систем связи – используемый (*C*-диапазон) и потенциально возможные для использования

Использование незадействованных в настоящее время спектральных диапазонов может значительно увеличить пропускную способность ВОЛС. Практически готова к использованию в коммерческих системах связи еще одна спектральная полоса – *L*-диапазон (1565–1625 нм). В *L*-диапазоне ширина спектра составляет 60 нм, или примерно 7 ТГц. Для спектральных областей 1300–1520 нм и 1610–1700 нм в настоящее время отсутствуют эффективные волоконные оптические усилители. Поэтому работы по созданию эффективных усилителей для спектральных областей 1300–1520 нм и 1610–1700 нм являются исключительно актуальными. В частности, существенно расширить рабочий диапазон спектра могут усилители на основе волокон, легированных висмутом [31, 32] (рис. 6).

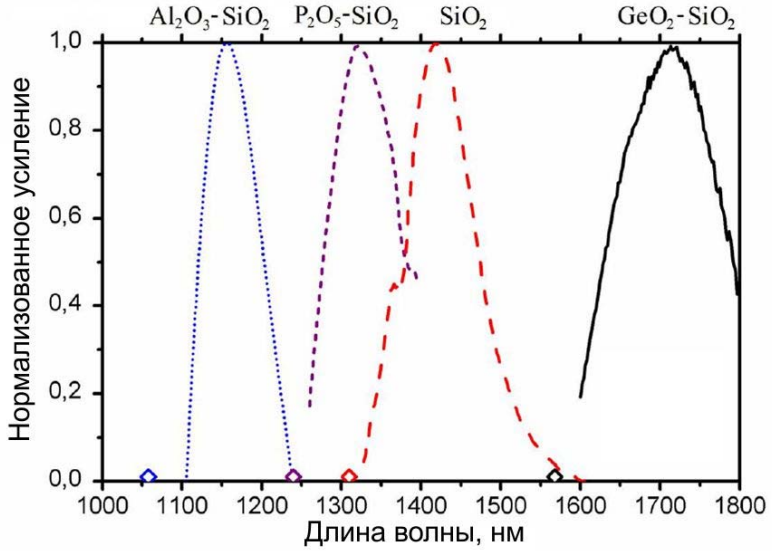


Рис. 6. Спектры усиления висмутовых волокон разного состава [31]

Разработка новых типов волокон

Эксплуатационный период кабельной инфраструктуры оценивается обычно в 20–30 лет, за это время на сети успевает смениться несколько поколений активного оборудования. Однако сегодня как никогда высока актуальность исследований в области создания новой инфраструктуры волоконно-оптических сетей связи, поскольку существующая инфраструктура близка к исчерпанию своей пропускной способности. В России исследования в этом направлении ведутся, в частности, в НЦВО РАН.

Кардинально увеличить пропускную способность волокна позволяют методы пространственного мультиплексирования, которые реализуются с использованием многосердцевинных и маломодовых волокон [33, 34, 35].

Поскольку у одномодовых волокон диаметр сердцевины менее 10 мкм, то даже в оболочке стандартного размера с диаметром 125 мкм можно расположить несколько сердцевин (рис. 7). При этом по каждой сердцевине можно передавать независимые потоки информации, как по отдельным одномодовым волокнам.

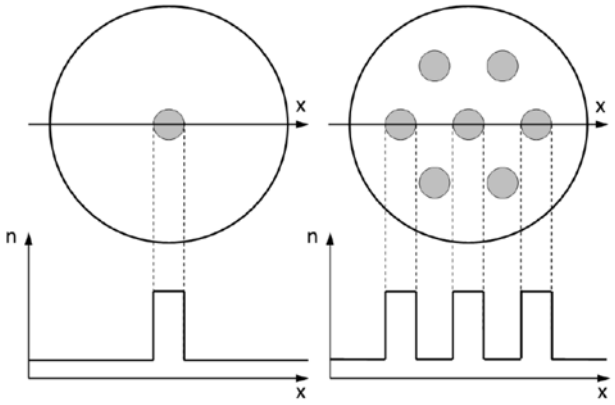


Рис. 7. Поперечные сечения (вверху) и профили показателя преломления вдоль оси *x* (внизу) одномодового волокна (слева) и многосердцевинного волокна (справа) [36]

Разработку многосердцевинных волокон активно ведут мировые лидеры по производству телекоммуникационного волокна и оборудования для оптических систем связи (OFS, *Corning, Alcatel-Lucent*, NTT, NEC, *Fujikura, Sumitomo* и др.), а также связанные с ними исследовательские лаборатории и центры. Продемонстрирована передача информации в таких волокнах со скоростями 1–2 Петабит/с на расстояние в несколько десятков километров. Однако для увеличения дальности передачи необходимо решить ряд технологических проблем, в первую очередь, создать усилители для многосердцевинных волокон.

Второй технологией, реализующей идею пространственного мультиплексирования, является технология маломодовых волокон. Сердцевина маломодового волокна поддерживает распространение нескольких про-

странственных мод (обычно 3–7), по каждой из которых может быть передан независимый поток информации (рис. 8).

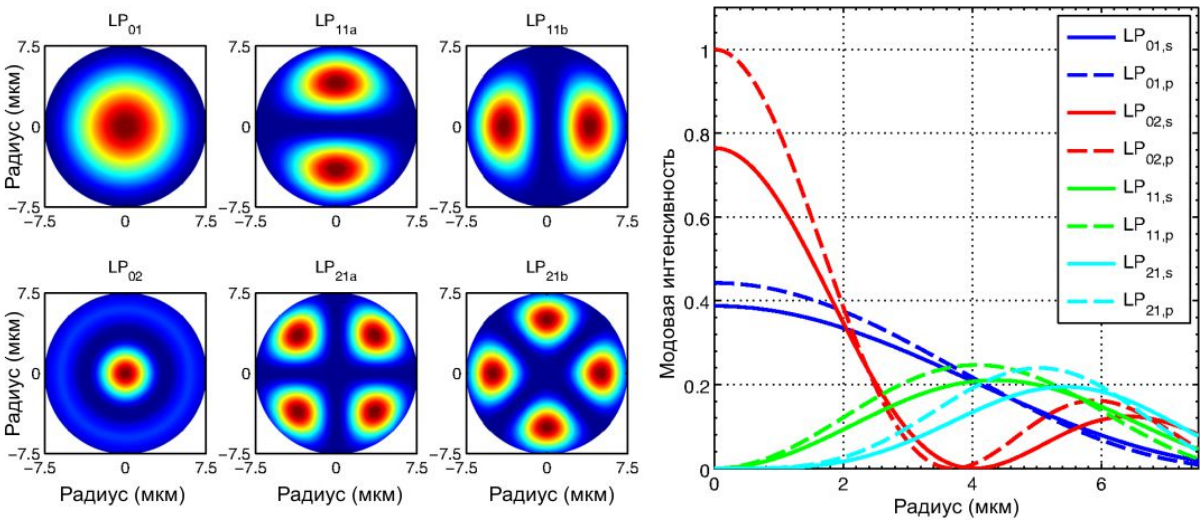


Рис. 8. Пространственные распределения нескольких поперечных мод в маломодовом волокне [37]

Объединение двух описанных подходов позволяет создать многосердцевинные многомодовые волокна. Например, недавно было продемонстрировано волокно [38], которое содержит 36 сердцевин, каждая из которых поддерживает распространение 3 пространственных мод. В таком волокне можно одновременно передавать 108 пространственно мультиплексированных информационных каналов.

Ведутся разработки и других новых типов волокон. В кварцевых волокнах достигнутые значения затухания близки к теоретическому пределу (примерно 0,14 дБ/км). Дальнейшее совершенствование кварцевых волокон направлено на увеличение площади сердцевины (и соответственно площади моды) с целью ослабления нелинейных эффектов и увеличения допустимой мощности, вводимой в волокно. Теоретически, затухание существенно меньшее, чем в кварцевых волокнах, можно получить в волокнах с полой сердцевиной. Разработку таких волокон ведут OFS, Corning и др. Однако, достигнутые в таких волокнах на практике затухания пока существенно больше, чем у стандартного волокна G.652. Тем не менее, уже сейчас такие волокна находят ограниченное применение в системах связи, где требуется достижение минимальной физической задержки сигнала (например, дата-центры бирж, суперкомпьютеры).

Заключение

При сохранении существующих темпов роста трафика, все возможности увеличения пропускной способности за счет существующего технологического задела будут исчерпаны примерно к 2020 г. Очевидна необхо-

димость разработки новых технологий и подходов, которые позволят обеспечить дальнейший рост пропускной способности опорных волоконно-оптических сетей связи. Приоритетными направлениями развития магистральных систем связи в перспективе, по-видимому, станут: расширение используемого спектрального диапазона, развитие многомодовых и многосердцевинных волокон и соответствующих оптических усилителей, а также интеграция фотоники и электроники для повышения компактности и энергоэффективности оборудования.

Список используемых источников

1. O'Mahony M. Future optical networks // In Optical Fiber Telecommunications V B: Systems and Networks. Elsevier Inc. 2008. PP. 611–640.

2. Tkach R. W. Scaling Optical Communications for the Next Decade and Beyond // Bell Labs Technical Journal, 2010, vol. 14, no. 4. PP. 3–9.

3. Гуркин Н. В., Наний О. Е., Трещиков В. Н., Убайдуллаев Р. Р. Производительность когерентных DWDM-систем с канальной скоростью 100 Гбит/с // Вестник связи. 2013. № 2. С. 39–40.

4. Nakazawa M., Hirooka T., Yoshida M., Kasai K. Extremely Higher-Order Modulation Formats // In Optical Fiber Telecommunications VI B: Systems and Networks. Elsevier Inc. 2013. PP. 297–336.

5. Конышев В. А., Леонов А. В., Наний О. Е., Трещиков В. Н., Убайдуллаев Р. Р. Рекордная производительность систем 100G как маркер перехода к эволюционному развитию ВОСП // Первая миля. 2015. № 6. С. 40–43.

6. Леонов А. В., Слепцов М. А., Трещиков В. Н. Развитие скоростных DWDM-систем по нескольким поднесущим // Первая Миля. 2016. № 2. С. 42–49.

7. Xia T. J., and Wellbrock G. A. Commercial 100-Gbit/s Coherent Transmission Systems // Optical Fiber Telecommunications VI B: Systems and Networks. I. P. Kaminow, T. Li, and A. E. Willner (editors). Academic (2013).

8. Raibon G. et al. High Symbol Rate Coherent Optical Transmission Systems: 80 and 107 Gbaud // J. Lightwave Technol. 2014. V. 32, no. 4. PP. 824–826.

9. Guan B. Bandwidth scalable and high fidelity spectrally-sliced transmitter / B. Guan et. al. // OFC. 2015. Paper M2G.2.

10. Weber H.-G., Ludwig R. Ultra-high-speed OTDM transmission technology // In Optical Fiber Telecommunications V B: Systems and Networks. Elsevier Inc. 2008. PP. 201–232.

11. Kawanishi S., Takara H., Uchiyama K. et al. Single Polarization Completely Time-Division-Multiplexed 100 Gbit/s Optical Transmission Experiment // In Proc. ECOC'93. N 3, 1993. PP. 53–56.

12. Chandrasekhar S., Liu X. Advances in Tb/s superchanal // In Optical Fiber Telecommunications VI B: Systems and Networks. Elsevier Inc. 2013. PP. 83–120.

13. Новиков А. Г., Трещиков В. Н., Плаксин С. О., Плоцкий А. Ю., Наний О. Е. Перспективные DWDM системы связи со скоростью 20 Тбит/с на соединение // Фотон-экспресс. 2012. № 3 (99). С. 34–38.

14. Leuthold J., Freude W. Optical OFDM and Nyquist multiplexing // In Optical Fiber Telecommunications VI B: Systems and Networks. Elsevier Inc. 2013. PP. 381–431.

15. Wright P., Lord A., Velasco L.. The Network Capacity Benefits of Flexgrid. ONDM, paper http://personals.ac.upc.edu/lvelasco/docs/research/2013-ONDM-2.pdf.

16. Gerstel O., Jinno M., Lord A., Ben Yoo S. Elastic Optical Networking: A New Dawn for the Optical Layer? // IEEE Commun Mag. 2012, vol. 50. PP. s12–s20.

17. Steve Frisken, Glenn Baxter, Dmitri Abakoumov, Hao Zhou, Ian Clarke, Simon Poole. Flexible and Grid-less Wavelength Selective Switch using LCOS Technology // In Proceedings of OFC/NFOEC 2011, OTuM3.

18. Doerr C. R., Okamoto K., Doerr C. R. Planar Lightwave Circuits in Fiber-Optic Communications // In Optical Fiber Telecommunications V A: Systems and Networks. Elsevier Inc. 2008. PP. 269–342.

19. Nagarajan R. Semiconductor Photonic Integrated Circuit Transmitters and Receivers / R. Nagarajan et al. // In Optical Fiber Telecommunications VI A: Systems and Networks. Elsevier Inc. 2013. PP. 62–147.

20. Bamiedakis N. Integrated and Hybrid Photonics for High-Performance Interconnects / N. Bamiedakis et al. // In Optical Fiber Telecommunications VI A: Systems and Networks. Elsevier Inc. 2013. PP. 458–504.

21. Bayvel P., Behrens C., Millar D. S. Digital Signal Processing (DSP) and Its Application in Optical Communication Systems // In Optical Fiber Telecommunications VI B: Systems and Networks. Elsevier Inc. 2013. PP. 221–288.

22. Ip E. Nonlinear compensation using backpropagation for polarization-multiplexed transmission // J Lightwave Technol. 2010, 28 (March). PP. 939–951.

23. Smith B. P. and Kschischang F. R. Future prospects for FEC in fiberoptic communications // IEEE J. Sel. Topics. Quantum Electron., Oct. 2010. Vol. 16, no. 5. PP. 1245–1257.

24. Schmalen L., de Lind van Wijngaarden A. J., and ten Brink S. Forward error correction in optical core and optical access networks // Bell Labs Tech. J. Mar. 2013. Vol. 18, no. 3. PP. 39–66.

25. Леонов А. В., Наний О. Е., Трещиков В. Н. Усилители на основе вынужденного комбинационного рассеяния в оптических системах связи // Прикладная фотоника. 2014. Т. 1, № 1. С. 26–49.

26. Gainov V., Gurkin N., Lukinih S., Akopov S., Makovejs S., Ten S., Nanii O. and Treshchikov V. Record 500 km unrepeatered 100 Gb s–1 transmission // Laser Phys. Lett. 10, 075107, 2013.

27. Gainov V., Gurkin N. V., Lukinih S. N., Makovejs S., Akopov S. G., Ten S. Y., Nanii O. E., Treshchikov V. and Sleptsov M. Record 500 km unrepeatered 1 Tbit/s (10x100G) transmission over an ultra-low loss fiber // Optics Express. 2014. N 22. PP. 22308–22313.

28. Gainov V., Gurkin N., Lukinih S., Shikhaliev I. I., Skvortsov P. I., Makovejs S., Akopov S., Ten S., Nanii O. and Treshchikov V. 500 km unrepeatered 200 Gbit·s−1 transmission over a G.652-compliant ultra-low loss fiber only // Laser Phys. Lett. 12, 066201(1)–(6), 2015.

29. Гайнов В. В., Конышев В. А., Леонов А. В., Лукиных С. Н., Наний О. Е., Скворцов П. И., Трещиков В. Н., Шихалиев И. И., Убайдуллаев Р. Р. Однопролётные оптические линии связи большой протяжённости // Прикладная фотоника. 2015. № 1. С. 5–22.

30. Гайнов В. В., Слепцов М. Н., Трещиков В. Н. Однопролётные ВОЛС большой протяжённости: как снизить стоимость транспортных сетей // Первая миля. 2015. № 2. С. 72–77.

31. Дианов Е. М., Фирстов С. В., Хопин В. Ф., Гурьянов А. Н., Буфетов И. А. Висмутовые волоконные лазеры и усилители, работающие в области 1,3 мкм // Квантовая электроника. 2008. Т. 38, № 7. С. 615–617.

32. Dvoyrin V. V., Medvedkov O. I., Mashinsky V. M., Umnikov A. A., Guryanov A. N., Dianov E. M. Optical amplification in 1430–1495 nm range and laser action in Bi-doped fibers // Opt Express. 2008, Vol. 16. No 21. PP. 16971.

33. Awaji Y. Transmission systems using multicor fibers / Y. Awaji et al. // In Optical Fiber Telecommunications VI B: Systems and Networks. Elsevier Inc. 2013. PP. 617–651.

34. Дианов Е. М., Семёнов С. Л., Буфетов И. А. Новое поколение волоконных световодов // Квантовая электроника. 2016. Т. 46, № 1. С. 1–10.

35. Sakaguchi J. et al. Realizing a 36-core, 3-mode fiber with 108 spatial channels // Proc. OFC, Th5C2, Los Angeles (2015).

36. Inao S., Sato T., Sentsui S., Kuroha T., and Nishimura Y. Multicore optical fiber // In Optical Fiber Communication, 1979 OSA Technical Digest Series (Optical Society of America, 1979), paper WB1. doi:10.1364/OFC.1979.WB1.

37. Herbster A. F., and Romero M. A. Few-mode erbium-doped fiber amplifier design method based on the signal-pump overlap integral // Optical Engineering. 2014, v. 53, No. 9, PP. 096101. doi:10.1117/1.OE.53.9.096101.

38. Igarashi K. et al 114 space-division-multiplexed transmission over 9,8-km weakly-coupled-6-mode uncoupled-19-core fibers // Proc. OFC, Th5C2, Los Angeles (2015).

UDC 004.896:621.865

TWO-COMPONENT MULTI-AGENT ROBOTIC SYSTEMS ELEMENTS INTERACTION MODEL SCENARIOS

W. Guilin[1], J. Lu[1], E. Borisov[2]

[1]Hunan University, China
[2]The Bonch-Bruevich Saint-Petersburg State University of Telecommunications

The article discusses the option of making a multi-agent robotic system able to function in different physical environments.

multi-agent systems, mobile robots, spherical robots, group interaction.

Recently, the problems of multi-agent robotic systems (MRS) are attracting serious attention. On the one hand this is caused by a purely pragmatic approach that proceeds from the several advantages of application of these systems, and on the other hand, the development of mechatronic systems, computing, machine vision systems, data transmission, communication and navigation allowing to create robots of different functionalities and for various purposes. Main trends in the development of multi-agent robotic, artificial intelligence and management systems are reflected in the works [1, 2, 3, 4, 5], and this list is far from complete. The enormous potential of MRS open up broad prospects for their use in various applications.

The formation of the list of such demands, development of methods, models and algorithms for group activities control, planning of behavior, task distri-

bution, processing and summarizing of heterogeneous sensory and command information is highly interesting for creation of advanced models of intelligent autonomous robots as well as multi-agent systems, organized on their basis.

Thus, in particular, the specificity of the problems of group control of autonomous robots in the composition of the MRC can be characterized by the following main factors: the exchange of information between robots in the vast majority of cases should be carried out through wireless communication channels; he size and composition of robots formation can reach tens or even hundreds of stand-alone units of various types and may change during the operation; the variation of parameters of spatial position, current status of the members of the formation can vary in a wide range of distances and speeds.

The use of MPC allows to increase the reliability of execution of a given goal or to resolve a particular range of tasks with loss of one or several robots at the expense of redistribution of functions among the remaining. One of the reasons for the development of MRS is the ability to replace complex and expensive robots by group (groups) of more simple and cheap devices. The use of MRS has a wide range of applications, shown in figure 1. The fundamental difference between MRS and other systems is the wide variability of strategies (control) for achieving the goal (s) as particular for a specific robot, as well as for a group of devices.

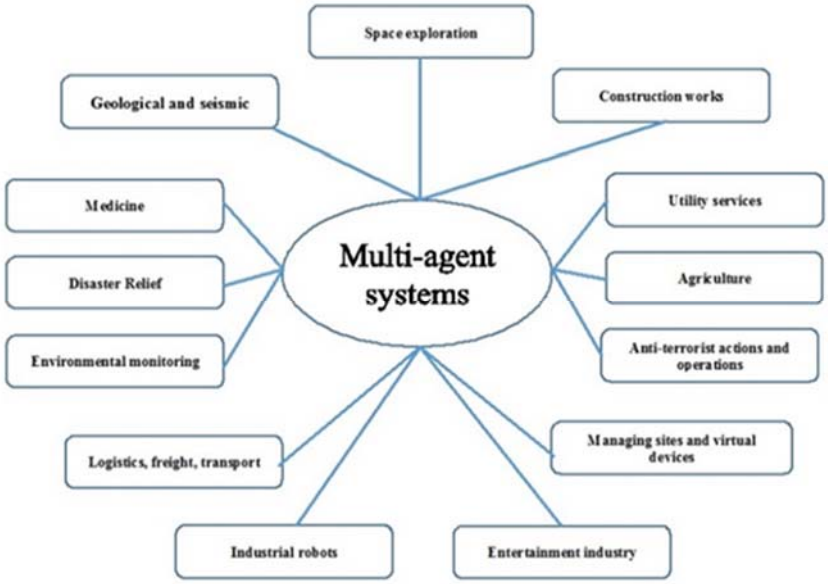


Figure 1. The list of typical tasks that could be solved by MRS

There are the following basic strategies of robots group behavior: centralized, combined, and decentralized ("schooling" or "swarm") [1, 2, 3, 4, 5]. The strategy of centralized control implies the concentration of all resources in a single access point, ensuring planning and coordination of robots in a team to solve problems. Centralized control strategies give good results for small

number of robots in the group. With increase of the size of the group, the load on communication channel and computing means of the control device grows.

The strategy of decentralized control involves collective actions (with the direct exchange of information between all robots). It provides for communication systems and data transmission channels between all robots of the group for the coordination and correction of their actions and mutual exchange of information about the current state of the environment.

Schooling control strategies of robots group behavior occupy a special place among others. Providing group interaction by this control strategy is limited to setting common application tasks, followed by adjusting its phases to the individual performers. Obviously, the robots in this control strategy must have certain intellectual and functional capabilities for decision-making for achieving the given task goal. At this, the structures of robots interaction should focus on a single control center for some of their constituent parts (robots). Such structures of group control can be based not only in accordance with the centralized, decentralized, but also with the combined structure formed hierarchically.

The main advantage of the schooling control strategies is their scalability. With increasing of the robots group size, the computational complexity of control tasks does not grow, which allows using of schooling strategies for managing very large groups of robots.

Multi-agent system of the spherical robots with increased maneuverability formed as a group must implement the following functions: environmental monitoring of hazardous facilities (nuclear, chemical and biological industry); patrolling of airports, industrial sites, exhibition halls, pavilions, etc.; searching for objects of interest, identifying them, monitoring, collecting information about them; monitoring the hygiene-epidemiological situation in the hotbeds of mass infections.

Developing of multi-agent robotic system asks for solving a number of technical, scientific and applied tasks, including design of a spherical robot, the interaction of these robots as a multi-agent system, finding solutions for traffic control in difficult conditions, communication and coordinate-time support, equipping with the necessary and sufficient number of monitoring sensors.

System in its basic configuration contains three robots and has the ability to increase the size of the group and to include the air-based means into it. The system is designed to accommodate complex equipment for maintenance of local environmental monitoring. The robots are adapted to work mainly in the prepared environment (e. g., manufacturing facilities). However, individual tasks of group system control in a non-determined nonstationary environment are also practiced. In general, the system uses the integrated (combined) group control algorithm, which applies to the principles of decentralized collective management and hierarchical variants of the control schemes, depending on the environmental conditions and the character of the task.

Spherical robots chassis with pendulum drive [6, 7, 8] are equipped with video surveillance equipment and instruments to analyze ambient air (gas analyzers). The chassis are standardized in terms of execution of motion and control systems, but differ by the set of on-board analyzers. This approach increases the durability and extends the functionality of the group, but makes it technically heterogeneous, which complicates control.

Because of the need to ensure the robot maximum positioning accuracy in combination with maximum smoothness of motion, a pendulum was chosen as a drive mechanism (figure 2). Motion control is accomplished by deflection of the pendulum.

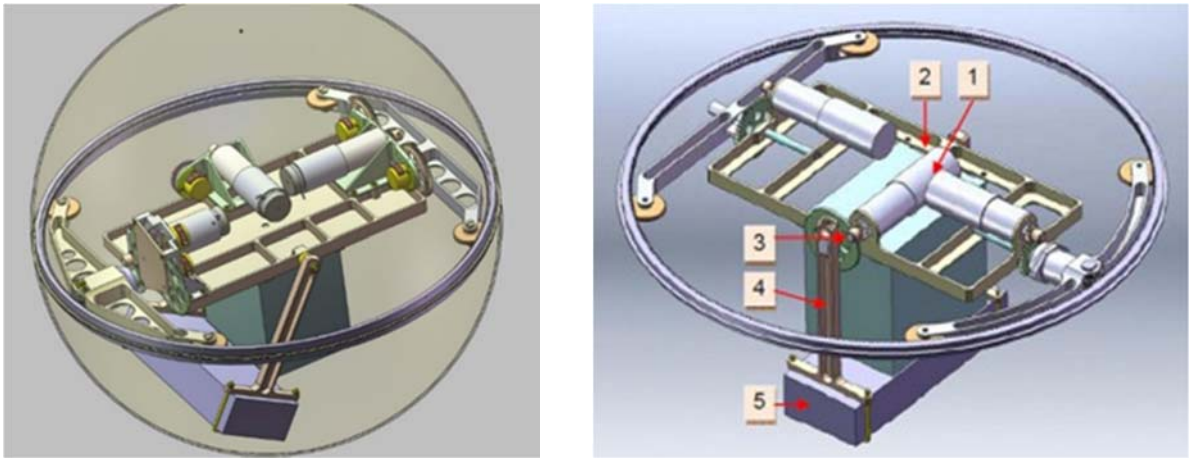


Figure 2. The principle of motion control of a spherical robot due to the deflection of a pendulum (left) and elements of the device of the pendulum drive (on the right): 1 – roll drives; 2 – frame; 3 – additional in-line transmission; 4 – pendulum arm; 5 – battery (load of the pendulum)

Figure 3 shows examples of deployment arrangements at characteristic modes. The wireless range determines the distance between the agents *L*. This realizes two-way communication between all agents, which allows the use of a decentralized team control strategy. Figure 3*a* shows the case of using all resources of multi-agent system for studying the object of interest. This is the preferable option of system deployment. A vehicle closest to the control center is selected as a master-robot.

As the distance to the object starts to grow, the group has to sacrifice scanning performance efficiency and use one or two agents as retransmitters (Figure 3*b*, and 3*c*). Since any robot in the group can act as a "master-robot", the survivability of the group increases. Disabling the "master" of the robot group in the case of exposure to the object of study does not entail the destruction of the group. With the increasing number of agents, the survivability of the group grows. In case of loss of radio contact with the control point, there are scenarios of group autonomous operation with the subsequent return of the vehicles to the base.

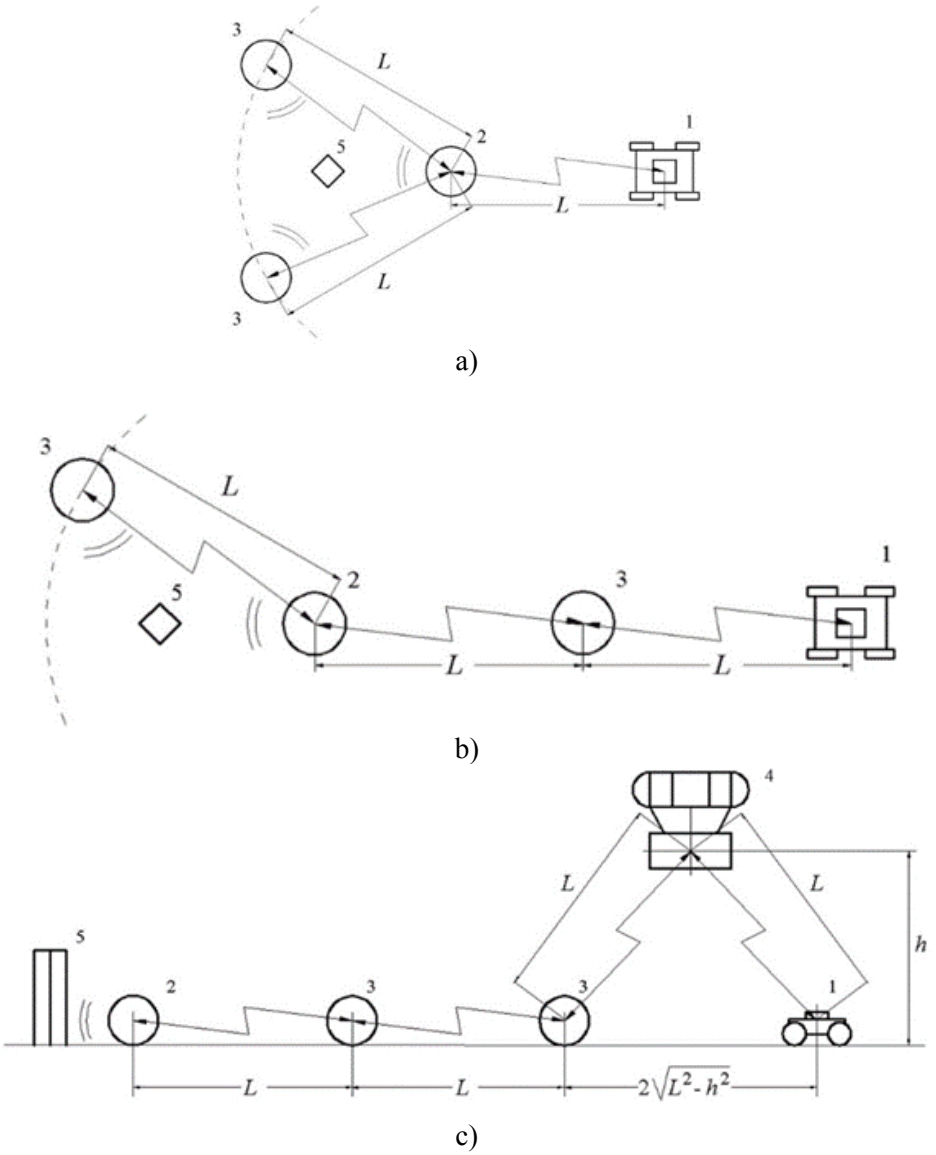


Figure 3. Basic system deployment option a) studying of object; b) studying of remote object; c) operation at the maximum distance; 1 – mobile control center (point); 2 – master-robot; 3 – slave-robot; 4 – additional retransmitter; 5 – the object of interest; *L* – the maximum allowable distance between agents; *h* – lifting height of the retransmitter

Radio communication operating in the range of 433 MHz (LoRaWAN) is used for control channels. Control channels equipment provides communication at distances up to 5 km, and organizes control channels between the control center and each of the elements of the system (robot). The capacity of the control channel is sufficient to transmit commands and data for system control. For organizing information channels radio equipment operating in the 2,4 GHz band (802,11 n) is used. The info channel has a high capacity, ensuring delivery of information from system elements. The data delivery route between the system elements may include multiple channels (hops). The algorithm of choice of optimal routes based on data about the quality of the channels between ele-

ments of the system [9, 10, 11] is used for organization of traffic delivery network. Figures 4–7 show the options of different network structures for organizing communication and control of spherical robots.

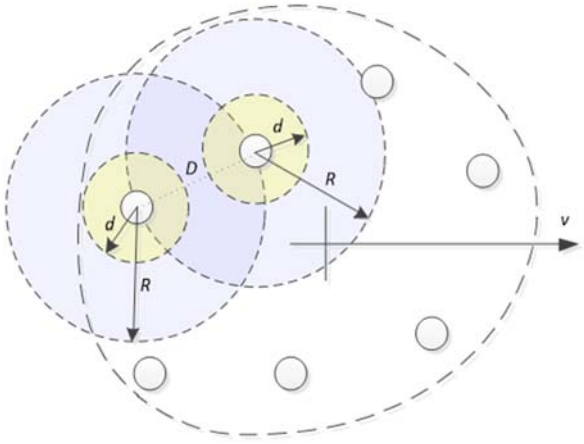


Figure 4. Model of a network with a stable position

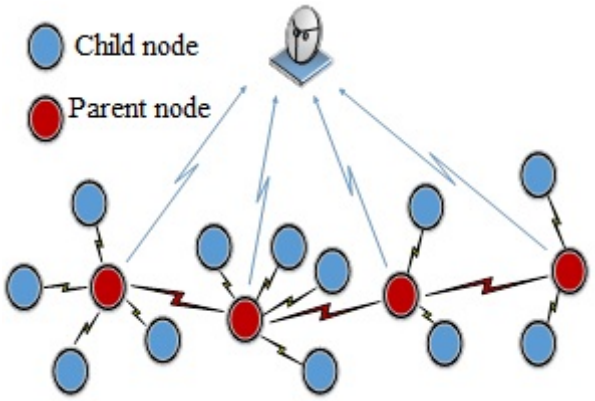


Figure 5. Communication and data transmission system for group interaction, as a self-organizing network

The selection of network structure is made dynamically, based on the data about the channels and traffic service quality and is performed using the algorithm of self-organization network. Coordinate and time support of spherical robots is planned to be solved through optimal integration of satellite navigation systems data, local radio navigation system and optical scanning devices data navigation system (for example, SLAM navigation) or using cooperative data processing [12, 13, 14].

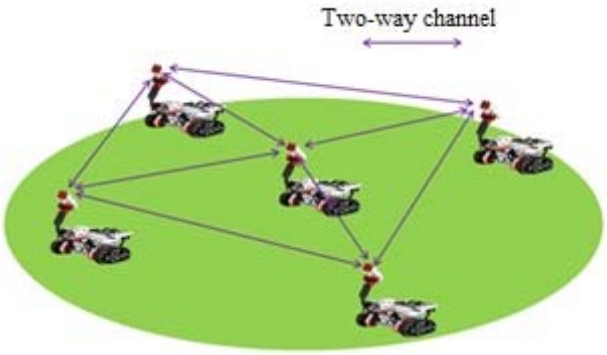


Figure 6. Decentralized network of autonomous mobile robots

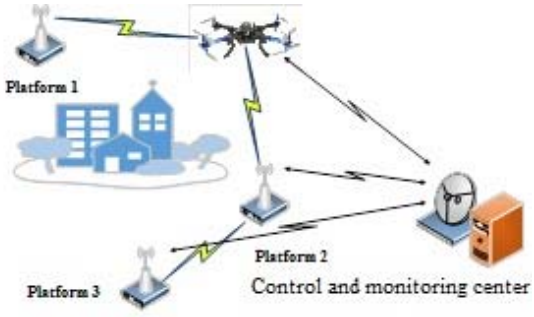


Figure 7. Interaction between nodes using a multicopter as a temporary node of a self-organizing network

Figure 8 shows a promising multi-component multi-agent robotic system, which allows operating in all known physical environments: space, air and water. This system has truly inexhaustible possibilities for monitoring the earth's surface, and the vast number of potentially ongoing interaction options.

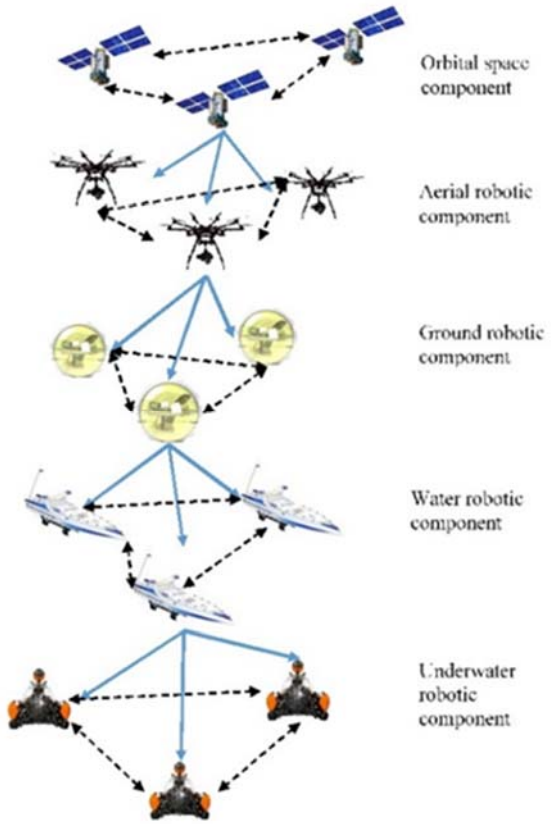


Figure 8. Multi-component multi-agent robotic system

In the system shown in figure 8, from the plurality of groups of robotic systems interaction options, we selected possible variants of interaction of surface mobile robots (SMR) and unmanned aerial vehicles (UAV). When placing UAV on board of SMR, the latest delivers the aircraft to the place of the flight task performance. At that, the UAV flight time is not consumed for the flight between original location and the flight task area. It greatly expands the operational area of the aircraft.

Besides, SMR has great power potential, part of which it is possible to use for UAV power supply. This can be done using tethered UAV, in which case the electric energy for the rotation of the propellers and power for the payload is supplied by the feeder lowering from the board of UAV to the SMR. In this case, the flight time of the UAV at a given height becomes significant. In another case, after the execution of the flight task, or when its battery becomes low, UAV is powered by the carrier in automatic mode and charge its battery from the power source of the robot or makes an automatic replacement.

When placing a specialized receiving and transmitting equipment on board of a SMR, it is possible to create a local radio navigation field with predetermined characteristics for use by the SMR. This will allow implementing coordinate and timing support to group of SMR during the suppression of the satellite orbital constellation by the interference.

Retransmitter lifted on the tethered UAV allows quickly deploy the radio network to cover large areas. The use of SMR as UAV carrier will not only provide it with power supply, but also permit to move to the position that is most convenient from the point of view of placing the relay node. UAV group with retransmitters on board will allow building up a self-organizing mesh network to ensure reliable automatic operation in terms of possible failure of some relay nodes and to establish a stable radio communication between the SMR and control point in dense urban areas. Besides, it is possible to implement tolerant delivery of information from the SMR group operating at a considerable distance.

Existence of SMR and UAV group allows carrying out remote areas examination without risk to the life of the operator. SMR moves over large areas of routing path, while UAV approaches inaccessible places and objects and at the end of the monitoring procedure returns to the surface carrier to move to the next take-off point. Installation on SMR and UAV boards of equipment for active collective technical vision will allow for localization, mapping and driving directions for SMR, modes of mutual coordinate support, coordinated search for objects of interest, forming a 3D image of the terrain surface, and in some cases to implement augmented reality to the control point controlling a group of robotic vehicles.

To ensure reliable autonomous operation of SMR group the mapping is performed by the method of the simultaneous navigation and SLAM (simultaneous localization and mapping).

Conclusions

When developing multi-agent robotic systems the tasks of traffic control and monitoring, communication and navigation must be addressed with a single system approach with the aim of achieving the set of criteria and indicators of quality.

In artificial self-organization, processes an important role is played by global as well as multiple local rules of self-organization, which are formulated by the developer at the design stage of the system setting up. In the general case, the unknown dynamics of the external environment up to the conscious counter actions to the goals and objectives of groups of robots, as well as of each of them individually should be taken into account when designing the system.

The a priori uncertainty and inconsistency of the robots knowledge about the status of the external environment, of other members of the group conditions, as well as, in general case, about their goals and objectives can significantly complicate the functioning of the system.

A wide variety of options and ways for achieving the goal, the structures of the specific group team, the distribution of roles of each robot in the group and the individual subgroups requires complex software, up to the elements of artificial intelligence, but it is unlikely this problem will be solved optimally for non-standard cases.

The distributed and dynamic nature of the planning robot team actions, which can vary significantly depending on the priority of the current task, requires rapid responding to a dynamically changing environment.

Technical problems associated with the fact that the team is a collection of heterogeneous physical objects operating in a real complex environment (the problem of reliable communication, navigation, collecting information from sensors, etc.) requires the centralized, decentralized and combined control depending on the situation.

Acknowledgment

The work is supported by the Russian Ministry of Education in the framework of the Federal Target Program "Research and development on priority directions of scientific-technological complex of Russia for 2014–2020" on the project "Development of methods and algorithms for adaptive motion control of multi spherical robots increased maneuverability in the face of uncertainty and significant external disturbances" (unique identifier project RFMEFI61315X0047).

References

1. Alexandrov V. A., Kobrin A. I. Architecture of a Mobile Robot as the Item of Hardware and Software Complex for Research of Algorithms of Group Control [Electronic resource] // Zhurnal radioelektroniki. 2011. No. 5. URL: http://jre.cplire.ru/koi/may11/index.html.

2. Gorodetsky V. I., Serebryakov S. V., Trotsky D. V. Knowledge-Based Specification Language and Reusable Software Supporting Autonomous Agents' Teamwork // Izvestiya Yuzhnogo federal'nogo universiteta. Tekhnicheskie nauki. 2011. No. 3 (116). PP. 23–41.

3. Dobrynin D. A., Karpov V. E. Simulation of Some Forms of Adaptive Behavior of Intelligent Robots // Informatsionnye tekhnologii i vychislitel'nye sistemy. 2006. No. 2. PP. 45–56.

4. Kalyaev I. A., Gaiduk A. R., Kapustyan S. G. Models and Algorithms of Collective Behavior in Groups of Robots. M. : Fizmatlit. 2009. 280 p.

5. Karpov V. E. Emotions of Robots // XII National Conference on Artificial Intelligence with International Participation of CAI-2010 (20-24 September 2010, Tver): Conference Proceedings, Moscow: Fizmatlit. 2010. Vol. 3. PP. 354–368 (in Russian).

6. Sang Shengju, Zhao Jichao, Wu Hao, Chen Shoujun, An Qi Modeling and Simulation of a Spherical Mobile Robot // ComSIS. 2010. Vol. 7, No. 1, Special Issue. PP. 51–62.

7. Dobretsov R. Yu., Borisov E. G., et al. Spherical Robot as a Platform for the Purpose of Ecological Monitoring // Transport. Transportnye sooruzheniya. Ekologiya. 2015. No. 3. PP. 35–50.

8. Dobretsov R. Yu., Vasiliev I. V. Silovoi i moshchnostnoi balans sfericheskogo dvizhitelia // Science Week of St. Petersburg Polytechnic University: Materials of the Forum with International Participation. Institute of Energy and Transport Systems. Part 1. SPb. : Publishing house of Polytechnic University, 2015. PP. 30–33.

9. Koucheryavy A. E., Prokop'ev A. V., Koucheryavy E. A. Samoorganizuyushchiesya seti. SPb. : Typography Lubavitch, 2011. 312 p.

10. Koucheryavy A., Bogdanov I., Paramonov A. The Mobile Sensor Network Lifetime under Different Spurious Flows Intrusion // 13th International Conference NEW2AN. Lecture Notes in Computer Science, Springer. 2013. PP. 28–30.

11. Koucheryavy A., Salim A. Prediction-based Clustering Algorithm for Mobile Wireless Sensor Networks // Proceedings of the International Conference on Advanced Communication Technology (ICACT 2010). Phoenix Park, Korea. 2010.

12. Borisov E. G., Mashkov G. M., Turecki L. S. Improving the Accuracy of Target Coordinates Determining in the Implementation of Cooperative Processing in Multiposition Radar System // Radiotekhnika. 2013. No. 5. PP. 4–9.

13. Mashkov G. M., Borisov E. G., Vladyko A. G. Analysis of Object Positioning Accuracy Provided by Range-Finding Systems of Various Types // Russian Aeronautics. 2015. Vol. 58. Iss. 4. PP. 401–406.

14. Mashkov G. M., Borisov E. G., Vladyko A. G., Gomonova A. I. The Use of Software-Defined Radio Systems in Multilateral Navigation Radio systems // Infocommunications Journal. 2015. Vol. 7, Iss. 2. PP. 26–31.

УДК 004.7:004.422.8

МЕТОДОЛОГИЧЕСКОЕ ПРОФИЛИРОВАНИЕ ИНТЕЛЛЕКТУАЛИЗАЦИИ ИНФОРМАЦИОННЫХ ИНФРАСТРУКТУР

Л. К. Птицына

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

Представлено системное обобщение современных направлений интеллектуализации информационных инфраструктур, систематизированы целевые ориентиры каждого из представленных направлений, сформированы требования к методологии интеллектуализации, предложена концепция методологического профилирования интеллектуализации, выделены типовые ситуации методологического профилирования интеллектуализации, определены ключевые составляющие методологических базисов для множества профилей, связанных с высокопроизводительными технологиями, сетевыми технологиями, информационными технологиями, безопасными технологиями, когнитивными технологиями, агентными технологиями, гипертехнологиями, раскрыты формализации процесса генерации ключевых составляющих методологических базисов, описаны проекты, реализованные на базе методологического профилирования интеллектуализации, приведены характеристики, демонстрирующие их достоинства и преимущества.

сетевые технологии, информационные технологии, безопасные технологии, когнитивные технологии, агентные технологии, гипертехнологии, генерация знаний, преодоление неопределённости, достижение целей, гарантии качества.

Научные основы интеллектуализации информационных инфраструктур относятся к области науки «Искусственный интеллект», в которой определяются, систематизируются, решаются, анализируются, оптимизируются и автоматизируются интеллектуальные задачи.

В искусственном интеллекте различаются три категории интеллектуальных задач:

– задачи воспроизведения способностей человека;

– задачи обеспечения рациональности, когда все действия, относящиеся к некоторой системе, выполняются правильно, в условиях обладания знаниями о том, что является правильным;

– задачи воссоздания окружающей среды для объектов, (и/или) субъектов и их взаимодействия.

Интеллектуализация информационных инфраструктур обеспечивается посредством решения всех категорий представленных задач.

Во множестве известных реализаций искусственного интеллекта выделяются следующие категории систем:

– системы с воспроизведением мыслительных процессов;

– системы с воспроизведением рациональных рассуждений;

– системы реализации функций, требующих интеллектуальности при их выполнении людьми;

– системы реализации рациональных действий.

Реализация систем базируется на одном из возможных подходов или их сочетании:

– подход, основанный на когнитивном моделировании;

– подход, основанный на применении законов мышления;

– подход, основанный на использовании Теста Тьюринга;

– подход, основанный на формировании модельно-аналитического интеллекта;

– подход, основанный на создании интеллектуальных агентов.

При функциональном определении интеллекта по тесту Тьюринга предусматриваются:

– средства обработки текстов на естественных языках;

– средства представления знаний;

– средства автоматического формирования логических выводов;

– средства машинного обучения;

– средства машинного зрения для восприятия объектов;

– средства робототехники для манипулирования объектами и перемещения в пространстве.

В концептуальном плане подход, основанный на формировании модельно-аналитического интеллекта, может сочетаться с каждым из других представленных базовых предпочтений и являться системным компонентом любого из средств, предусматриваемых согласно тесту Тьюринга. В связи с этим к модельно-аналитическому интеллекту предъявляются такие требования, которые, в первую очередь, касаются обеспечения необходимо качества функционирования систем искусственного интеллекта. Профилирование качества функционирования систем искусственного интеллекта осуществляется в контексте области их применения. При подобной концепции интеллектуализации информационных инфраструктур её методология распространяется на методологический базис, включающий:

выбор профилей качества, обоснование выделения системы классов моделей процессов функционирования информационных инфраструктур и методов их связывания, определение системы методик построения модельного ряда, разработку и применение методов анализа модельного ряда в системе выделенных классов, ситуационное разграничение аналитических формализаций, формирование инвариантов для верификации аналитических формализаций, отображение аналитических формализаций на инфокоммуникационные ресурсы, проектирование, создание и сопровождение программного обеспечения, управление качеством выполняемых интеллектуальной системой работ согласно определяемым требованиям. В соответствии с архитектурой информационных инфраструктур методологический базис образуется для множества профилей, связанных с высокопроизводительными технологиями [1], сетевыми технологиями [2, 3], информационными технологиями [4], безопасными технологиями [5], когнитивными технологиями [6], агентными технологиями [7, 8], гипертехнологиями [9].

Ключевые особенности методологического базиса отчётливо проявляются при профилировании интеллектуализации локального интерфейса управления [2, 3]. Методологическим базисом обеспечивается определение гарантий качества локального интерфейса управления как на уровне отдельно взятого виртуального соединения, так и на уровне трактов связи. При соблюдении гарантий учитываются особенности различных физических сред трактов связи и ситуаций в окружающей среде.

Методологическое профилирование интеллектуализации агентных технологий ориентируется на формирование их модельно-аналитического интеллекта в пассивных и активных инфокоммуникационных средах. Модельно-аналитический интеллект формируется применительно к ситуациям преодоления априорной неопределённости относительно информационной инфраструктуры и ситуациям достижения выбранных целей для информационных агентов.

Связывание формализаций анализа различных классов объектно-ориентированных моделей информационных агентов выполняется согласно концептуальной модели интеллектуального агента из состава многоагентной системы в инфокоммуникационной среде, представленной на рисунке.

Представленные методологические профили интеллектуализации внедрены в инфраструктурах предприятий судостроения, авиастроения, связи и банковской сферы. В каждом из реализованных проектов обеспечивается повышение качества функционирования систем на основе внедрённых модулей модельно-аналитического интеллекта.

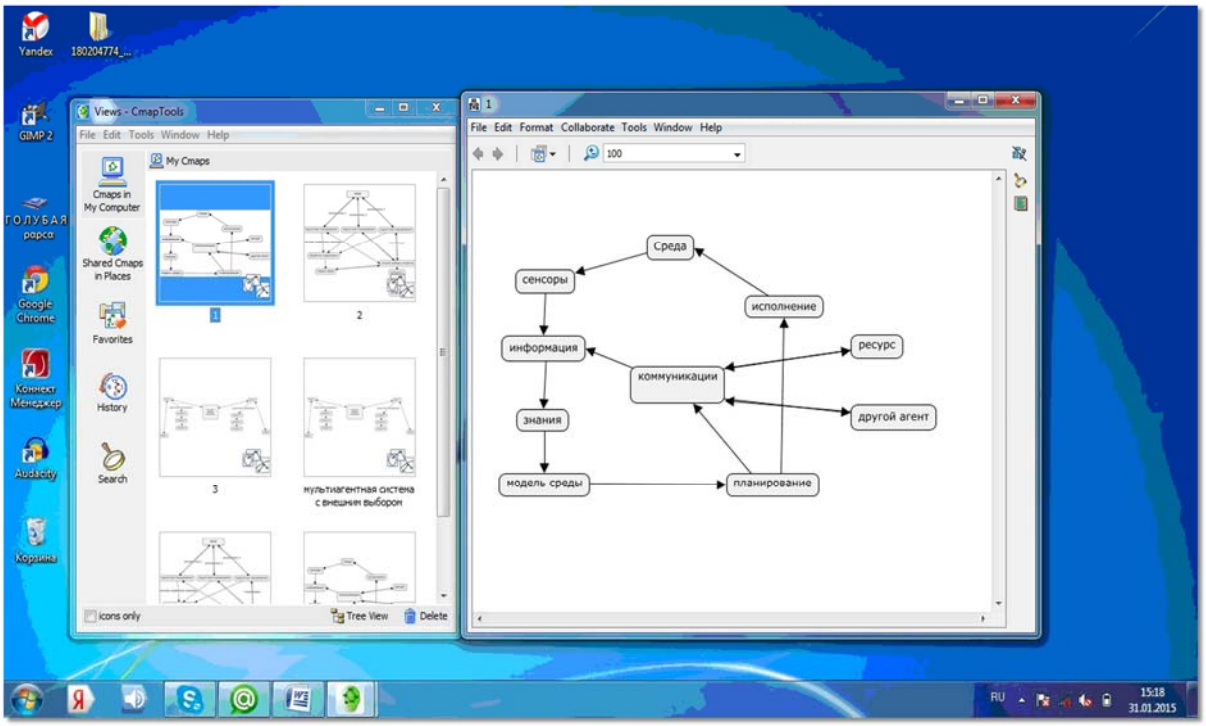


Рисунок. Концептуальная модель интеллектуального информационного агента из состава многоагентной системы в инфокоммуникационной среде

Список используемых источников

1. Птицына Л. К., Соколова Н. В. Параллельные вычислительные процессы в системах мониторинга и управления : учеб. пособие. СПб. : Изд-во Политехн. ун-та, 2008. 134 с. ISBN 978-5-7422-2066-4.

2. Птицын А. В., Птицына Л. К. Системно-аналитическое обеспечение локального интерфейса управления трактом связи // Телекоммуникации. 2013. № 2. С. 9–14.

3. Птицына Л. К. Моделирование систем. Система моделирования локального интерфейса управления в сетях коммутации кадров : учеб. пособие. СПб. : СПбГУТ, 2013. 84 с.

4. Птицына Л. К., Смирнов Н. Г. Программное обеспечение компьютерных сетей. Управление крупно-гранулярными процессами на основе языка BPEL : учеб. пособие. СПб. : Изд-во Политехн. ун-та, 2011. 105 с. ISBN 978-5-7422-2951-3.

5. Птицын А. В., Птицына Л. К. Генерация системно-аналитического ядра безопасных информационных технологий : монография. СПб. : Изд-во Политехн. ун-та, 2011. 262 с. ISBN 978-5-7422-3143-1.

6. Птицына Л. К., Добрецов С. В. Интеллектуальные технологии и представление знаний. Планирование действий интеллектуальных агентов в информационных сетях : учеб. пособие. СПб. : Изд-во Политехн. ун-та, 2006. 172 с. ISBN 5-7422-1101-5.

7. Птицына Л. К., Птицын А. В. Объектно-ориентированный анализ достижимости целей программными интеллектуальными агентами [Электронный ресурс] // Актуальные проблемы инфотелекоммуникаций в науке и образовании. II Международная научно-техническая и научно-методическая конференция: сб. научных статей. СПб. : Санкт-Петербургский государственный университет телекоммуникаций им. проф. М. А. Бонч-Бруевича, 2013. С. 636–640. URL: http://www.sut.ru/doci/nauka/sbornic_confsut_2013_no_copy.pdf (дата обращения 15.04.2016).

8. Птицына Л. К., Лебедева А. А. Разработка системно-аналитического ядра информационных интеллектуальных агентов с динамической синхронизацией их действий [Электронный ресурс] // Актуальные проблемы инфотелекоммуникаций в науке и образовании. III Международная научно-техническая и научно-методическая конференция: сб. научных статей. СПб. : Санкт-Петербургский государственный университет телекоммуникаций им. проф. М. А. Бонч-Бруевича, 2014. С. 505–509. URL: http://www.sut.ru/doci/nauka/iiiapino2014.pdf (дата обращения 15.04.2016).

9. Птицын А. В., Птицына Л. К. Аналитическое моделирование комплексных систем защиты информации. Гамбург. Saarbrucken: LAP LAMBERT Academic Publishing, 2012. 293 с. ISBN 978-3-659-23299-2.

УДК 331.108.2

ИНФОРМАЦИОННО-АНАЛИТИЧЕСКАЯ СИСТЕМА ПОДДЕРЖКИ ПРИНЯТИЯ УПРАВЛЕНЧЕСКИХ РЕШЕНИЙ: ОПЫТ СОЗДАНИЯ И ПЕРСПЕКТИВЫ РАЗВИТИЯ

И. А. Громов

Комитет по информатизации и связи Санкт-Петербурга

Для эффективного управления регионом органам государственной власти необходимо иметь оперативную статистическую информацию. Разрабатываются междисциплинарные инструменты для сбора необходимых данных. Предлагаемая информационно-аналитическая система позволит обеспечить решение различных задач в отраслевом, временном и территориальном разрезе.

информационно-аналитическая система, органы государственной власти, сбор информации, мониторинг, анализ, комплексное прогнозирование.

Введение

Эффективное управление регионом невозможно без информационно-аналитического обеспечения органов государственной власти ведомственными и статистическими данными, результатами мониторинга и анализа социально-экономического развития региона, оперативными прогнозами ключевых показателей регионального развития. Качество предоставляемых информационно-аналитических материалов влияет на эффективность принимаемых управленческих решений и зависит от ряда условий, в том числе наличия комплекса инструментов, используемых для проведения мониторинга, анализа и прогнозирования.

К числу таких инструментов следует отнести информационно-аналити-ческие системы, обеспечивающие функционирование информационной базы с достаточной ретроспективой и полнотой информации

и апробированного комплексного прогнозно-аналитического инструментария, позволяющего решать различные задачи в отраслевом, временном и территориальном разрезе в автоматизированном режиме.

В качестве информационно-аналитической платформы для анализа и прогнозирования социально-экономического развития региона может выступать государственная информационная система «Интегрированная система информационно-аналитического обеспечения исполнительных органов государственной власти Санкт-Петербурга»[1] (далее Система, ИС ИАО), функционирующая на средствах СПб ГУП «СПб ИАЦ» – подведомственной организации Комитета по информатизации и связи. ИС ИАО была разработана в 2001 году [1, 2, 3], когда подобных систем практически не было, и явилась одной из первых разработок центра. За последние 3 года Система получила мощное развитие и в настоящее время обеспечивает информационно-аналитическую поддержку исполнительных органов государственной власти Санкт-Петербурга.

Система подключена к Единой мультисервисной телекоммуникационной сети исполнительных органов государственной власти Санкт-Петербурга[2] (ЕМТС) и обеспечивает информационно-аналитическую поддержку всем специалистам и руководителям ИОГВ Санкт-Петербурга. Основным фундаментом ИС ИАО является Хранилище данных, которое систематически пополняется информацией из различных источников: ведомственная статистика, государственная федеральная и региональная статистика и др.

На рисунке 1 изображено место ИС ИАО в контуре регионального управления.

На средствах ИС ИАО осуществляется:

– сбор и накопление информации, характеризующей различные аспекты социально-экономического развития города;

– мониторинг и анализ основных социально-экономических процессов развития Санкт-Петербурга и его районов;

– анализ социально-экономического развития Санкт-Петербурга в сравнении с другими субъектами РФ;

– комплексное прогнозирование социально-экономического развития Санкт-Петербурга по различным сферам жизнедеятельности города;

– мониторинг общественного мнения населения Санкт-Петербурга, в том числе в разрезе районов;

[1] Согласно постановлению Правительства Санкт-Петербурга от 24 апреля 2014 г. № 279, ИС ИАО является государственной информационной системой Санкт-Петербурга. Оператором Системы является Санкт-Петербургское государственное унитарное предприятие «Санкт-Петербургский информационно-аналитический центр».

[2] На сегодняшний день ЕМТС является мощным инструментом, позволяющим получить доступ к различным информационным ресурсам. Это позволяет различным учреждениям осуществлять оперативное взаимодействие с подразделениями, в том числе используя защищенные каналы связи.

– обеспечение руководства и специалистов исполнительных органов государственной власти Санкт-Петербурга статистическими и опросными данными и аналитическими материалами в режиме «удаленного доступа»;

– поддержка управленческих решений членов Правительства Санкт-Петербурга и руководителей исполнительных органов государственной власти Санкт-Петербурга путем обеспечения их информационно-аналитическими материалами, включая оценку возможных последствий принятия управленческих решений, а также справочными и презентационными материалами по вопросам жизнедеятельности города.

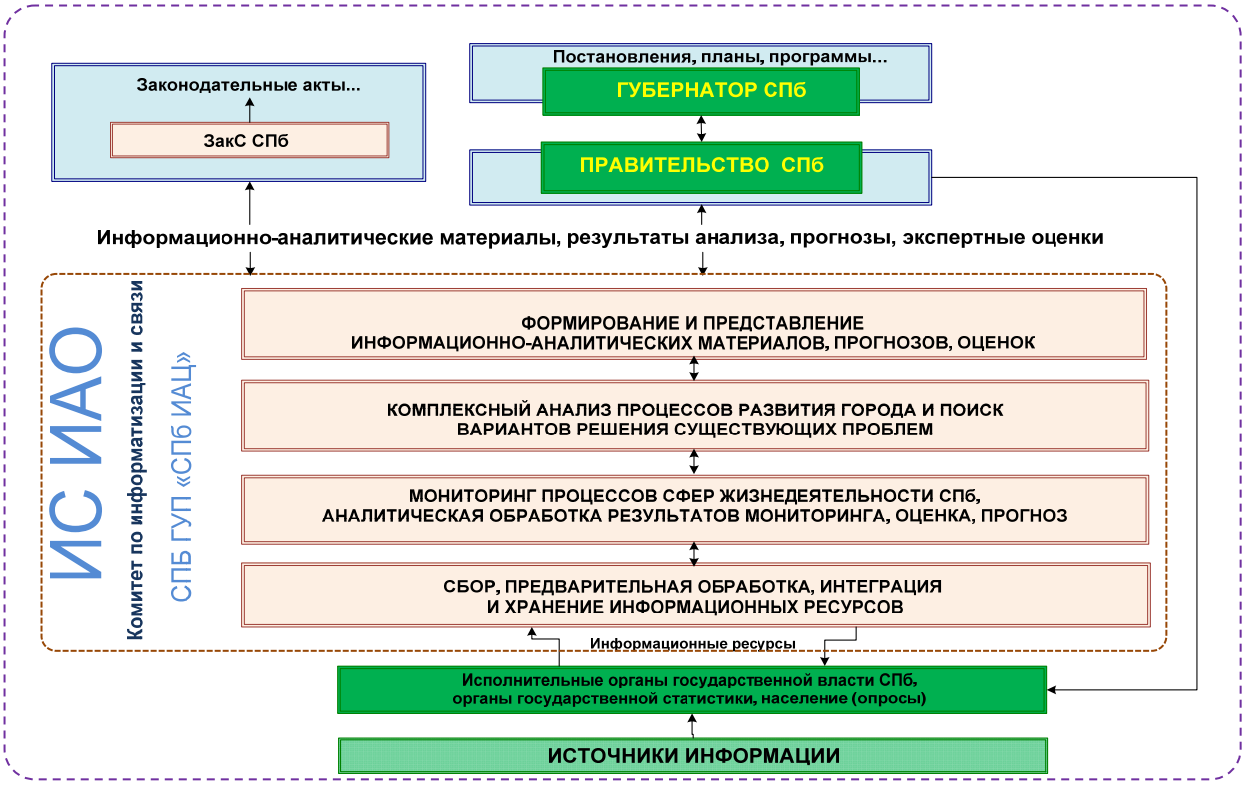


Рис. 1. Место ИС ИАО в контуре управления

Важным аспектом успешного планирования регионального развития является использование научно-обоснованных подходов, современных методов и программных средств прогнозирования. К прогнозу социально-экономического развития региона предъявляются серьезные требования – он должен быть многовариантным, достоверным, согласованным, сбалансированным, учитывать информацию как о стартовых условиях региона, так и о возможных вариантах интенсивности развития экономических процессов в будущем, а также возможные изменения внешнеполитических и внешнеэкономических условий.

1 Инструментальные средства ИС ИАО

В составе ИС ИАО функционируют инструментальные средства моделирования, предназначенные для решения прогнозно-аналитических задач на основе научно-обоснованных подходов. Это в том числе средства оперативного анализа и прогнозирования и комплексного прогнозирования на средне- и долгосрочную перспективу (рис. 2).

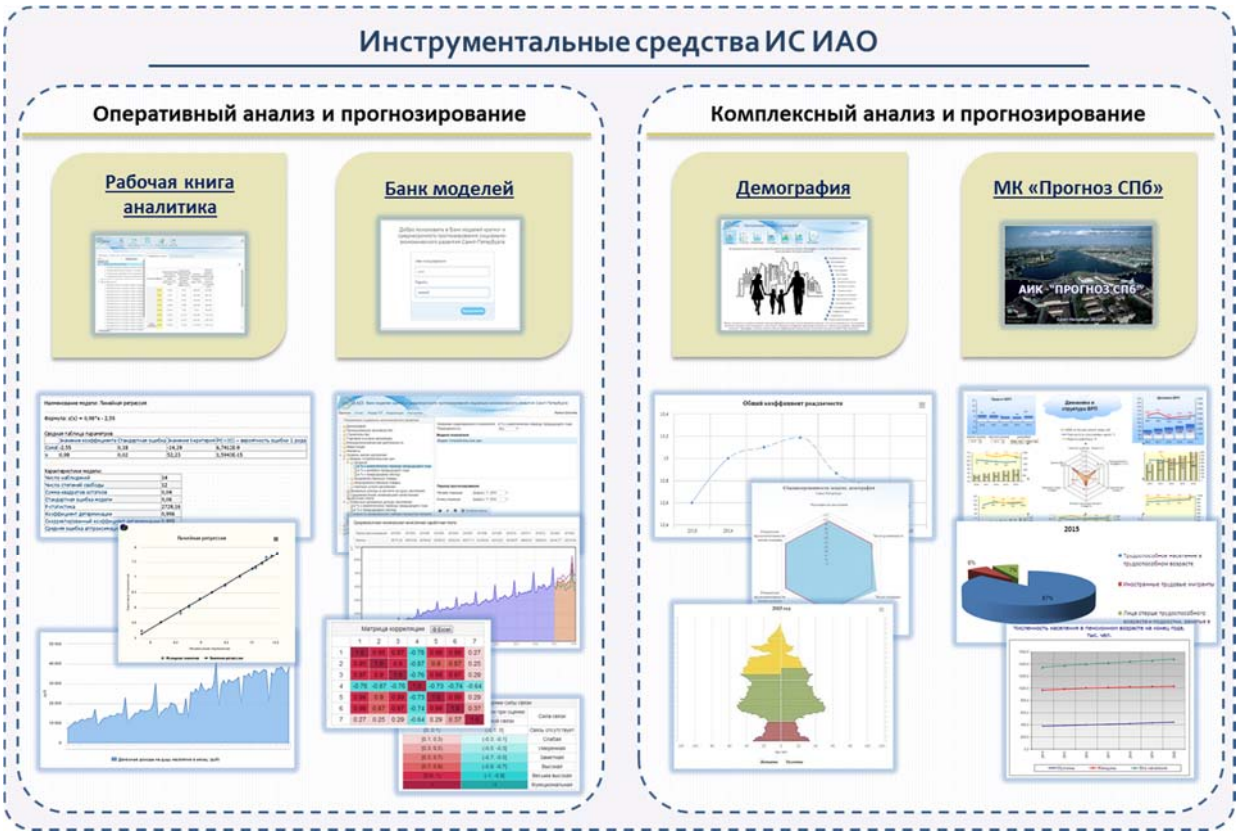


Рис. 2. Инструментальные средства анализа и прогнозирования

1.1 Хранилище данных

Информационной базой инструментальных средств анализа и моделирования является Хранилище данных ИС ИАО, которое содержит свыше 36 тыс. первичных показателей (> 9 млн записей) и более 2400 информационно-аналитических материалов по различным тематикам.

В Хранилище данных информация структурирована и предметно-ориентирована, что обеспечивает оперативный доступ к нужному показателю или информационно-аналитическому материалу. В нем содержатся официальные статистические и ведомственные данные по показателям социально-экономического развития Санкт-Петербурга и других субъектов СЗФО и РФ, каждое значение имеет свой источник информации.

1.2 Оперативный анализ и прогнозирование

Рабочая книга аналитика

Рабочая книга аналитика предназначена для проведения оперативного анализа статистической информации по различным показателям, характеризующим основные сферы жизнедеятельности региона. Данный инструмент позволяет анализировать массивы данных и формировать отчеты по выбранным показателям.

В Рабочей книге аналитика имеется возможность сравнительной оценки социально-экономического положения различных субъектов СЗФО и РФ, районов и муниципальных образований Санкт-Петербурга. Для проведения сравнительного анализа используются графическое и картографическое представление данных.

Банк моделей

Банк моделей кратко- и среднесрочного прогнозирования социально-экономического развития Санкт-Петербурга (Банк моделей) представляет собой удобный инструментарий, позволяющий специалистам, не обладающим специальными навыками моделирования, формировать прогнозы социально-экономического развития региона на кратко- и среднесрочную перспективу в режиме онлайн за считанные минуты.

Информация в Банк моделей поступает непосредственно из Хранилища данных ИС ИАО, тем самым отчетные данные обновляются в режиме реального времени, что позволяет формировать прогнозы на актуальных статистических данных.

В программный продукт заложены наиболее известные методы эконометрического моделирования, что дает гарантию получения надежных математически обоснованных прогнозов. В автоматическом режиме происходит оценка качества моделей по определенным критериям, вследствие чего имеется возможность оперативно отслеживать устаревшие модели и поддерживать актуальность и надежность формируемых прогнозов.

1.3 Комплексный анализ и прогнозирование

Демография

Программный компонент прогнозирования ключевых индикаторов, характеризующих развитие демографической ситуации в регионе («Демография»), предназначен для формирования прогноза численности и возрастно-половой структуры населения региона, а также основных показателей демографического развития региона.

Прогнозирование возрастно-половой структуры в программном компоненте «Демография» осуществляется на основе задаваемого экспертно сценария, отражающего динамику показателей рождаемости, смертности

и миграционного прироста на прогнозном периоде с использованием метода передвижки возрастов и с учетом планов комплексного освоения территорий. Прогноз формируется как по Санкт-Петербургу в целом, так и по его районам. Для формирования прогноза используются сбалансированные статистические данные, что позволяет получать полностью согласованный прогноз на период до 2040 г.

Результаты прогнозирования могут использоваться для территориального планирования и для формирования планов бюджетов различных уровней.

Моделирующий комплекс «Прогноз СПб»

Моделирующий комплекс «Прогноз СПб» (МК «Прогноз СПб») пред-назначен для анализа и комплексного прогнозирования социально-экономического развития Санкт-Петербурга по различным сферам жизнедеятельности города. Фундаментом МК «Прогноз СПб» является имитационная модель социально-экономической деятельности региона [4], отражающая процессы образования, перераспределения и использования материальных, финансовых и трудовых ресурсов Санкт-Петербурга в их причинно-следственной взаимосвязи.

Построение имитационной модели социально-экономического развития Санкт-Петербурга базируется на концепции «баланс балансов», которая обеспечивает полную сбалансированность получаемого прогноза по всем направлениям социально-экономического развития для любого временного интервала.

С использованием инструментальных средств моделирующего комплекса проводится верификация и коррекция исходной информации о состоянии региона и устраняется противоречивость данных. Процесс верификации данных и настройка модели на фактические данные в МК «Прогноз СПб» осуществляется в автоматизированном режиме.

На базе МК «Прогноз СПб» могут определяться различные варианты социально-экономического развития Санкт-Петербурга в зависимости от состояния внешней и внутренней среды региона, в соответствии с задаваемыми экспертно сценарными условиями.

2 Прогнозно-аналитические задачи, решаемые на средствах ИС ИАО

Значимую роль в организации управленческой деятельности исполнительных органов государственной власти занимает решение задач прогнозирования и индикативного планирования. К прогнозно-аналитическим задачам, решаемым на средствах ИС ИАО, относятся следующие задачи.

2.1 Моделирование и прогнозирование социально-экономических процессов на основе сложившихся тенденций

Формирование прогноза отдельных социально-экономических процессов осуществляется на основе методов анализа временных рядов. Инструментальные средства в составе ИС ИАО позволяют оперативно проводить анализ динамики развития города по отдельным показателям, выявлять скрытые закономерности в данных, осуществлять моделирование и формировать кратко- и среднесрочные прогнозы.

К числу решаемых прогнозно-аналитических задач относятся:

– прогнозирование основных показателей, характеризующих уровень жизни населения;

– разработка прогноза индексов промышленного производства по видам экономической деятельности;

– прогнозирование уровня потребительских цен на основные продовольственные товары в регионе;

– формирование прогноза состояния преступности в регионе;

– прогнозирование ключевых показателей, характеризующих жилищные условия горожан.

Систематически проводится апостериорная верификация прогноза, что обеспечивает надежность и качество предоставляемых прогнозных оценок.

2.2 Выявление взаимного влияния факторов социально-экономического развития региона

Исследование взаимного влияния факторов социально-экономического развития региона позволяет выявить причины поведения изучаемых процессов и способы обеспечения желаемого их развития. Опираясь на результаты анализа взаимовлияния, появляется также возможность определить будущее состояние исследуемых факторов в зависимости от динамики коррелируемых показателей.

Примерами решаемых прогнозно-аналитических задач являются:

– исследование влияния факторов социально-экономической природы на расслоение населения Санкт-Петербурга по доходам;

– анализ взаимного влияния показателей потребительского рынка и заработной платы;

– выявление основных социально-экономических факторов, оказывающих влияние на криминогенную ситуацию в регионе.

2.3 Многовариантное прогнозирование

Многовариантное прогнозирование направлено на выявление основных тенденций регионального развития в зависимости от состояния внешней и внутренней среды региона (рис. 3).

Результаты прогнозирования используются для оценки последствий принимаемых решений, подготовки предложений по решению существующих и избеганию потенциальных проблем. В частности, к таким задачам относятся:

– прогнозирование численности и возрастно-половой структуры населения по городу и его районам по однолетним возрастно-половым интервалам;

– прогнозирование баланса трудовых ресурсов – основных показателей, характеризующих рынок труда региона в разрезе видов экономической деятельности и форм собственности;

– долгосрочное прогнозирование индикаторов социально-экономического развития региона по различным сферам жизнедеятельности (на период до 20 лет). Результаты прогнозирования могут быть использованы для формирования долгосрочной стратегии развития региона по различным направлениям.

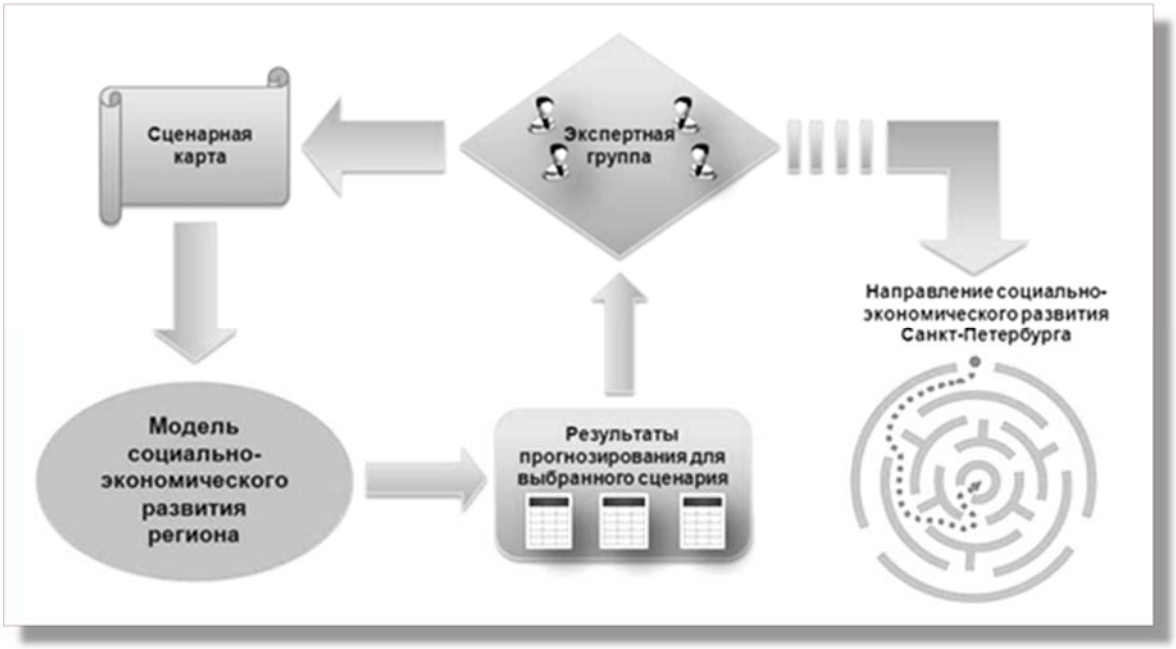


Рис. 3. Многовариантное прогнозирование

2.4 Оценка реализации стратегий и приоритетных национальных и региональных программ

Эффективность приоритетных национальных и региональных программ можно оценить путем решения задач индикативного планирования (рис. 4).

Традиционно индикативное планирование рассматривается как процесс формирования системы индикаторов, характеризующих направление развития экономики страны (региона), и установление мер государственного воздействия на социальные и экономические процессы для достижения заявленных целевых значений этих индикаторов. Методологически индикативное планирование является технологией прогнозного исследования, обратной ситуационному прогнозированию. Оно требует решения обратных задач, когда поставленная цель декомпозируется в рациональную последовательность принимаемых решений.

Данный подход позволяет определить систему мер государственного регулирования социально-экономических процессов в регионе, обеспечивающих достижение запланированных значений индикаторов развития города по различным направлениям к установленному сроку. Основными документами, содержащими эти индикаторы, являются:

– майские указы Президента РФ;

– Стратегия социально-экономического развития СЗФО на период до 2020 г.;

– Стратегия социально-экономического развития Санкт-Петербурга до 2030 г.

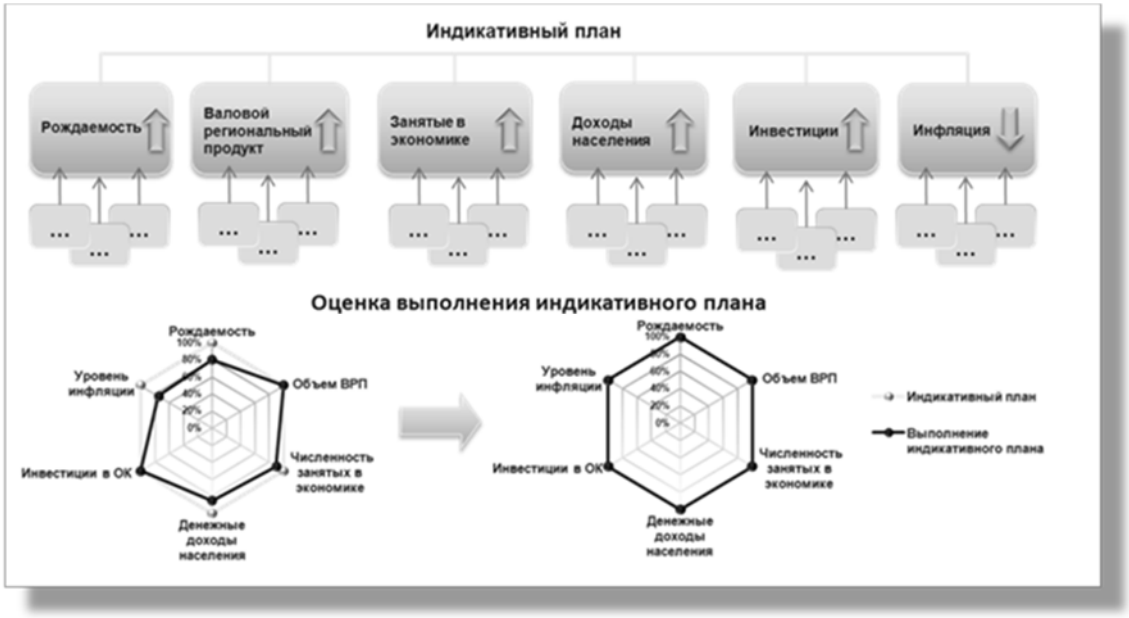


Рис. 4. Индикативное планирование

3 Направления развития ИС ИАО

Все руководители и специалисты ИОГВ могут иметь доступ к имеющейся в Системе статистической информации, информационно-аналитическим материалам и инструментальным средствам анализа и прогнозирования. Это является важным преимуществом ИС ИАО, так как дает возможность всем органам государственной власти Санкт-Петербурга ра-

ботать с единой информационной базой, опираться при планировании развития города на единый прогноз регионального развития.

Всеохватывающая, структурированная, качественно представленная информация по всевозможным направлениям жизнедеятельности Санкт-Петербурга составляет основу эффективных решений в области управления городом. В 2016 г. принято решение об интеграции информационных систем с целью аккумулирования информации о функционировании и развитии города в единой базе. Платформой для интеграции информационных систем может выступать ИС ИАО. В настоящее время ведутся работы по организации взаимодействия ИС ИАО с такими информационными системами как Территориальная отраслевая региональная информационная система, Автоматизированная информационная система мониторинга наркоситуации в Санкт-Петербурге, Автоматизированная информационная система обеспечения безопасности жизнедеятельности Санкт-Петербурга, портал «Наш Санкт-Петербург» и др.

К сожалению, в настоящее время возможности ИС ИАО используются не в полной мере. Нередко кадровые перестановки в администрациях районов и отраслевых комитетах Санкт-Петербурга приводят к недостаточной информированности специалистов и руководителей ИОГВ о преимуществах Системы. Вот почему важным направлением развития ИС ИАО является ее популяризация среди органов государственной власти. Достижение данной цели предполагается путем установления регламента работы с ИС ИАО и организации более интенсивного систематического обучения специалистов и руководителей ИОГВ работе с Системой.

Заключение

Для повышения эффективности государственной региональной политики необходимо определение мер государственного регулирования, которые бы способствовали достижению целевых ориентиров социально-экономического развития субъекта РФ. Инструментальные средства моделирования и прогнозирования в составе ИС ИАО позволяют решать широкий спектр прогнозно-аналитических задач, обеспечивающих информационно-аналитическую поддержку исполнительных органов государственной власти Санкт-Петербурга.

В рамках функционирования ИС ИАО осуществляется мониторинг основных показателей жизнедеятельности региона, формируются многовариантные сбалансированные прогнозы социально-экономического развития Санкт-Петербурга, учитывающие информацию, как о стартовых условиях региона, так и о возможных вариантах интенсивности развития экономических и социальных процессов в будущем, а также возможные изменения внешнеполитических и внешнеэкономических условий. Прогнозно-аналитические средства системы дают возможность «проиграть»

стратегии развития региона и выявить последствия принимаемых управленческих решений, что позволяет находить оптимальные решения для достижения поставленных целей, сохраняя баланс между различными ресурсами (материальными, трудовыми, финансовыми и организационными).

Список используемых источников

1. Об организации информационно-аналитического обеспечения Администрации Санкт-Петербурга: Приказ Губернатора Санкт-Петербурга от 17.01.2001 г. № 3-п [Электронный ресурс]. URL: http://docs.cntd.ru/document/8345709 (дата обращения 18.04.2016).

2. Руководство по информационно-аналитическому взаимодействию исполнительных органов государственной власти Санкт-Петербурга (в рамках ИС ИАО). Утверждено губернатором Санкт-Петербурга 07.05.2001 г.

3. Регламент подготовки аналитических документов для губернатора Санкт-Петербурга и Правительства Санкт-Петербурга (в рамках ИС ИАО). Утвержден губернатором Санкт-Петербурга 07.05.2001 г.

4. Цыбатов В. А. Моделирование экономического роста / под науч. ред. Г. Р. Хасаева. Самара : Изд-во Самар. гос. экон. ун-та, 2006. 385 с. ISBN 5-94622-202-3.

УДК 654.1

К 100-ЛЕТИЮ КЛОДА ШЕННОНА – ОСНОВАТЕЛЯ ТЕОРИИ ИНФОРМАЦИИ

В. И. Коржик

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

Излагаются краткие сведения из биографии К. Э. Шеннона, основные направления его научной деятельности и основные результаты его исследований.

К. Э. Шеннон, биография, основные научные результаты.

1 Краткие биографические сведения

Клод Элвуд Шеннон – выдающийся американский математик, инженер и криптограф, известный во всём мире как «отец теории информации».

Клод Элвуд Шеннон родился 30 апреля 1916 г. в г. Petoskey (шт. Michigan). Родители: отец – Claude, Sr. (бизнесмен), мать – учительница.

Образование: получил степень бакалавра в университете Michigan по специальности электротехники и математики (1936), степень магистра в Massachusetts Institute of Technology (MIT, 1937).

Основные научные достижения:

– символический анализ переключательных схем (1938);

– алгебра в теоретической генетике (1940);

– работа в Bell Labs в области криптографии и противопожарных систем;

– работа (совместно с A. Turing) по взлому шифров и засекречиванию речевых сигналов (1940–1945);

– разработка методов сглаживания и предсказания сигналов (1945);

– меморандум “Mathematical Theory of Cryptography” (1945), (рассекречено в 1949 г.);

– публикация основного труда К. Шеннона “A Mathematical Theory of Communication” (1948) в журнале Bell System Technical Journal (BSTJ).

Дополнительные научные достижения К. Шеннона:

– построение устройства, которое решило бы проблему «Кубика-Рубика»;

– разработка программ для игры в шахматы (1950);

– применение теории информации в теории игр и биржевых операций.

2 Увековечивание памяти К. Шеннона (скончался в 2001 г.)

Создано шесть скульптур К. Шеннона в Университете Michigan, MIT, в университете San-Diego, в Bell Labs и в “AT&T Shannon's Labs”.

Международное общество IEEE on IT учредило специальную премию “The Claude E. Shannon Award”, которая присуждается учёным по всему миру за выдающиеся заслуги в области «Теории информации». Список лауреатов этой премии представлен ниже [1]:

1972 – Claude E. Shannon
1974 – David S. Slepian
1976 – Robert M. Fano
1977 – Peter Elias
1978 – Mark Semenovich Pinsker
1979 – Jacob Wolfowitz
1981 – W. Wesley Peterson
1982 – Irving S. Reed
1983 – Robert G. Gallager
1985 – Solomon W. Golomb
1986 – William Lucas Root
1988 – James Massey
1990 – Thomas M. Cover
1991 – Andrew Viterbi
1993 – Elwyn Berlekamp
1998 – Neil Sloane
1999 – Tadao Kasami
2000 – Thomas Kailath
2001 – Jack Keil Wolf
2002 – Toby Berger
2003 – Lloyd R. Welch
2004 – Robert Mc-Elice
2005 – Richard Blahut
2006 – Rudolf Ahlswede
2007 – Sergio Verdú
2008 – Robert M. Gray
2009 – Jorma Rissanen
2010 – Te Sun Han
2011 – Shlomo Shamai (Shitz)
2012 – Abbas El Gamal

1994 – Aaron D. Wyner
1995 – George David Forney
1996 – Imre Csiszár
1997 – Jacob Ziv
2013 – Katalin Marton
2014 – János Körner
2015 – Robert Calderbank
2016 – Alexander Holevo

Один из лауреатов из Советского Союза – д-р физ.-мат. наук, профессор Марк Семёнович Пинскер. Большинство лауреатов хорошо известно российским учёным по их значительному вкладу в теорию связи и криптографию (*Slepian, Fano, Gallager, Golomb, Massey, Tomas, Cover, Viterbi, Berlekamp, Wyner, Ziv, Kasami, Kailath, Berger, Mc-Elice, Blahut, Alswede, El-Gamal*).

Ниже приведены два основных направления в науке, созданных и развитых К. Шенноном.

3 Теория информации (теоремы кодирования)

В каналах без помех (кодирование источников сообщений)

Если задан источник сообщений своим алфавитом и вероятностями появления отдельных символов и канал связи, заданный своим алфавитом, то пределы возможности сжатия источника (экономного кодирования) определяются такой характеристикой источника как его энтропия

$$H(A) = -\sum_{i=1}^{k} p(a_i) \log p(a_i).$$

(Это характеристика также предложена Шенноном).

В каналах с помехами

Пусть задан дискретный канал с помехами, определяемый полным набором переходных вероятностей $P\left(y/x\right)$ входных символов x в выходные y. Тогда существует основная характеристика этого канала C (названная К. Шенноном пропускной способностью). Теорема Шеннона гласит, что, если выполняется условие:

$$V_u < \frac{C \cdot V_k}{H(A)},$$

где V_u – скорость выдачи символов источником, а V_k – скорость передачи канальных символов, то существует такой способ кодирования/декодирования (т. е. преобразования последовательностей символов источника в последовательности символов канала и обратно), что при увеличении длин этих последовательностей, вероятность ошибки после декодирования стремится к нулю.

Если же это неравенство не выполняется, то такого способа кодирования не существует.

Таким образом, благодаря гениальной догадке Шеннона, было доказано, что при определённых условиях, можно получить сколь угодную надёжность связи, не изменяя параметров канала и не снижая скорости передачи информации!

До 1948 г. Большинство инженеров-связистов полагало, что повышение достоверности связи возможно только за счёт уменьшения скорости передачи (например, многократного повторения символов), за счёт увеличения мощности сигналов, или увеличения используемой полосы частот каналов связи.

Аналогичная теорема была сформулирована и доказана для непрерывного канала, определяемого своей полосой пропускания и отношением сигнал/шум, а также для непрерывных источников информации при среднеквадратической оценке верности передачи непрерывных сообщений.

Заметим, что теоремы Шеннона были «Теоремами существования», т. е. они доказывали факт существования желаемых методов кодирования/декодирования, но не указывали, как найти такие методы.

Результаты, доказанные Шенноном, актуальны и в настоящее время – действительно, цена мощности, полосы пропускания или временных затрат остаются высокими и сейчас, тогда как цена обработки сигналов (т. е. кодирования/декодирования) постоянно уменьшается из-за развития технологии микросхем и компьютеров.

Основные результаты К. Шеннона были сформулированы в его фундаментальной монографии «Работы по теории информации и кибернетике», переведенной в СССР Р. Л. Добрушиным и О. В. Лупановым с предисловием А. Н. Колмогорова в 1963 г.

На рисунке приведён автограф Шеннона с его наилучшими пожеланиями профессору Л. М. Финку во время лекции Шеннона в Ленинградском электротехническом институте связи (ЛЭИС) в СССР.

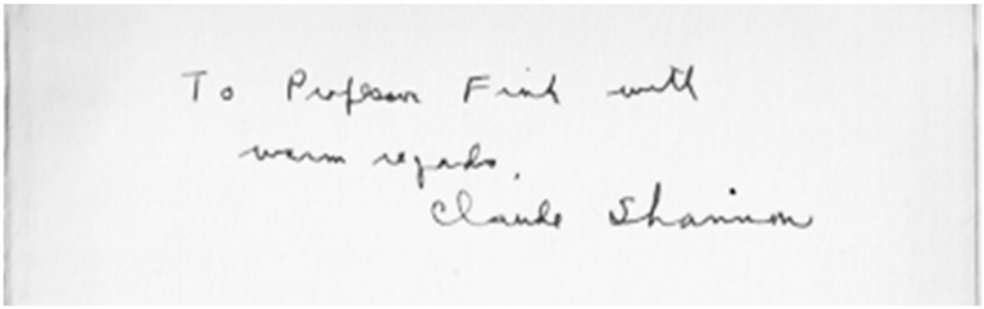


Рисунок. Автограф Шеннона с пожеланиями профессору Л. М. Финку

Направления развития теории информации в «пост-шенноновский период»

Математическое «устрожение» теорем кодирования было выполнено Добрушиным, Пинскером, Fano, Wolfowitz, Solomon, Thomas-Cover и другими.

Расчёт пропускных способностей различных каналов связи произведён Финком, Цыбаковым, Fano, Gallager, Csiszar.

Отыскание конструктивных методов кодирования/декодирования, приближающихся к потенциальному пределу Шеннона (*Slepian, Elias, Peterson, Gallager, Massey, Viterbi, Forney, Ziv, Sloan, Berger, Blahut, Verdu, Calderbank*, Финк, Зигангиров, Зяблов, Габидулин). Последние достижения в теории кодирования привели к тому, что реально используемые методы кодирования и декодирования уступают сейчас потенциальному энергетическому пределу Шеннона для ряда каналов связи, всего лишь на доли дБ! (Заметим, что в 1960–70 гг. первые два места в теории связи занимали американские и советские учёные).

4 Теория секретных систем (шифрования/дешифрования)

Необходимые и достаточные условия идеального шифрования были доказаны Шенноном для весьма общего вида шифра. Теорема Шеннона-Хеллмана [2] – дает возможность рассчитать расстояние единственности, то есть длину криптограммы, при которой сообщение может быть расшифровано единственным образом:

$$n_{pe} \sim N \Big/ \big(1 - H(M)\big).$$

Из этого условия следует, что все криптосистемы с «секретным ключом» могут быть взломаны при возможности перебора этого ключа.

Неравенство для количества информации в криптограмме о сообщении также предложил Шеннон:

$$I(E; M) \geq H(M) - H(K).$$

Из этого неравенства следует, что можно попытаться определить, что в данной криптограмме зашифровано именно данное сообщение даже для «невзламываемых» шифров.

«Пост-шенноновский» период теории секретных систем

Основной результат: A. Wyner (лауреат премии Шеннона) “Wire-tapchannelconcept” (1975).

Пусть имеется два канала – основной и «подслушивающий». Тогда при выполнении определённых условий можно при помощи специального рандомизационного кодирования обеспечить нулевую утечку информации

по каналу перехвата и надёжную передачу информации по основному каналу.

Дальнейшее развитие этого направления, получившего название “Keyless Cryptography” или “Physical-levelsecurity”, представлено в работах Csiszar, Alswede, Korner, Maurer, Wolf, Коржика, Яковлева.

Заключение

Из всего вышеизложенного можно видеть, что выдающийся американский учёный К. Шеннон является «Эйнштейном» теории связи, труды которого остаются актуальными и наш век цифровой связи.

Хотелось бы думать, что наши студенты, а также научные работники и преподаватели будут помнить славное имя Шеннона и передавать эти знания последующим поколениям инженеров-связистов.

Список используемых источников

1. http://www.itsoc.org/honors/claude-e-shannon-award

2. Коржик В. И., Просихин В. П., Яковлев В. А. Основы крипрографии : учеб. пособие; СПбГУТ. СПб., 2014. 276 с. ISBN 978-5-89160-097-3.

UDC 004; 621.398

HEURISTICS FOR AUTOMATIC VERIFICATION OF PAIRING–BASED CRYPTOGRAPHIC PROTOCOLS[3]

Harri Forsgren and Timo Karvi

University of Helsinki, Finland

We propose an automated method to aid the analysis of security protocols that use pairing-based cryptography. Our method is based on the constraint satisfiability problem. We start by presenting an algorithm to generate all the execution sequences and constraints, with or without an attacker. Then we define the normal forms of terms of various type and introduce a heuristic method to solve the constraints.

The same example protocol, Nalla’s identity-based tripartite authenticated key agreement protocol, is used in all these phases to describe our method. Finally, we estimate our method against many other erroneous identity-based key agreement protocols and propose further developments.

Nalla’s identity-based, agreement protocol, algorithm.

[3] Доклад оглашен на пленарном заседании IV Международной научно-технической и научно-методической конференции «Актуальные проблемы инфотелекоммуникаций в науке и образовании», состоявшейся в Санкт-Петербургском государственном университете телекоммуникаций им. проф. М. А. Бонч-Бруевича 3–4 марта 2015 г.

1 Introduction

There are many alternatives how to realize the automatic or semi-automatic security protocol verification. Tools can be general purpose such as Isabelle [1] or specifically designed for security proofs such as NRL Protocol Analyzer [2].

Our framework is based on constraint solving approach as described by Millen and Shmatikov [3]. A similar approach has been applied recently in [4] and [5].

Early verification methods were based on a Dolev-Yao model [6]. There the security of protocols relied only on a ”black box” encryption operation, which was assumed unbreakable, and on using simple encryption keys that have no structure from where to seek weaknesses. During the recent years, interest has grown to develop ways to find attacks by exploiting the algebraic properties of both the encryption method and the encryption keys generated during the protocol execution ([7], [3]). Cryptographic protocols based on elliptic curve pairings are one case where verification with only black box encryption – if even possible – is unlikely to bring much trust on security of the protocols in question.

We study in this paper how to extend the constraint solving method introduced by Millen and Shmatikov [3] to the analysis of simple cryptographic protocols utilizing elliptic curve cryptography. First, we give an example of the techniques and problems of this approach. After this, we consider the normal forms of the terms involved in pairing-based operations. Next, we consider how to solve the constraints generated during the verification of pairing-based protocols.

Our approach is heuristic. This means that the method does not guarantee a success. If flaws are not found, this does not mean that the protocol under analysis is correct. It only means that the protocol has no flaws, if the attacker uses terms whose size is under certain limit we have set in our analysis. However, practice has shown that if there is an attack, it is usually realized with modifications that do not increase the sizes of the original terms.

Our method is meant to be used by security protocol developers. When designing a new protocol, it is valuable, if developers can use a simple software with which to make first analyses. If these do not reveal mistakes, then it is possible to proceed to deeper and more complicated analyses or to formal proofs.

We have simulated our method manually and it has proved to be reliable in the sense that it has found all the mistakes mentioned in [8].

2 Basic Principles of the Automatic Constraint-Based Verification of Elliptic Curve Cryptographic Protocols

In this section, we introduce the constraints-based verification of cryptographic protocols, especially identity-based elliptic curve protocols.

We use a concrete example to clarify the basic principles and the technical problems.

2.1 Nalla's Protocol with Signatures

As an example, we use the protocol of Nalla ([9]), which is an identity-based key agreement protocol in an environment, where there is a single key generating authority, PKG. The PKG chooses the following system parameters and calculates the following private keys:

- G_1 is an additively denotated group of order q. Usually G_1 is the group of elliptic curve points;
- G_2 is a multiplicatively denotated cyclic group of the same order q. Usually it is the group of the roots of the unity used in elliptic curve pairings;
- $\hat{e}$: $G_1 \times G_1 \rightarrow G_2$ is a modified Weil pairing which is got from the ordinary;
- Weil pairing $e : G_1 \times G_1 \rightarrow G_2$ by the formula $\hat{e}(P,Q) = e(P, \Phi(Q))$, where $\Phi: G_1 \rightarrow G_1$ is an automorphism of G_1;
- P is a random generator of G_1, chosen by PKG;
- $H1 : \{0, 1\}^* \rightarrow G_1$ and $H2 : G_1 \rightarrow Z_q^*$ are hash functions;
- $s \in Z_q^*$ is a master key, randomly chosen by the PKG;
- $P_{pub} = sP$ is the public key of PKG;
- $Q_{ID} = H_1(ID)$ is the public key of the identity ID, computed by PKG;
- $S_{ID} = sQ_{ID}$ is the private key of ID, computed by PKG and sent via a secure channel to ID.

The PKG publishes its public parameters G_1, G_2, P, P_{pub}, H_1 and $\hat{e}$ (or e). Consider now the situation, where three entities A, B and C, belonging to PKG, agree about the session key. The protocol of Reddy and Nalla proceeds as follows. First, A chooses its ephemeral key $a \in Z_q^*$. Similarly, B and C choose $b \in Z_q^*$ and $c \in Z_q^*$, respectively. Then the messages are sent:

1. $A \rightarrow B,C : P_A = aP,\ T_A = a^{-1}(H_2(P_A)S_A)$.

2. $B \rightarrow A,C : P_B = bP,\ T_B = b^{-1}(H_2(P_B)S_B)$.

3. $C \rightarrow A,B : P_C = cP,\ T_C = c^{-1}(H_2(P_C)S_C)$.

After the messages are exchanged, the participants verify the messages. A computes $e(P_B, T_B)e(P_C, T_C)$ and $e(P_{pub}, H_2(P_B)Q_B + H_2(P_C)Q_C)$ and verify that they are equal.

After a successful verification, A computes the session key:

$$K_A = e(P_B, P_C)^a.$$

Similarly B and C compute the keys:

$$K_B = e(P_A, P_C)^b \text{ and}$$

$$K_C = e(P_A, P_B)^c.$$

It can be seen that $K_A = K_B = K_C$. We denote the shared session key as K_{ABC}.

2.2 Nalla's Protocol as a Constraint Sequence

We continue with our example protocol. Figure shows a small part of the, generated constraint sequence tree.

We have labelled the arrows. For example, $-B : (P_{AB}, T_{AB})$ means that B receives a pair (P_{AB}, T_{AB}). In this case, the received units may be either those units A has sent or some other units the enemy has sent. During the generation phase, we leave this open and represent the received units by variable, in this case by variables P_{AB} and T_{AB}. Similarly, $+C : (P_C, T_C)$ means that C sends two units of data.

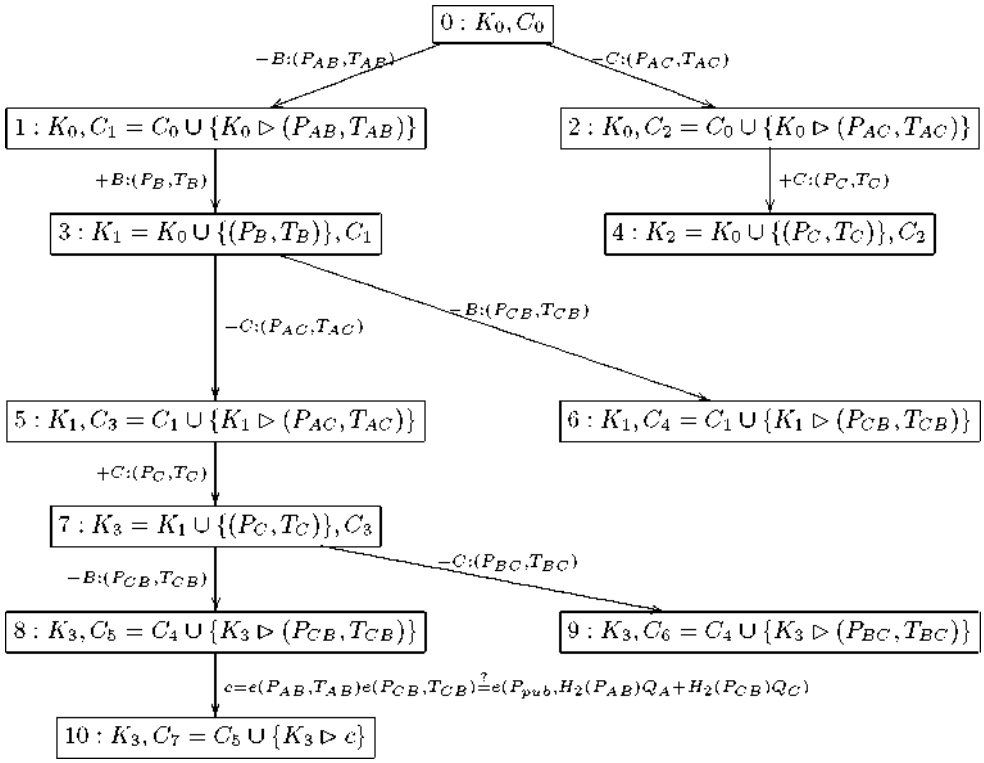


Figure. Part of Nella key-exchange protocol with signatures execution tree

At the same time with the development of the tree the knowledge sets and constraints are formed. First, we must determine the attacker's initial knowledge set K_0. It consists of the public parameters of the PKG and a random value $a_I \in Z_q^*$ (I means "intruder"). The random value a_I is useful, because the attacker can use it in modifying or generating messages. Moreover, we must give to the attacker enough constants so that he can generate his own terms needed in a protocol. Here we take only one constant in order to restrict the sizes

of the sets, but when using computers we can generate more constants to the attacker. Thus

$$K_0 = \{a_I, P_{pub}, P, Q_A, Q_B, Q_C.$$

Our model does not have parallel communication. Everything is serialized, so at first there are two possibilities: either B receives a message sent by the intruder or C receives the same message. Here P_{AB}, T_{AB}, P_{AC} and T_{AC} are variables and the values they are substituted for come from the intruder's knowledge. However we do not solve the variables now, but we create a constraint $K_0 \triangleright (P_{AB}, T_{AB})$ to be solved later. After B has received a message, it sends its response. The response message is added to the intruder's knowledge $K_1 = K_0 \cup \{(P_B, T_B)\}$.

The constraint sequence we are going to solve here consists of constraints C_0, C_1, C_3, C_5 and C_7. We can now list the tasks to be solved before the method can be applied automatically.

– Terms, especially ground terms (i.e. terms not containing variables), should have normal forms. There should be rewrite rules, which transform terms into normal forms.

– Generally, solving the constraints is based on unification. Both syntactic and equational unification is applied. It is also possible to proceed heuristically trying to substitute various terms for variables, in which case some constraints can be solved, some not.

– How to represent the received terms. In the previous example, we used a variable to represent a term, which was received. It is, however, sometimes possible to make assumptions about the structure of the received terms. This must be taken into account when designing the specification language for security protocols.

– How to decide, if the protocol has a flaw. In our example, it is natural to just to check if the equation can be solved. If this is the case, then this shows that an intruder can send his own or public parameters and the other participants believe that they come from A. In other situations, one participant should sign or encrypt a message chosen by him, and the attacker can then try to deduce this message from his knowledge.

Our method will be heuristic. This means that the method does not quarantee the verification or detection of flaws, but it can be used in the design process. If the method does not find a flaw, then there are good reasons to believe that the analyzed protocol is correct and it is time to proceed to formal proofs or more complicated verification techniques.

3 Normalization of Points and Pairing Forms on Elliptic Curves

Consider a typical setting using identity-based encryption. We have a finite, abelian, and additively denotated group G_1 and a pairing $\hat{e}$: $G_1 \times G_1 \rightarrow G_2$,

where G_2 is usually a multiplicatively marked cyclic group. We choose the pairing to be a modified Weil pairing. In order to be able to manipulate the symbolic terms created by an identity-based security protocol, we must develop rewriting rules and normal forms for the elements in G_1 and in G_2 as well as for pairings and various expressions. Expressions may contain natural number symbols, variables, and function symbols (for example hash functions). Moreover, exponents or coefficients may be integers or natural numbers and in a protocol they could be added or multiplied. Thus, we need normal forms and rewriting rules for numbers as well.

The group *G1* is usually of the form *E[n],* i. e. it is a torsion group of elliptic curve points. Thus an element in G_1 is represented by a point on the elliptic curve E. The neutral element is represented by an infinite point O. If a and b are integers or elements in a finite field, we use the notation $a \cdot b$ or $a \times b$ for the multiplication between integers. If P is an elliptic curve point and a is an integer, we denote by $a.P$ the multiplication of P by a.

We try to transform an expression of elliptic curve points into O or:

$$\sum_{i=1}^{m} a_i.P_i + \sum_{j=1}^{n} b_j.X_j + \sum_{k=1}^{p} f_k.(A_k),$$

where a_i and b_j are natural number expressions, $P_i \neq O$ for all i, $P_i \neq P_j$ if $i \neq j$, X_j are variable symbols, and f_k are function symbols on some arguments A_k. In some applications, a_i and b_i may be expressions containing not only natural numbers, but integers or elements from a finite field. In applications, f_k*'s* are often hash functions.

Next, we develop term rewriting systems for finite fields and elliptic curve point expressions as well as for expressions containing pairings. The rules for integer expressions can be deduced from finite field expressions which contain only addition, substraction, and multiplication.

The finite field expressions are defined as follows. Let A be a set of symbolic elements, V a set of variables, *0* and *1* constants. The operators are $+$, $-$, $\times$, and *inv*. Term can be built in a normal way using this signature. We write usually $-a$ (inverse with respect to addition) and a^{-1} (inverse with respect to multiplication) instead of *inv(a).*

We transform the finite field (and integer) expressions into the following form,

$$t_1 + t_2 + \cdots + t_n,$$

where there are no + in t_i's.

In order to get the finite field and elliptic curve point expressions into a normal form, we have the rewrite rules of Table 1, where a and b are elements in a finite field, finite field variables or finite field functions, and P and Q are point symbols, point variables, or point functions. It is assumed that there is an order between the integer symbols, variables and functions as well as between the point symbols, variables and functions. We can prove

Theorem 1. *The rewriting systems in Table 1 terminate*

Proof: The proof is based on polynomial orders. The details will appear in the fuller version of this paper.

TABLE 1. Normalization rules for elements in a finite field and elliptic curve points, respectively

$$a + 0 \to a,$$
$$0 + a \to a,$$
$$a + (-a) \to 0,$$
$$(-a) + a \to 0,$$
$$-(-a) \to a,$$
$$-(a + b) \to (-a) + (-b),$$
$$1 \times a \to a,$$
$$a \times 1 \to a,$$
$$a \times a^{-1} \to 1,$$
$$(a^{-1})^{-1} \to a,$$
$$(a \times b)^{-1} \to a^{-1} \times b^{-1},$$
$$a \times (b + c) \to (a \times b) + (a \times c),$$
$$(a + b) \times c \to (a \times c) + (b \times c),$$

$$0.P \to O,$$
$$1.P \to P,$$
$$a.O \to O$$
$$P + O \to P,$$
$$O + P \to P,$$
$$a.(b.P) \to (a \cdot b).P,$$
$$a.(P + Q) \to a.P + b.Q,$$
$$a.P + b.P \to (a + b).$$

Of the functions, we consider only the normal forms of pairings. Other functions are either simple, as hash functions, or very protocol-specific. The normal form for pairing expressions is:

$$\prod_{i \in I} \prod_{j \in J} e(P_i, P_j)^{a_{ij}},$$

where the symbols a_{ij} represent terms of integers or integer variables. The *terms* $(P_i, P_j)^{a_{ij}}$ are in the alphabetical order, first with respect to P_1 and P_j , and then with respect to the exponents.

The rules in Table 2 normalize the terms of the form $\hat{e}\ (P,Q)$, where $\hat{e}$ is the modified Weil pairing and P and Q are terms representing points on an elliptic curve. The symbols *a, b,* and *c* represent integer expressions. We assume that the symbols can be arranged in some order (alphabetical, for example). This order extends naturally to the order of terms. On the right there are the normalization rules for the expressions of the elements in G_2 which is a multiplicatively denotated cyclic group.

TABLE 2. Normalization rules for pairings and cyclic group G2, respectively

$$\hat{e}\ (aP,Q) \to \hat{e}\ (P,Q)^a,$$
$$\hat{e}\ (P, aQ) \to \hat{e}\ (P,Q)^a,$$
$$\hat{e}\ (P_1 + P_2,Q) \to \hat{e}\ (P_1) \cdot \hat{e}\ (P_2,Q),$$
$$\hat{e}\ (P,Q_1 + Q_2) \to \hat{e}\ (P,Q_1) \cdot \hat{e}\ (P,Q_2),$$

$$a^0 \to 1,$$
$$a^1 \to a,$$
$$1 \cdot a \to a,$$
$$a \cdot 1 \to a,$$
$$(a^m)^n \to a^{mn},$$
$$a^m a^n \to a^{m+n},$$
$$(ab)^n \to a^n b^n.$$

Theorem 2. *The rewriting systems in Table 2 terminate*

Proof: The proof is based on deduction orders. The details will appear in the fuller version of this paper.

4 Solving the constraints

Consider now the constraint:

$$K_3 \triangleright e(P_{AB}, T_{AB})e(P_{CB}, T_{CB}) = e(P_{pub}, H_2(P_{AB})Q_A + H_2(P_{CB})Q_C).$$

Here, symbols P_{AB}, T_{AB}, P_{CB} and T_{CB} are variables. We can simplify the task by assuming that the attacker modifies only *A*'s data. If this assumption does not lead to a solution, we can check other cases where the attacker modifies *B*'s and *C*'s data, too.

Our assumption implies that:

$$P_{CB} = P_C,\ T_{CB} = c^{-1}(H_2(P_C)S_C).$$

So we must determine the values of P_{AB} and T_{AB}. Remember that:

$$K_3 = \{\pm a_I^{-1},\ \pm a_I,\ \pm P_{pub},\ \pm P,\ \pm Q_A,\ \pm Q_B,\ \pm Q_C, \pm P_B,\ \pm T_B,\ \pm P_C,\ \pm T_C\},$$

where we have divided or modified the terms known to the attacker into the basic terms using the inference rules in Table 3. We proceed by trying systematically all the terms constructed from the elements of K_3. In the constructions, we apply the inference rules in Table 3. After substituting terms for variables P_{AB} and T_{AB}, we normalize both sides of the equation and then compare them. We start by constructing term classes $T_0, T_1, T_2, \cdots$, where T_{i+1} represent terms that contain one operation more than the terms in T_i. It is clear that the sizes of the classes increase very fast. This means that we cannot proceed to terms that are large. On the other hand, experience has shown that if a security protocol is flawed, attacks use only normal size terms and the normal sizes tend to be quite manageable in our approach.

TABLE 3. Intruder's inference rules

Member $\overline{T \cup \{t\} \vdash t}$	Pairing $\frac{T \vdash t \ T \vdash u}{T \vdash t(t,u)}$ P
Encryption $\frac{T \vdash t \ T \vdash k}{T \vdash E(k,t)}$ E	Unpairing $\frac{T \vdash (t,u)}{T \vdash t} \ \frac{T \vdash (t,u)}{T \vdash u}$ UL, UR
Decryption $\frac{T \vdash E(k,t) \ T \vdash k}{T \vdash t}$ D	Function $\frac{T \vdash t}{T \vdash f(t)}$ F
Inversion	Multiplication

$$\frac{T \vdash t}{T \vdash t^{-1}}\ \mathrm{I}$$

Point addition

$$\frac{T \vdash P \quad T \vdash Q}{T \vdash P+Q}\ \mathrm{PA}$$

EC pairing

$$\frac{T \vdash a.P \quad T \vdash b.Q \; T \vdash c}{T \vdash e(P,Q)^{abc}}\ \mathrm{EP}$$

$$\frac{T \vdash t_1 \ldots T \vdash t_n}{T \vdash t_1 \ldots\ldots t_n}\ \mathrm{M}$$

Scalar multiplication

$$\frac{T \vdash a \quad T \vdash P}{T \vdash a.P}\ \mathrm{PM}$$

In our example, we have the following class sizes:

T_0: basic terms, 18 elements, if we consider both a term and its additive inverse.
T_1: terms with one operation, 207 elements.
T_2: terms with two operations are one of the types $P+Q+R$, $a.P+Q$, $H_2(P).Q$, $a.b.P$, altogether a little more than 2000 elements.
T_3: terms with three operations, about 15000 elements.

We notice that the number of terms increases very fast, but for the classes T_2 and T_3 the sizes are still manageable. There is furthermore a possibility to restrict the knowledge set K_3. We have assumed that the attacker does not modify B's and C's packets. This gives a reason to believe that the knowledge set:

$$K_0' = \{\pm a_I\,,\ \pm a_I^{-1},\ \pm P_{pub},\ \pm P,\ \pm Q_A\}$$

might be sufficient. This arrangement would reduce the number of terms sharply.

As for our protocol example, level T_3 terms are sufficient (even level T_2, if we take the structure of T_A into account). If we test the substitutions:

$$\mathrm{P_{AB}} = -\mathrm{a_I P_{pub}},\ \mathrm{T_{AB}} = a_I^{-1}(\mathrm{H_2(P_{AB})\cdot Q_A}),$$

the constraint $K_3 \triangleright \mathrm{c}$ has a solution and a non-trivial man-in-the-middle attack has been found. Notice that the constraint has also a solution with $P_{AB} = P_{pub}$ and $a_I = 1$, but this attack is easily repelled and that is why it cannot be considered as a real attack.

Shim has shown a very similar attack ([10]), but she used different attacker's constants which make the attack to work only when ordinary Weil pairing is used. With our constants, the attack works also with respect to the modified Weil pairing.

5 Analysis of some other protocols

We have checked possibilities to analyze the erroneous protocols mentioned in [8]. These protocols are Zhang-Liu-Kim [11], Nalla-Reddy [12], and Shim-Woo [13]. In addition, the protocol in [14] has been included (see also [15]). The execution tree is in all these examples quite small with depth less

than 5 and with modest branching. So in order to evaluate our method, the main criteria is the sizes of the terms.

Zhang-Liu-Kim's protocol has a flaw that allows a man-in-the-middle attack against participants. The terms sent by the participants belong to class T_5. It would be a hard task to generate them all. However, the attacker modifies only the arguments in the terms. If the analysis is started by keeping the form of the terms intact and modifying only the arguments, the complexity of the terms reduces considerably. In this case, the attack is found by testing only terms in T_2, a trivial task for a computer.

Nalla-Reddy is a protocol family consisting of three protocols ID-AK-1, ID-AK-2, and ID-AK3. There are passive attacks against ID-AK-2 and ID-AK-3 and thus it is not necessary for the attacker to modify terms, but he can use just the terms in his knowledge sets. For ID-AK-1, there is a man-in-the-middle attack and it necessary to use only terms in T_1.

The same is true for the rest of our test protocols. So the heuristic method seems to detect all the errors in these protocols and it would be a useful aid for protocol designers.

6 Conclusions and Further Research

We have presented a heuristic method to analyze identity-based key agreement protocols. The heuristics generates first an execution tree and adds to every branch of this tree knowledge and constraint sets. The constraints are solved by trying systematically to substitute bigger and bigger terms for variables. It is evident that we cannot increase the sizes of terms very much, but even with reasonable small terms, we can find mistakes. Our method is meant to help protocol designers to detect errors early, before publishing their results or before proceeding to formal proofs or more complicated analysis methods. The need for this kind of software is evident, if we have followed publications on identity-based security algorithms. It seems that more than half of the presented algorithms have errors. Some of these errors could be found by deeper analyses, but a simple automatic or interactive tool would be of great help.

Our next step is develop basic software, which uses our method. This would make it possible to understand the real capacity of this method. Our method is easily parallelizable. After the basic implementation we are planning to extend our program so that it can be run in a powerful computer cluster. This would make it possible test quite large terms so that most practical mistakes are found.

References

1. Nipkow T., Paulson L. C., Wenzel M. Isabelle / HOL – A Proof Assistant for Higher-Order Logic. Vol. 2283 of LNCS. Springer, 2002.

2. Meadows C. The NRL protocol analyzer: An overview // Journal of Logic Programming, 1996, 26 (2), pp. 113–131.

3. Millen J., Shmatikov V. Symbolic protocol analysis with an Abelian group operator or Diffie-Hellman exponentiation // Journal of Computer Security, 2005, 13 (3), pp. 515–564.

4. Schmidt B. Formal Analysis of key Exchange Protocols and Physical Protocols. PhD thesis, ETH Zurich, 2012.

5. Meier S. Advancing Automated Security Protocol Verification. PhD thesis, ETH Zurich, 2013.

6. Dolev D., Yao A. C. On the security of public key protocols // IEEE Transactions on Information Theory, 1983, 29 (2), pp. 198–208.

7. Shmatikov V. Decidable analysis of cryptographic protocols with products and modular exponentiation.13th European Symposium on Programming (ESOP ’04). Vol. 2986 of LNCS. Springer-Verlag, 2004, pp. 355–369.

8. H¨olbl M., Welzer T., Brumen B. Comparative study of tripartite identity-based authenticated key agreement protocols // Informatica, 2009, 3 (3), pp. 347–355.

9. Nalla D. ID-based tripartite key agreement with signatures. Cryptology ePrint Archive, Report 2003/144, 2003.

10. Shim K. Cryptanalysis of ID-based tripartite authenticated key agreement protocols. Cryptology ePrint Archive, Report 2003/115, 2003.

11. Zhang F., Liu S., Kim K. ID-based one-round authenticated tripartite key agreement protocol with pairings. Cryptology ePrint Archive, Report 2002/122, 2003.

12. Nalla D., Reddy K. ID-based tripartite key agreement with signatures. Cryptology ePrint Archive, Report 2003/004, 2003.

РАДИОТЕХНОЛОГИИ СВЯЗИ

УДК 621.396.67

ПРОЕКТИРОВАНИЕ МИКРОПОЛОСКОВОГО ЭЛЛИПТИЧЕСКОГО ПОЛОСНО-ПРОПУСКАЮЩЕГО ФИЛЬТРА СО СТРУКТУРОЙ ИЗ ДВУХ РЕШЕТОК ОДИНАКОВОЙ ЭЛЕКТРИЧЕСКОЙ ДЛИНЫ

Ф. С. Авгари

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

В статье рассмотрены вопросы проектирования структур, состоящих из двух параллельно соединенных решеток, связанных многопроводных линий одинаковой длины, которые являются одними из самых компактных структур с нулями передачи на конечных частотах. В процессе исследований используется линейное преобразование емкостной матрицы, которое позволяет получить удобные для реализации геометрические размеры структуры.

эллиптический фильтр, полосно-пропускающий фильтр, прототип, СВЧ-устройства, сосредоточенная емкость, закороченная линия, преобразование емкостных матриц, многопроводная линия.

Эллиптические фильтры СВЧ обладают большей частотной избирательностью по сравнению с фильтрами Чебышёва или Баттерворта. Для реализации полосно-пропускающих характеристик эллиптических фильтров используются несколько различных структур. Одной из самых компактных структур с нулями передачи на конечных частотах является структура на связанных многопроходных линиях (рис. 1*а*). Известно, что решетка связанных резонаторов реализует полиномиальные характеристики (гребенчатые и встречно-стрежневые цепи). Для получения нулей передачи было предложено параллельное соединение двух решеток. На рис. 1*б* показан прототип, в котором резонансные контуры разделены так, что получилось две лестничные цепи из элементов *L* и элементов *C*. Они имеют общие узлы 1–4. Известно, что индуктивная лестничная цепь реализуется решеткой закороченных отрезков связанных линий, а емкостная – решеткой разомкнутых линий. Если теперь эти две решетки соединить параллельно в узлах 1–4, то получится структура, показанная на рисунке 1*в*. Эта структура имеет реализуемые геометрические размеры только при высоких нагрузках. В закороченной решетке добавляются трансформирующие входные линии.

Приведенная структура используется для реализации характеристик ППФ с полосой пропускания выше 5 %. Для более узких полос начинают резко связываться сосредоточенные емкости разомкнутых концов линий решетки, коррекция которых, как правило, удовлетворительных результатов не дает. Первая паразитная полоса пропускания рассматриваемой структуры зависит от электрической длины резонаторов и находится приблизительно в диапазоне $(2\omega_0 - 5\omega_0)$. Однако требуется тщательная коррекция неоднородностей, чтобы убрать узкие паразитные полосы, которые появляются всегда в районе частоты $2\omega_0$. При проектировании структуры, показанной на рисунке 1*а*, возможно проведение линейного преобразования матриц нормированных статических емкостей решеток, которое позволяется в достаточно широких пределах изменить геометрию связанных линий. Недостатком этой структуры при реализации на НПЛ является наличие заземленных линий, что усложняет технологию изготовления.

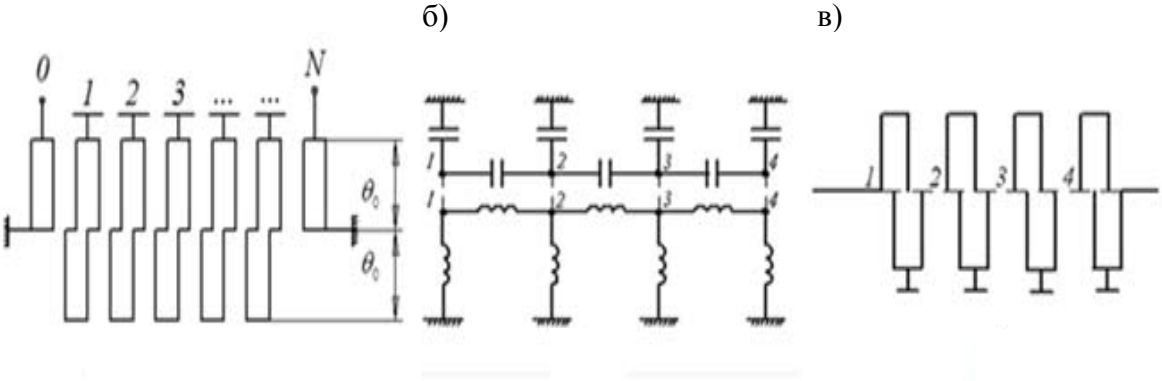


Рис. 1. Структуры из параллельно соединенных двух решеток, связанных многопроводных линий одинаковой длины и реализация прототипа с полюсами затухания параллельным соединением двух решеток, связанных многопроводных линий

Расчет полосковой структуры, состоящей из параллельного соединения двух решеток, связанных многопроводных линий одинаковой длины

Общий вид рассматриваемой структуры, имеющей характеристику затухания с полюсами на конечных частотах, показан на рисунке 1*а*. Методика расчета этой цепи проводится на основе прототипа НЧ, параметры которого $L_i^{'}$, $C_i^{'}$ найдены по тем или иным требованиям к характеристикам (рис. 2*а*).

1. Задаются электрической длиной резонаторов $\frac{\pi}{6} \le \theta_0 \le \frac{\pi}{3}$.

Чем больше θ_0, тем лучше физическая реализуемость структуры. Но при этом увеличиваются габариты и первая паразитная полоса пропус-

кания приближается к $2f_0$. Чем меньше θ_0, тем больше усложняется реализуемость структуры. Но при этом уменьшаются габариты и удаляется первая паразитная полоса пропускания к $5f_0$ [1]. На практике, если нет особых требований к структуре и ее характеристике, выбирают $\theta_0 = \frac{\pi}{4}$; паразитная полоса при этом будет на $3f_0$.

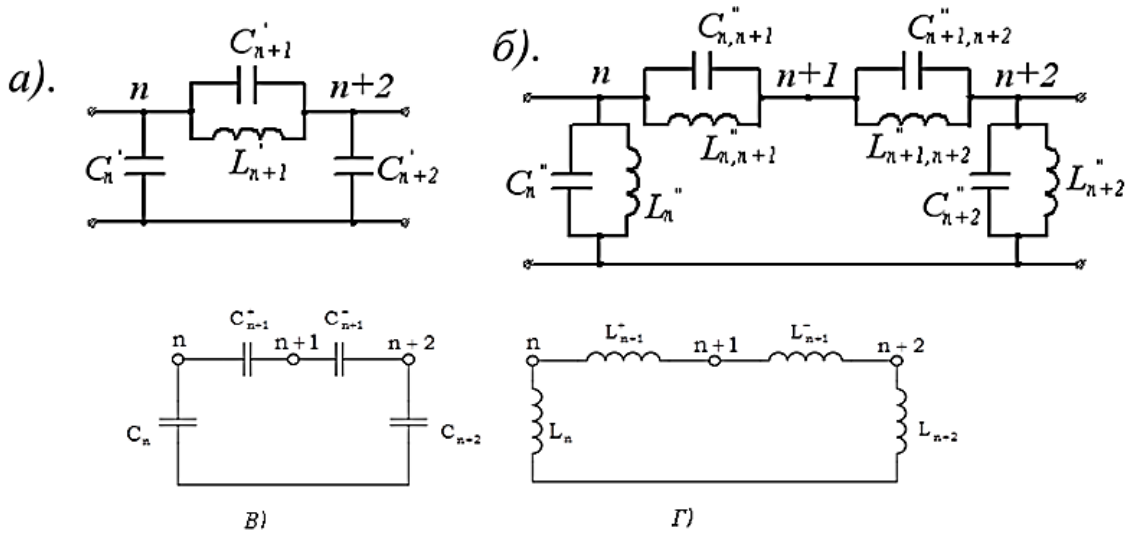


Рис. 2. Переход от прототипа НЧ к решеткам связанных линий

2. Постоянная двойного частотного преобразования Ричардса

$$a = \frac{tg\theta_0 \cdot tg\theta_0 \dfrac{f_1}{f_0}}{tg^2 \dfrac{f_1}{f_0} - tg^2\theta_0},$$

где f_1 – верхняя граничная частота полосы пропускания.

3. Вспомогательные коэффициенты

$$m_{n+1}^{\pm} = a\left\{1 + \left[\sqrt{(\frac{\Omega_{n+1}}{2a})^2 + 1} \pm \frac{\Omega_{n+1}}{2a}\right]^2\right\}, \text{ где } \Omega_{n+1} = \frac{1}{\sqrt{C_{n+1}^{'} L_{n+1}^{'}}}.$$

4. Нормированные значения элементов прототипа ППФ (рис. 2*б*).

$$C_n^{''} = \frac{aC_n^{'}}{tg\theta_0};\ L_n^{''} = \frac{1}{aC_n^{'} tg\theta_0};\ C_{n,n+1}^{''} = \frac{C_{n+1}^{'} m_{n+1}^{-}}{tg\theta_0};\ L_{n,n+1}^{''} = \frac{1}{C_{n+1}^{'} m_{n+1}^{+} tg\theta_0};$$

$$C_{n+1,n+2}^{''} = \frac{C_{n+1}^{'} m_{n+1}^{+}}{tg\theta_0};\ L_{n+1,n+2}^{''} = \frac{1}{C_{n+1}^{'} m_{n+1}^{-} tg\theta_0};\ C_{n+2}^{''} = \frac{aC_{n+2}^{'}}{tg\theta_0};\ L_{n+2}^{''} = \frac{1}{aC_{n+2}^{'} tg\theta_0}.$$

5. Нормировочный коэффициент $K_0 = \frac{120\pi}{R}$.

6. Элементы матрицы нормированных статистических ёмкостей короткозамкнутой решетки связанных линий $[C]_{\text{КЗ}}$ (рис. 2*в*).

7. Элементы матрицы нормированных статистических ёмкостей разомкнутой решетки связанных линий $\left[\tilde{C}\right]_{XX}$ (рис. 2*г*).

8. Линейное преобразование матриц: необходимо выбрать $n_0 = n_{N+1} = 1$. Остальные коэффициенты n_i произвольны и выбираются из условия физической реализуемости структуры [1]. Пределы реализуемости связанных линий на НПЛ с подложкой $\varepsilon = 9,6$. Нормированные емкости на землю выходных линий $9 \geq C_{00} \geq 3$. Нормированные емкости связи $3 \geq C_{i,i+1} \geq 0,8$. Нормированные емкости на землю внутренних связанных линий $7 \geq C_i \geq 1,5$.

9. В результате линейного преобразования матриц должна быть получена лестничная емкостная цепь с реализуемыми значениями $C_{i,i+1}$ и C_i. Для структуры на НПЛ все узлы должны иметь емкость на землю.

10. Геометрические размеры связанных линий и эффективные диэлектрические проницаемости определяются по методикам, изложенным в [2, 3].

11. Длина линий решетки $l = \frac{1,5 \cdot 10^{11}}{\pi f_0 \sqrt{\varepsilon_{\text{эфф}}}} \theta_0$.

Пример. Рассчитать геометрические размеры (табл.) структуры на НПЛ с $\varepsilon = 9,6$, реализующей характеристику ППФ Золотарева-Кауэра. Прототип приведен на рис. 3*а*. Значения элементов прототипа: $C_1' = 0,7486$; $C_2' = 0,0374$; $C_3' = 0,7486$; $L_2' = 1,0213$. Сопротивления нагрузок R = 50 Ом, центральная частота ПЭП f_0 = 3 ГГц. Эскиз структуры показан на рис. 3*б*.

1. $\theta_0 = \frac{\pi}{4}$.

2. $a = \frac{tg\theta_0 \cdot tg\theta_0 \frac{f}{f_0}}{tg^2\theta_0 \frac{f}{f_0} - tg^2\theta_0} = 12,73885.$

3. $\Omega_2 = \frac{1}{\sqrt{L_2' C_2'}} = \frac{1}{\sqrt{1,0213 \cdot 0,0374}} = 5,117.$

Значения нормированных емкостей короткозамкнутой решетки с трансформирующими линиями приведены на рис. 3*в*. Значения нормированных емкостей разомкнутой решетки приведены на рис. 3*г*.

ТАБЛИЦА. Значения геометрических размеров

$\frac{W_0}{h}=0,75$	$\frac{W_1}{h}=0,89$	$\frac{W_2}{h}=1,23$	$\frac{W_3}{h}=0,7$	$\frac{W_4}{h}=0,75$	$\frac{W_1'}{h}=0,72$	$\frac{W_2'}{h}=1,4$	$\frac{W_3'}{h}=0,7$
$\frac{S_{01}}{h}=0,33$	$\frac{S_{12}}{h}=0,6$	$\frac{S_{23}}{h}=0,36$	$\frac{S_{34}}{h}=0,325$		$\frac{S_{12}'}{h}=0,33$	$\frac{S_{23}'}{h}=0,67$	
$\frac{1}{\sqrt{(\varepsilon_{эфф})_{КЗ}}}=0,372$, $l_1==4,65$ мм					$\frac{1}{\sqrt{(\varepsilon_{эфф})_{ХХ}}}=0,38$, $l_2==4,75$ мм		

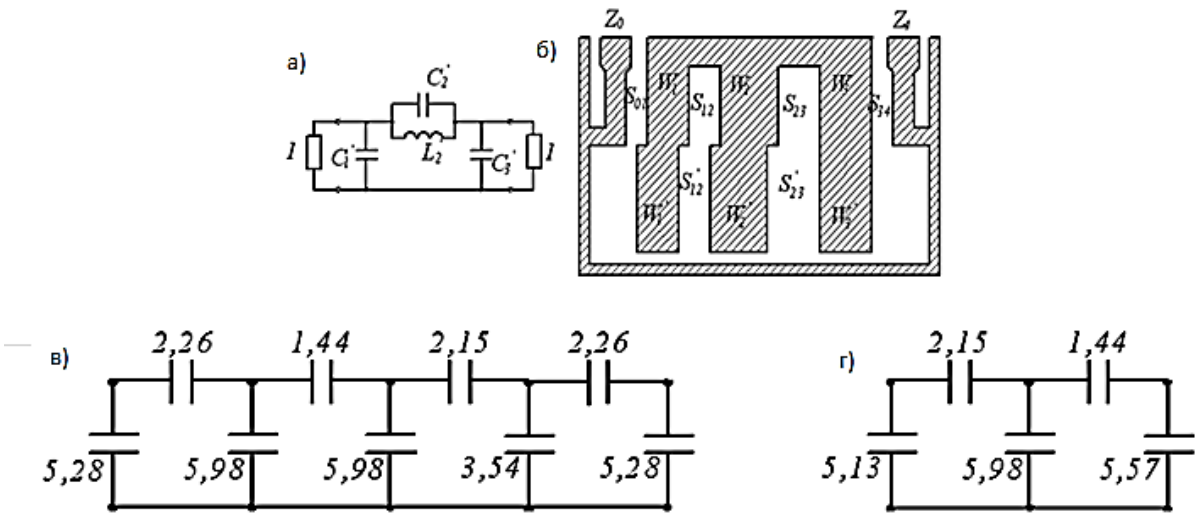


Рис. 3. Полосковая структура из двух решеток одинаковой длины

Список используемых источников

1. Кубалова А. Р., Томашевич С. В. Анализ и синтез микроволновых эллиптических фильтров; СПбГУТ. – СПб., 2013. – 368 с. ISBN 978-5-89160-089-8.

2. Мазепова О. И. и др. Справочник по элементам полосковой техники / под ред. Фельдштейна А. Л. М. : Связь, 1979. 336 с.

3. Леонченко В. П., Фельдштейн А. Л., Шепелянский Л. А. Расчет полосковых фильтров на встречных стержнях. М. : Связь, 1975. 312 с.

Статья представлена научным руководителем, доктором технических наук, профессором С.В. Томашевичем.

УДК 621.396.93

АНАЛИЗ МЕХАНИЗМОВ БАЛАНСИРОВКИ НАГРУЗКИ В ГЕТЕРОГЕННЫХ СЕТЯХ СТАНДАРТА LTE

Х. А. Аль-Амери, А. Н. Степутин

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

Построение гетерогенной сети позволяет увеличить пропускную способность сети и расширить зону её покрытия. Однако абонентская нагрузка в гетерогенных сетях LTE распределена по зоне обслуживания сети неравномерно. Существующие механизмы балансировки нагрузки, описанные в спецификациях 3GPP, не решают данные проблемы в полной мере. В данной статье рассматривается механизмы балансировки нагрузки в мультисервисных гетерогенных сетях стандарта LTE.

LTE, гетерогенные сети, балансировка нагрузки, технология CRE, eICIC, CoMB.

Гетерогенная сеть (HetNet) может включать в себя следующие типы базовых станций (БС): макро-БС, микро-БС, пико-БС и фемто-БС [1]. Это позволяет увеличить пропускную способность сети и расширить зону ее покрытия, а также предоставлять услуги пользователям по более низкой цене и с лучшим качеством. Структура гетерогенных сетей при использовании маломощных узлов показана на рисунке 1.

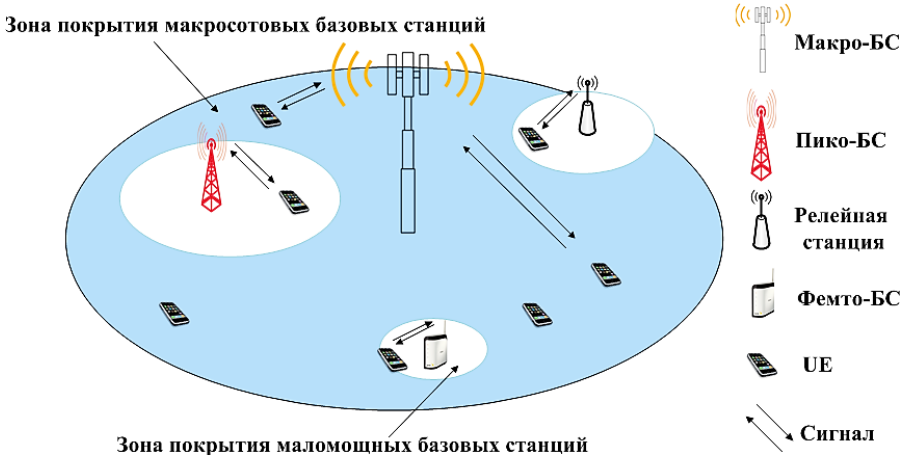


Рис. 1. Развёртывание гетерогенных сетей при использовании маломощных узлов

Типовые характеристики БС HetNet стандарта LTE приведены в таблице 1.

Неравномерное распределение абонентов в реальных сетях приводит к перегрузке одних базовых станций и простою других. Балансировка нагрузки между базовыми станциями БС гетерогенной сети позволяет увеличить производительность и эффективность сети. В сетях LTE для каждого

абонентского терминала (*User Equipment*, UE) определены два состояния: активный режим *(Connected Mode*) и режим ожидания *(Idle Mode)*. Рассмотрим в отдельности балансировку распределения трафика в каждом состоянии.

ТАБЛИЦА 1. Характеристики базовых станций LTE

Типы узлов	Мощность передатчика, дБм	Зона покрытия	Расположение	Число абонентов	MIMO
Макросота	46	< 40 км	вне здания	до 1000	2×2, 4×4
Микросота	30–37	< 2 км	вне здания	до 200	2×2, 4×4
Пикосота	23–30	< 300 м	внутри или вне здания	до 100	2×2
Фемтосота	< 23	< 50 м	внутри здания	до 16	2×2

Балансировка нагрузки UE в режиме ожидания

Перераспределение трафика в режиме ожидания осуществляется с помощью реселекций сот и включает в себя пользователей, которые не требуют сетевых ресурсов. Абонентские терминалы UE самостоятельно выполняют реселекцию от одной соты к другой в соответствии с параметрами, которые передаются в системной информации (значений гистерезиса, приоритеты позиционирования абонента, и т. д.) [2]. Условие реселекции сот можно записать в виде следующего неравенства:

$$R_s = Q_{meas,s} + Q_{Hyst},$$
$$R_n = Q_{meas,n} - Q_{Offset}, \quad (1)$$

где R_s – для обслуживающей соты, а R_n – для соседней соты. Переключение на соседнюю соту происходит, если $R_n > R_s$, Q_{meas} – уровни измеренных сигналов соответствующих сот. Для устранения множественных переключений на границах сот в (1) введен запас между двумя пороговыми уровнями измеренных сигналов, называемый гистерезисом Q_{Hyst}, а в параметры соседней соты Q_{Offset}. Цель этого параметра – избежать многократную нежелательную передачу UE от одной БС к другой. Оператор также регулирует минимальные временные интервалы между последующими переключениями.

При этом следует учитывать, что частая реселекция сот приводит к более быстрому расходованию аккумуляторной батареи UE.

Балансировка нагрузки UE в активном режиме

Мобильность абонента в радиосетях обеспечивается за счет процедуры хэндовера, которая позволяет переключить обслуживание абонентского терминала UE с одной БС на другую в процессе разговора. Хэндовер между

соседними сотами одной технологии называется горизонтальным (внутрисистемным), хэндовер между разными уровнями сетей называется вертикальным (межсистемным). Для обеспечения корректной горизонтальной передачи обслуживания абонентов необходимо учитывать такие параметры как уровень принимаемого сигнала (RSSI), требуемая мощность, качество обслуживания абонента, скорость передвижения, информация о местоположении и требования пользователя к скорости передачи данных [3].

С учетом размеров маломощных сот, любое движение UE через макросоты вызывает много ненужных и часто повторяющихся хэндоверов. Таким образом, разработка эффективной методики хэндовера является непростой задачей. Управление процедурой хэндовера лежит в основе некоторых методов балансировки нагрузки в сети.

В данной статье описывается механизмы распределения трафика между БС-ями различных типов в гетерогенных сетях за счет расширения зон покрытия пико-БС.

Технология расширения зон покрытия (CRE)

Для балансировки нагрузки между БС гетерогенной сети в системе LTE применяется технология расширения зон покрытия CRE (*Cell Range Expansion*), которая позволяет искусственно увеличить зону обслуживания малой соты (например, пико-БС) и тем самым разгрузить макросоты [4]. Условие переключения пользователя с макро-БС на пико-БС можно записать в виде следующего неравенства (2):

$$\boldsymbol{RSRP}_{pico} + \boldsymbol{Offset}_{CRE} \geq \boldsymbol{RSRP}_{macro}, \qquad (2)$$

где $\boldsymbol{RSRP}_{pico}$ (*Reference Signal Received Power*) – средний уровень принимаемой мощности от пико-БС, $\boldsymbol{Offset}_{CRE}$ – величина искусственно положительного смещения, $\boldsymbol{RSRP}_{macro}$ – средний уровень принимаемой мощности от макро-БС, изначально обслуживающей пользователя. Структура CRE пико-БС изображена на рисунке 2.

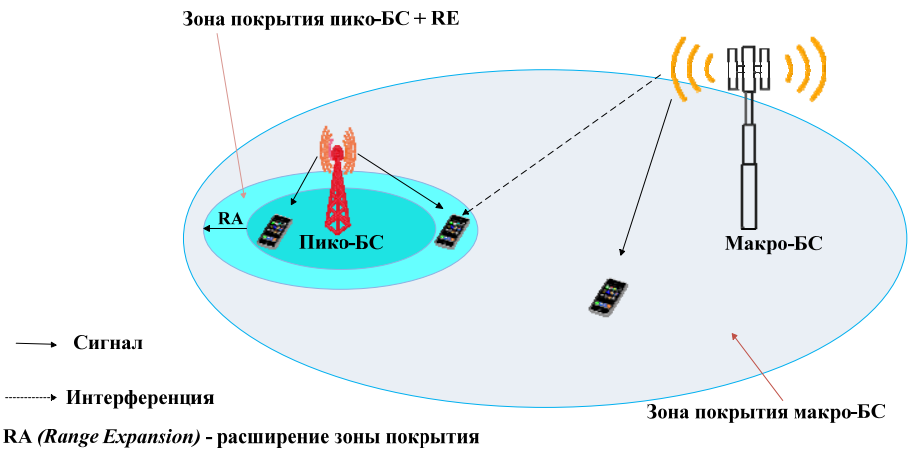


Рис. 2. Технология CRE для балансировки трафика в гетерогенных сетях LTE

Следует отметить, что применение данного механизма CRE приводит к повышению уровня внутриканальных помех в приемниках пользователей, ассоциированных с пико-БС [5]. Способы борьбы с такими помехами является улучшенная координация межсотовой интерференции **eICIC** (*enhanced ICIC)* и координация многоточечных передачи и приема **CoMP** (*coordinated multipoint*), специфицированные в 3GPP Release 10.

Координированная передача данных по схеме eICIC

В технологии eICIC предлагается усовершенствование методов снижения внутрисистемных помех во временной области за счет применения субкадров с ограниченной активностью ABS *(Almost Blank Subframes),* позволяющий маломощным узлам использовать эти субкадры на краю соты, в то время как обслуживание пользователей макро-БС прекращается во всех субкадрах ABS, что позволяет сократить влияние помех от макро-БС на краю малых сот.

Координированная передача данных по схеме CS/CB CoMP

При координации с планированием физических ресурсов и формированием диаграмм направленности CS/CB CoMP *(Coordinated Scheduling and Coordinated Beamforming)* между соседними БС-ями гетерогенной сети для каждого субкадра осуществляется динамическая координация и адаптивный выбор параметров передаваемых сигналов: модуляции, скорости кодирования, вид пространственной обработки сигналов. Однако, в отличие от схемы eICIC, требует интенсивного обмена служебной информацией между станциями. Поэтому в схемах CoMP несколько соседних БС объединяются в так называемый кластер с помощью высокоскоростных линий связи с малой задержкой. В результате применения такой схемы существенно уменьшается уровень взаимных внутриканальных помех в приемниках UE, обслуживаемых БС-ями кластера.

Сравнительный анализ методов балансировки нагрузки

В таблице 2 приведен сравнительный анализ двух схем eICIC и CS/CB CoMP, для распределения трафика между базовыми станциями гетерогенной сети стандарта LTE [4, 6].

Сравнительный анализ методов балансировки нагрузки показал, что:

1. При применении схемы eICIC можно достичь большего выигрыша в пропускной способности по сравнению со схемой CS/CB CoMP с небольшим числом координируемых станций с одновременно низким уровнем внутриканальных помех. Схема eICIC требует для своего внедрения лишь обновление программного обеспечения на базовых станциях и не требует аппаратных изменений.

2. При применении схемы CS/CB CoMP больших кластеров выигрыш в пропускной способности получился больше по сравнению со схемой eICIC. Этот метод, в свою очередь, требует аппаратных изменений (например, наличие центрального процессора для цифровой обработки сигналов от всех БС, входящих в один кластер) и, как следствие, высокие финансовые затраты на реализацию метода.

ТАБЛИЦА 2. Сравнительный анализ eICIC и CS/CB CoMP

Критерии эффективности методов	Технология расширения зон покрытия (CRE)		
	eICIC	CS/CB CoMP	
		Частичная координация	Полная координация
Средняя пропускная способность, Мбит/с	Высокая	Низкая	Очень высокая
Уровень внутриканальных помех	Низкий	Очень высокий	Высокий
Подавление внутриканальных помех	Не огранчено	Ограничено	Ограничено
Затраты на реализацию метода	Низкие	Высокие	Очень высокие
Сложность реализации	Простая (программная функция)	Сложная (аппаратные средства)	
Балансировка нагрузки	Не ограничено	Ограничено	Не ограничено
Координация	Полная	Частичная	Полная
Технические спецификации 3GPP	Rel.10 / Rel.11	Rel.11 / Rel.12	
Объем обмена информацией между БС	Небольшой	Средний	Большой

Список используемых источников

1. Wei Bao and Ben Liang. Handoff rate analysis in heterogeneous cellular networks // A Stochastic Geometric Approach, DECE University of Toronto, Canada-2014. PP. 95–102.

2. Фокин Г. А. Управление самоорганизующимися пакетными радиосетями на основе радиостанций с направленными антеннами : дис. … канд. техн. наук : 05.13.13 / Фокин Григорий Алексеевич. СПб., 2009. 144 с.

3. Касенхан А. Разработка методов и моделей поддержки эффективной беспроводной связи в системах оперативных служб: дис. … канд. техн. наук : 6D070400 / Касенхан Арай. Алматы. 115 с.

4. Морозов Г. В. Анализ пропускной способности систем сотовой связи, использующих координированную передачу сигналов базовыми станциями для подавления взаимных непреднамеренных помех: дис. … канд. физ.-мат. наук : 01.04.03 / Морозов Григорий Владимирович. Нижний Новгород, 2015 – 108 с.

5. Sonia B. S. LTE-Advanced HetNet Investigations Under Realistic Conditions. Aalborg University, Denemark. June 2014. 114 с.

6. Степутин А. Н., Ромашенков Н. О., Фокин Г. А. Разгрузка сетей LTE через сети Wi-Fi // Научно-технический вестник информационных технологий, механики и оптики. 2015. Т. 15. № 6. С. 1139–1146.

УДК 621.396.96

ПОЗИЦИОНИРОВАНИЕ ИСТОЧНИКОВ РАДИОИЗЛУЧЕНИЯ В УСЛОВИЯХ ВЫСОКОГОРЬЯ РЕСПУБЛИКИ ЙЕМЕН С ИСПОЛЬЗОВАНИЕМ БЕСПИЛОТНЫХ ЛЕТАТЕЛЬНЫХ АППАРАТОВ

А. Х. Аль-Одхари

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

В настоящей работе предлагается использование беспилотных летательных аппаратов для повышения точности позиционирования источников радиоизлучения традиционным разностно-дальномерным методом. Выполнено сравнение полученных оценок для случая с подвижными и стационарными приемниками; предложен вариант их территориального распределения для повышения точности позиционирования.

позиционирование, TDOA, беспилотный летательный аппарат.

В Йемене, как и в других странах мира, террористы ведут активную деятельность и скрываются в пещерах высокогорной местности. Для нейтрализации объектов террористической угрозы (далее, объектов) их необходимо предварительно обнаружить и локализовать. Сложность решения данной задачи определяется тем обстоятельством, что предполагаемые объекты скрываются в пещерах высокогорья республики Йемен. Оценка точности позиционирования разностно-дальномерным методом проводилась в работах [1, 2, 3, 4, 5, 6], однако там не были учтены особенности ландшафта. Для повышения точности позиционирования традиционным разностно-дальномерным методом с учетом ландшафта предполагается использование беспилотные летательные аппараты (БПЛА). В настоящей работе представлены результаты исследований по оценке точности позиционирования для случая, когда сбор навигационных измерений производится стационарными и подвижными станциями обнаружения (далее, приемными станциями) на основе БПЛА с использованием моделирования в среде MatLab.

Разностно-дальномерный метод (TDOA)

Метод TDOA (*Time Difference of Arrival*) основан на предположении о том, что если объект излучает сигнал в момент времени t_0, то время прихода сигнала на приемную станцию определяется по формуле [7]:

$$t_i = t_0 + \frac{D_i}{c},$$

где t_i – время прихода сигнала на приемную станцию i, D_i – расстояние между излучателем и приемными станциями, c – скорость света. При использовании двух или более приемных станций можно оценить разность прихода сигнала и, таким образом, убрать t_0 из предыдущего выражения, что приводит к уравнению вида:

$$t_2 - t_1 = \frac{D_2 - D_1}{c}.$$

Это основная форма уравнения TDOA [8], которая описывает гиперболу в трехмерном пространстве. Пусть x_0, y_0, z_0 – координаты излучателя, а x_1, y_1, z_1 и x_2, y_2, z_2 – координаты антенны приемной станции 1 и 2, соответственно, тогда уравнение TDOA:

$$\sqrt{(x_2 - x_0)^2 + (y_2 - y_0)^2 + (z_2 - z_0)^2},$$
$$-\sqrt{(x_1 - x_0)^2 + (y_1 - y_0)^2 + (z_1 - z_0)^2} = c(t_2 - t_1).$$

Имея 4 приемные станции, можем записать систему из трех уравнений, решив которую найдем координаты излучателя x_0, y_0, z_0.

Все методы TDOA подвержены ошибкам в измерении. Шум и погрешность измерения являются двумя основными источниками ошибок [9]. В настоящей работе рассмотрим ошибки, вызванные шумом, и оценим их в терминах стандартного отклонения.

Стандартное отклонение дает хорошее представление о точности, поэтому выполняется моделирование, чтобы проанализировать точность стандартного отклонения для каждой оси и общего стандартного отклонения [9].

Общее стандартное отклонение определяется по следующей формуле:

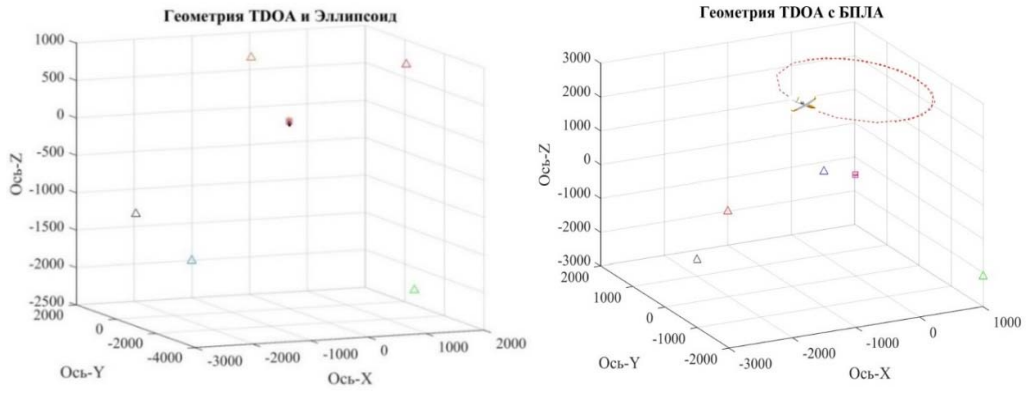
$$\sigma_{total} = \sqrt{\sigma_x^2 + \sigma_y^2 + \sigma_z^2},$$

где σ_x – стандартное отклонение по оси *x*, σ_y – стандартное отклонение по оси *y*, σ_z – стандартное отклонение по оси *z*.

Сравнение между подвижными приемными станциями БПЛА и стационарными приемными станциями.

Моделирование проводится по двум сценариям.

Первый сценарий: 5 стационарных приемных станций. Второй сценарий: 4 стационарных приемных станции и 1 подвижная приемная станция БПЛА. На рисунке 1*а* показано расположение пяти стационарных приемных станций, которые пытаются обнаружить излучатель.



а) б)

Рис. 1. Расположение приемных станций: а) пять стационарных приемных станций, б) четыре стационарных приемных станции и одна подвижная БПЛА

Второй сценарий: 4 стационарных приемных станции и 1 подвижная БПЛА.

В этом сценарии БПЛА летает над рабочей зоной на постоянной высоте. Используются 20 точек вкруг излучателя, и проводится 500 экспериментов для каждой точки БПЛА.

На рисунке 1*б* показано расположения четырех стационарных приемных станций и одной подвижной приемной станции БПЛА, которые пытаются обнаружить излучатель.

Результаты моделирования представлены в таблице 1, откуда видно, что использование беспилотного летательного аппарата позволяет повысить точность позиционирования примерно в 2 раза по сравнению с первым сценарием.

ТАБЛИЦА 1. Стандартные отклонения

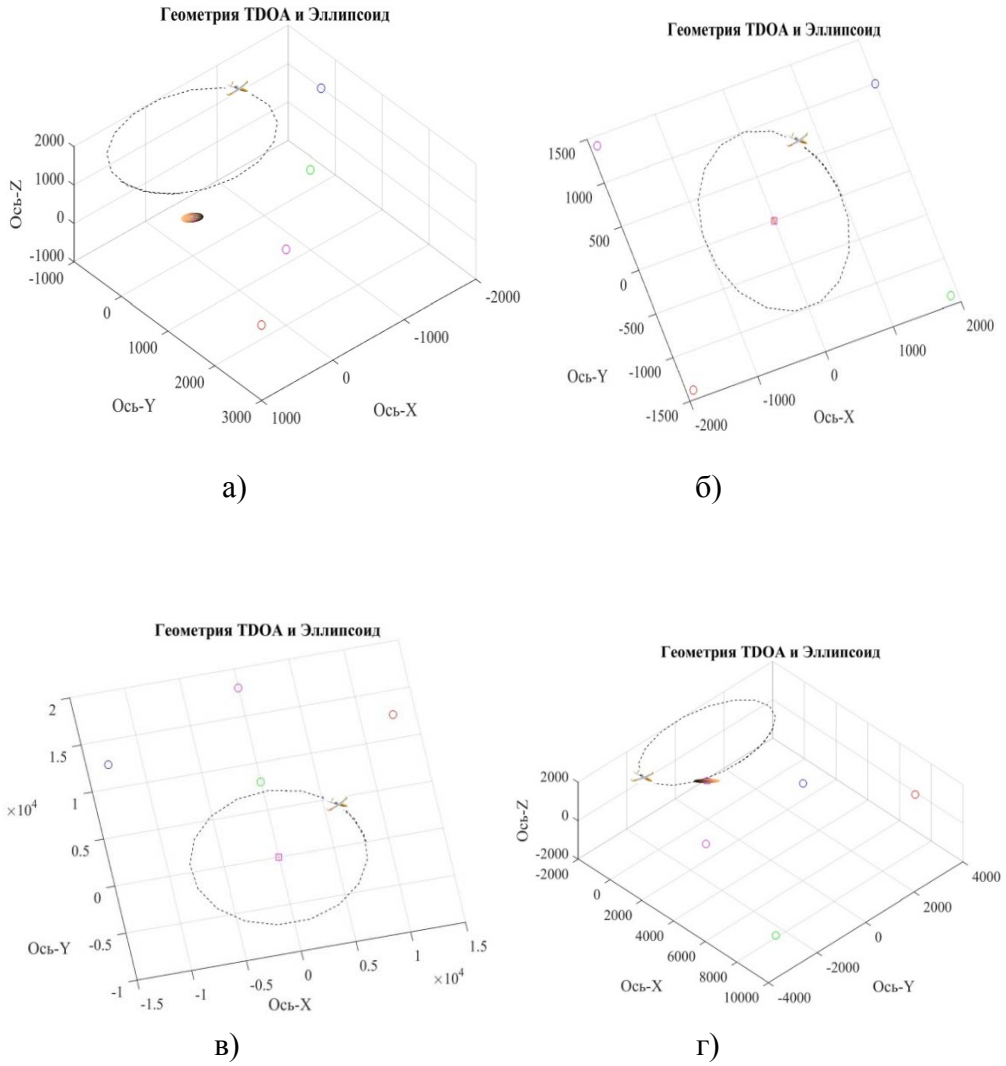
Стандартное отклонение	Стационарные приемные станции, м	Приемные станции с БПЛА, м
σ_x	28,9116	22,5403
σ_y	31,7818	27,0807
σ_z	71,5295	28,0882
σ_{total}	83,4412	45,3060

Оптимальное распределение приемных станций для повышения точности

Четыре приемных станции и одна БПЛА могут быть территориально распределены следующим образом: прямая линия, ромб, квадрат и прямоугольник, как показано на рисунке 2 [10].

Результаты моделирования представлены в таблице 2, откуда видно, что сценарий 2 имеет минимальное общее стандартнее отклонение. Далее для повышения точности позиционирования предполагается использовать второй вариант территориального распределения приемных станции.

Таким образом, использование БПЛА позволяет повысить точность позиционирования примерно в 2 раза по сравнению со случаем стационарных приемных станций, а наиболее подходящим территориальным распределением является их расположение вокруг излучателя.



а) б)

в) г)

Рис. 3. Геометрия TDOA

ТАБЛИЦА 2. Варианты территориального распределения приемных станций

№	Сценарий	Общее стандартные отклонения, м
1	Приемные станции расположены на прямой линии, рисунок 2*а*	794,7994
2	Приемные станции расположены вокруг излучателя, рисунок 2*б*	42,7457
3	Приемные станции расположены в форме ромба, рисунок 2*в*	330,7548
4	Приемные станции расположены в форме треугольника, рисунок 2*г*	1257,3010

Список используемых источников

1. Сиверс М. А., Фокин Г. А., Духовницкий О. Г. Позиционирование абонентских станций в сетях мобильной связи LTE разностно-дальномерным методом // Системы управления и информационные технологии. 2015. Т. 59. № 1. С. 55–61.

2. Sivers M., Fokin G. LTE positioning accuracy performance evaluation // Lecture Notes in Computer Science. 2015. Т. 9247. PP. 393–406.

3. Киреев А. В., Фокин Г. А. Позиционирование базовой станции в сетях LTE средствами пространственной обработки сигналов [Электронный ресурс] // Актуальные проблемы инфотелекоммуникаций в науке и образовании. III Международная научно-техническая и научно-методическая конференция: сб. научных статей / под ред. С. М. Доценко, сост. А. Г. Владыко, Е. А. Аникевич, Л. М. Минаков. СПб. : Санкт-Петербургский государственный университет телекоммуникаций им. проф. М. А. Бонч-Бруевича, 2014. С. 124–128. URL: http://www.sut.ru/doci/nauka/iiiapino2014.pdf (дата обращения 13.04.2016).

4. Фокин Г. А. Оценка точности позиционирования абонентских станций в сетях LTE разностно-дальномерным методом [Электронный ресурс] // Актуальные проблемы инфотелекоммуникаций в науке и образовании. IV Международная научно-техническая и научно-методическая конференция: сб. науч. ст. в 2 т. / под ред. С. В. Бачевского, сост. А. Г. Владыко, Е. А. Аникевич, Л. М. Минаков. СПб. : Санкт-Петербургский государственный университет телекоммуникаций им. проф. М. А. Бонч-Бруевича, 2015. С. 170–173. URL: http://www.sut.ru/doci/nauka/4.apino.2015.sut.pdf (дата обращения 13.04.2016).

5. Киреев А. В., Фокин Г. А. Позиционирование источников радиоизлучения в сетях LTE с использованием круговой антенной решетки / Наука и инновации в технических университетах : материалы Девятого Всероссийского форума студентов, аспирантов и молодых ученых. СПб. : Санкт-Петербургский политехнический университет Петра Великого. 2015. С. 25–26.

6. Киреев А. В., Фокин Г. А. Пеленгация источников радиоизлучения LTE мобильным пунктом радиоконтроля с круговой антенной решеткой // Труды Научно-исследовательского института радио. 2015. № 2. С. 68–71.

7. Ezzat G. B. Closed-form solution of hyperbolic geolocation equations // IEEE Transactions on Aerospace and Electronic Systems. 2006. N 42. – PP. 1396–1404.

8. Zakavat S. A, Buehrer R. M. Handbook of position location: Theory, Practice, and Advances // Wiley-IEEE.2011. P. 1281. ISBN 978-0-470-94342-7.

9. Yan-Ping L., Feng-Xun G., Yan-Qiu M. Optimal distribution for four-station TDOA location system // Biomedical Engineering and Informatics (BMEI), 3rd International Conference, 2010. – PP. 2858–2862.

10. Poisel R. Electronic warfare target location methods: Norwood. MA : Artech House, 2012. 439 p. ISBN 13: 978-1-60807-523-2.

Статья представлена научным руководителем, кандидатом технических наук, доцентом Г. А. Фокиным.

УДК 621.376

АВТОМАТИЗАЦИЯ АППРОКСИМАЦИИ НЕТРАДИЦИОННЫХ ЗАВИСИМОСТЕЙ ФИЛЬТРОВЫХ УСТРОЙСТВ

А. В. Ананьев[1], А. В. Прикота[2]

[1]Военный учебно-научный центр Военно-воздушных сил
«Военно-воздушная академия им. профессора Н. Е. Жуковского и Ю. А. Гагарина»
[2]Общество с ограниченной ответственностью «Эремекс»

На примере цифровых дисперсионных линий задержки с бесконечной импульсной характеристикой с чебышевской аппроксимацией группового времени запаздывания предложен подход к разрешению проблем автоматизированного синтеза, обусловленных сложностью поиска векторов начального приближения и низкой устойчивостью поиска оптимального решения.

неклассическая аппроксимация, автоматизация проектирования, дисперсионная линия задержки, бесконечная импульсная характеристика.

Все существующие частотные характеристики фильтровых устройств условно можно разделить на две группы: имеющие аналитическое решение и не имеющие его. К первой группе следует отнести, например, аппроксимации амплитудно-частотных характеристик фильтров нижних частот с аппроксимацией Баттерворта, Чебышева, инверсные Чебышева, Золотарева. К группе характеристик не имеющих аналитического решения следует отнести, например, неклассические полиномы третьего порядка [1], наклонное групповое время запаздывания [2] и др. Неклассические, в том числе равноволновые приближения, оптимальные по Чебышеву, требуют применения численных алгоритмов. Основы теории синтеза оптимальных фильтровых устройств, включающие этап аппроксимации частотных характеристик на основе численных методов, достаточно полно изложены в [3]. К работам, отражающим современное состояние и успехи практической реализации численных методов приближения следует отнести [4, 5, 6]. Анализ приведенных публикаций позволяет констатировать факт, что одной из нерешенных проблем практической реализации получения равноволновых приближений является поиск начальных значений векторов коэффициентов аппроксимирующих функций.

Целью исследований является разработка подхода к автоматизации аппроксимации неклассических частотных характеристик, не имеющих аналитического решения.

Поставленная цель может быть достигнута на основе разработки системы автоматизированного синтеза частотных характеристик. Рассмотрим ее составляющие на примере системы синтеза наклонного группового времени запаздывания (ГВЗ) (рис. 1), описываемого выражением:

$$y(\omega) = \alpha_1 \pm \alpha_2 \omega,$$

где α_1, α_2 – действительные коэффициенты, определяющие положение прямой, ω – угловая частота. Блок анализа входных данных и управления ходом решения обеспечивает взаимодействие всех элементов системы.

Субблок анализа входных данных обеспечивает обработку входных данных, включая вычисление требуемого коэффициента перекрытия по частоте $k_\omega = \omega_æ / \omega_{-æ}$, где $\omega_{-æ}$, $\omega_æ$ – нижняя и верхняя угловые частоты, определение типа характеристики (возрастающая или убывающая, полосовая или низкочастотная), неравномерности аппроксимации $a_{\max}$ (дБ) на основании чего осуществляется выбор ближайшего решения в базе данных.

Субблок контроля текущего решения обеспечивает устойчивость поиска физически реализуемых решений и остановку работы системы при достижении требуемой точности решения. Так, для рассматриваемого случая передаточная функция может быть представлен в виде:

$$H(z) = \prod_{i=1}^{N/2} \frac{a_i + b_i e^{-j\omega} + e^{-j2\omega}}{1 + b_i e^{-j\omega} + a_i e^{-j2\omega}},$$

где a_i, b_i – коэффициенты передаточной функции; N – порядок аппроксимирующей функции, $z = e^{-j\omega}$, поэтому контролируемым условием являет выполнение неравенств $b_i > 0$, $a_i > 0$, $i = 1...N/2$.

Субблок вычисления текущего приближения по данным субблока контроля обеспечивает адаптивное формирование векторов приближений коэффициентов и частот альтернанса Чебышева. Наличие опорных решений, содержащихся в базе начальных приближений позволяет осуществлять линейное преобразование частот экстремальных отклонений, в соответствие с выражением:

$$\hat{\omega}_{i\,\text{пр}} = \hat{\omega}_i \times \left(\hat{\omega}'_æ \div \hat{\omega}_æ \right), \; i = 1...N+2,$$

где $\hat{\omega}_æ$ – новое требуемое значение граничной частоты, что адаптирует алгоритм Ремеза к условиям решаемой задачи, и, как следствие, повышает устойчивость поиска оптимальных физически реализуемых решений линейном уменьшении коэффициента наклона:

$$\alpha_{2_{пр}} = \alpha_2 \div \frac{\hat{\omega}'_{ае}}{\hat{\omega}_{ае}}.$$

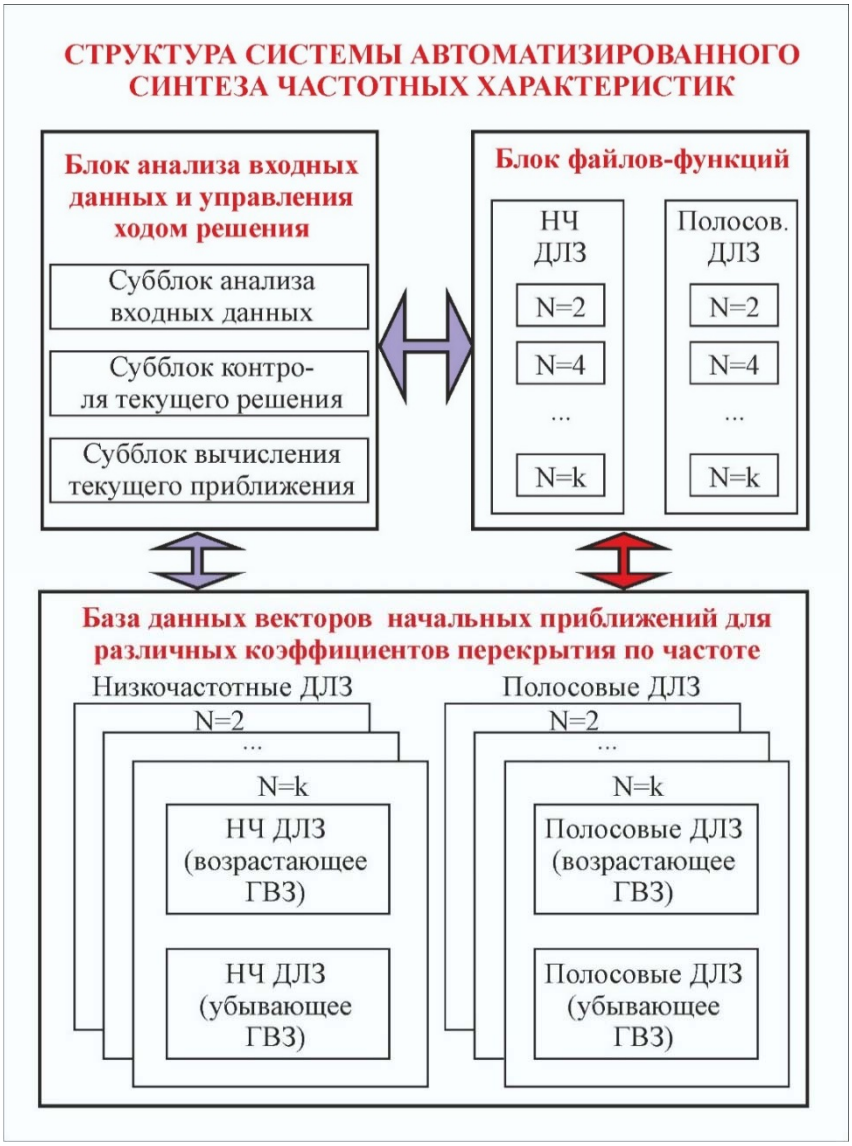


Рис. 1. Структура системы автоматизированного проектирования

Блок файлов функций реализуемый, например, в формате систем уравнений [7], является инструментом, обеспечивающим численное решение задачи аппроксимации.

База данных обеспечивает начальное приближение для первой итерации решения систем уравнений и, в свою очередь, может быть сформирована с использованием известных решений задачи аппроксимации для дисперсионных линий задержки [2]. Основу базы данных составляют вектора начальных приближений коэффициентов передаточных функций $\mathbf{A} = \{a_i\}$ и соответствующих им векторов частот экстремальных отклонений в нормированном диапазоне частот $\mathbf{\Omega} = \{\Omega_i\}$.

На рисунке 2 представлен результат аппроксимации, основанный на подходе, заложенном в предлагаемую систему автоматизированного синтеза: верхний график результирующее ГВЗ, нижний – разность аппроксимируемой и аппроксимирующей функции, свидетельствующая о существовании альтернанса Чебышева.

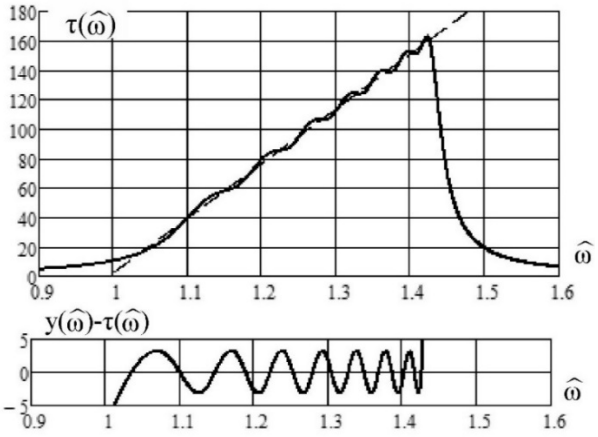


Рис. 2. Результат аппроксимации

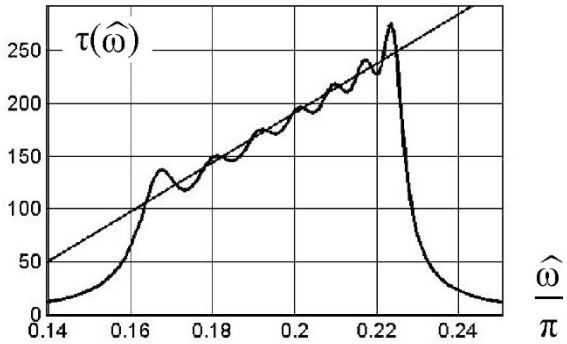


Рис. 3. Результат аппроксимации в среде MATLAB

Отдельно остановимся на функции разработки фазовых цепей с БИХ “iirgrpdelay”, представленной в программной среде MATLAB [8]. В основу работы оператора положен алгоритм квазиНьютона [4]. Функция позволяет аппроксимировать различные зависимости ГВЗ в нормированной полосе частот на интервале [0, 1]. В том числе, существует вариант вызова функции, при котором можно получить аппроксимации близкие к Чебышевским, при этом справочные материалы Matlab содержат предупреждение о необходимости проверки расположения полюсов полиномов на предмет устойчивости передаточной функции и непосредственно самой зависимости временной задержки от частоты.

Для сравнительной оценки предлагаемого подхода в работе осуществлена аппроксимация требуемого закона ГВЗ с применением оператора “iirgrpdelay” программной среды Matlab. Полученный результат приведен на рисунке 3. Характер отклонения аппроксимирующей функции от аппроксимируемой позволяет судить о наличии альтернанса Валле-Пуссена, однако максимумы отклонений аппроксимирующей функции от аппроксимируемой примерно равны только в середине интервала аппроксимации, а на краях – существенно больше. Кроме того, в ходе решения возникли трудности обеспечения минимальной задержки сигнала в целом.

Таким образом, разработанный подход позволяет разрешить проблему начального приближения и обеспечивает устойчивость поиска оптимальных решений. Предложенный подход может быть распространен, как минимум, на все случаи гладких аппроксимирующих функций.

Список используемых источников

1. Ananjev A. V., Zmii B. F. Synthesis of ARC filter devices with enhanced stability // Telecommunications and Radio Engineering. 2012. Vol. 71. Iss. 20. PP. 1859–1869.

2. Ananjev A. V., Zmii B. F. Synthesis of transfer functions in phase devices for processing chirp signals with different frequency ratios // Telecommunications and Radio Engineering. 2013. Vol. 72. Iss. 12. PP. 1107–1116.

3. Ланнэ А. А. Оптимальный синтез линейных электронных систем. М. : Связь, 1978. – 336 с.

4. Змий Б. Ф. Синтез линейных устройств обработки сигналов на активных четырехполюсниках высших порядков : монография. Воронеж : ВАИУ, 2008. – 325 с.

5. Antoniou A. Digital Signal Processing. New York : McGraw-Hill, 2006. 965 p. ISBN 1-904275-26-5.

6. Ricardo Pach´on, Lloyd N. Trefethen Barycentric-Remez algorithms for best polynomial approximation in the chebfun system // Journal: Bit Numerical Mathematics – BIT. 2009. Vol. 49. No. 4. PP. 721–741.

7. Ананьев А. В. Реализация численных методов чебышевского приближения в среде Mathcad // Информатика: проблемы, методология, технологии : материалы докладов XIV Международной научно-технической конференции. ВГУ. Воронеж. 2014. Т. 1. С. 43–46.

8. MATLAB Filter Design Toolbox. URL: http://www. mathworks.com/help/dsp/ref/iirgrpdelay.html?s_tid=srchtitle/ (дата обращения 10.12.2015).

УДК 004.932.2

АНАЛИЗ МЕТОДОВ ОБРАБОТКИ ВИДЕОДАННЫХ ДЛЯ АВТОМАТИЧЕСКОГО ВЫДЕЛЕНИЯ ЦЕЛЕЙ

А. А. Ангелуц, С. М. Одоевский

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

Рассмотрены и проанализированы методы обработки изображений применительно к задаче автоматического обнаружения целей. В результате проведенного анализа выбран метод, на основе которого будут проводиться дальнейшие исследования, направленные на разработку методики обработки изображений для автоматического обнаружения целей находящихся на поверхности воды.

видеоданные, движущаяся телекамера, методы обработки, фильтрация, обнаружение, метод оптического потока, фильтр Калмана.

В настоящее время, как в мире, так и в Российской Федерации всё большее значение приобретают морские робототехнические комплексы, в том числе необитаемые катера. Использование таких робототехнических комплексов требует надежного навигационного обеспечения и освещения надводной обстановки. Важной составной частью комплекса обеспечивающего

навигационную безопасность является система видеонаблюдения. Одной из актуальных задач направленных на усовершенствование систем видеонаблюдения на морских подвижных объектах является разработка методики выделения движущихся объектов на сложном неоднородном фоне при наличии различного рода помех и создание на этой основе системы мониторинга.

В данной работе исследуются некоторые методы обработки видеосигналов для обеспечения автоматического выделения априорно неизвестных целей, находящихся на поверхности воды при создании бортовых систем обнаружения и сопровождения объектов необитаемых катеров. В качестве исходных данных выступают кадры видеопоследовательности, полученные с телекамеры, закрепленной на борту катера на фиксированной высоте относительно ватерлинии, а также текущие параметры ориентирования, определенные навигационным оборудованием. Статью следует рассматривать как начальный теоретический задел для дальнейших исследований в области автоматического обнаружения целей.

Как показывают различные исследования, в последнее время увеличился интерес к созданию систем автоматического видеонаблюдения, находящих применение в различных областях человеческой деятельности, например, при создании бортовых систем беспилотных летательных аппаратов [1, 2], систем мониторинга обстановки на железной дороге, систем распознавания лиц и т. д.

На данный момент известны такие методы обработки изображений для выделения объектов как сегментация, линейная и нелинейная пространственная фильтрация, на основе методов пространственно-временных изменений, на основе геометрических преобразований [3, 4].

Сегментация разделяется на следующие типы:

– выделение областей изображения с известными свойствами – заключается в поиске определенных областей, о которых имеется априорная информация;

– разбиение изображения на однородные области – никакая априорная информация о свойствах областей не используется, зато на само разбиение изображения накладываются некоторые условия (например, все области должны быть однородны по цвету и текстуре);

– методы, основанные на операторах выделения краев – при данном подходе задача сегментации формулируется как задача поиска границ регионов. Методы поиска границ хорошо разработаны для полутоновых изображений;

– методы теории графов – изображение представляется в виде взвешенного графа, с вершинами в точках изображения. Вес ребра графа отражает сходство точек в некотором смысле Разбиение изображения моделируется разрезами графа;

– бинаризация – пороговые методы бинаризации работают со всем изображением, находя какую-то характеристику (порог), позволяющую разделить все изображение на чёрное и белое.

Следующим методом обработки изображений является линейная и нелинейная пространственная фильтрация. Данная фильтрация направлена на подавление шумов изображений, поступивших с телекамеры с целью формирования кадра с минимальным уровнем шумов, позволяющим осуществить дальнейшую обработку. На этом этапе предлагается проводить фильтрацию на основе фильтра Калмана – эффективного рекурсивного фильтра, оценивающего вектор состояния динамической системы, используя ряд неполных и зашумленных измерений.

Работа алгоритма включает два этапа: предсказание и корректировку. Важнейшей особенностью фильтра Калмана является быстродействие, он обеспечивает выделение изображения на фоне шума в реальном времени.

Методы на основе пространственно-временных изменений часто применяются для построения переднего плана [4].

Методы вычитания фона часто применяются для детектирования движущихся объектов. Суть их заключается в нахождении попиксельной разности между текущим кадром и некой моделью фона. Такая модель должна представлять собой сцену без движущихся объектов. При этом необходимо ее регулярное обновление, для того чтобы учитывать изменение условий освещенности и настроек камеры, таких как поворот, наклон и изменение фокусного расстояния.

Недостатками метода вычитания фона являются:

– возможная классификация фоновых пикселей как переднеплановых. например для падающих снега и дождя, волн, теней, отбрасываемых движущимися объектами;

– латентность в обновлении модели фона;

– высокие требования к ресурсам вычислительной системы.

При использовании вероятностных методов задний план формируется в результате моделирования стохастического «пиксельного процесса», т. е. для каждого пикселя изменение его интенсивности от кадра к кадру рассматривается как временной ряд, состоящий из скалярных величин для полутоновых изображений, и векторов – для цветных. В результате фон представляет собой гауссову смесь, т. е. линейную комбинацию одномерных, нормально распределенных случайных величин. Более совершенными являются алгоритмы, создающие попиксельную модель всей сцены, в которой используются отдельно гауссовы смеси для фона, переднего плана и теней. Основываясь на времени существования и дисперсии каждого гауссиана в смеси, можно определить, какие из них относятся к фону. Пиксели, значения которых не укладываются в фоновые распределения, считаются пе-

реднеплановыми до тех пор, пока не появится гауссиан, позволяющий с достаточной точностью отнести их к фону. Такой подход позволяет учитывать медленные изменения освещенности путем подстройки параметров гауссианов. Кроме того, в рамках вероятностных методов возможен адекватный анализ распределений с несколькими максимумами, что является типичным для ситуаций с падающими тенями, отражениями, качающимися ветвями и др. Однако быстрые изменения фона и освещенности сцены данные алгоритмы описать не могут [3].

Методы временной разности отделяют передний план от фона при помощи попиксельного вычитания двух или более последовательных кадров. Достоинством является хорошее определение динамических изменений сцены, недостатком – отсутствие возможности обнаруживать остановившиеся объекты.

Для выделения переднего плана из видеопоследовательности перспективным является метод оптического потока. Понятие потока обычно используется для описания когерентного движения точек или характерных признаков между последовательными кадрами. Выделение фона, на вычислении оптического потока, использует характеристики вектора потока движущихся объектов для нахождения тех областей видеопоследовательности, в которых происходят изменения. Также с помощью оптического потока можно получить информацию о расположении, размерах и некоторых других параметрах таких областей. С помощью методов оптического потока может быть проведено выделение движущихся объектов, даже в случае перемещения камеры. Алгоритмы являются ресурсоемкими и чувствительными к шуму [3].

Методы на основе нейронных сетей используют свойство нейронной сети адаптироваться к входным данным за счет введения настраиваемых обратных связей. Каждый пиксель фона управляется своей нейронной сетью, в результате чего через некоторое время, требуемое для настройки (обучения) нейронной сети, формируется модель фона, способная заданным образом подстраиваться к изменениям входного изображения.

Геометрические преобразования заключаются в изменении расположения точек изображения в пространстве. Причины возникновения геометрических преобразований: перемещение объекта наблюдения, перемещения камеры, изменение ориентации камеры, непрямолинейность распространения света связанная с присутствием в атмосфере различных видов неоднородностей, например, перепадов температуры.

При оценивании параметров преобразования смещения изображения используются корреляционные методы. Необходимо вычислить взаимную корреляционную функцию наблюдаемого и эталонного изображений.

При наличии неоднородного фона алгоритм, использующий вычисление максимума взаимной корреляционной функции, может давать грубые ошибки. Использование нормированных функций может решить данную

проблему. Достоинства нормированных функций – уменьшение влияния колебаний яркости изображения на точность определения координат. Недостаток – увеличение объема требуемых вычислений [4].

Для снижения вычислительных затрат при реализации корреляционных алгоритмов могут применяться алгоритмы быстрых спектральных преобразований, таких как быстрое преобразование Фурье и быстрое преобразование Хартли [5]. В отличие от преобразования Фурье, отображающего вещественные функции в комплексную область и несимметричного по комплексной переменной, преобразование Хартли осуществляет преобразования только в вещественной области, отображая вещественные сигналы в вещественные.

В данной работе проведен аналитический обзор некоторых методов и алгоритмов, применяемых на различных стадиях процесса обнаружения объектов на изображениях.

Для дальнейшего исследования наиболее подходящим является метод оптического потока позволяющий выделять движущиеся объекты при перемещении телекамеры, а также, поскольку в результате движения телекамеры возможно наличие на изображении геометрических искажений целесообразно применить методы на основе геометрических преобразований с использованием двумерного быстрого преобразования Хартли.

Список используемых источников

1. Алпатов Б. А., Бабаян П. В., Коблов Ю. С., Муравьев В. С., Стротов В. В., Фельдман А. Б. Автоматизация разработки и исследования алгоритмов машинного зрения для навигации беспилотных летательных аппаратов на базе специализированного программного комплекса // Известия ЮФУ. Технические науки. 2012. № 3 (128). С. 85–91.

2. Кочкин В. А. Автоматическое выделение динамических объектов на фоне подстилающей поверхности // Наука и образование МГТУ им. Н.Э. Баумана. Электрон. Журн. 2014. № 12. С. 889–901.

3. Ярышев С. Н. Цифровые методы обработки видеоинформации и видеоаналитика : учебн. пособие. СПб. : СПбГУ ИТМО, 2011. 83 с.

4. Алпатов Б. А., Бабаян П. В., Балашов О. Е., Степашкин А. И. Методы автоматического обнаружения и сопровождения объектов. Обработка изображений и управление. М. : Радиотехника, 2008. 176 с. ISBN 978-5-88070-201-5.

5. Брейсуэлл Р. Преобразование Хартли. М. : Мир, 1990. 175 с. ISBN 5-03-001632-5.

УДК 654.078

РАЗВЕРТЫВАНИЕ DAS СИСТЕМЫ В ТРК «ЛЕТО»

Р. А. Андреев[1], Е. В. Боброва[1], А. В. Качнов[2]

[1]Научно-производственная инновационная фирма «Гиперион»
[2]Научно-производственное предприятие «Авиационная и Морская Электроника»

Рассмотрены основные моменты развертывание DAS системы в ТРК «Лето». Представлены технические решение по реализации радиопокрытия на основе DAS систем.

DAS, радиопокрытие, частотно-территориальное планирование.

В современном обществе мобильная связь плотно вошла в повседневный обиход. Многие люди ведут переговоры, отвечают на письма, проводят видеоконференции с использованием ноутбуков и/или смартфонов. Известны разные способы обеспечения широкополосного доступа абонентов как в помещениях, так и за их пределами [1].

Для оператора одной из важнейших задач улучшения качества связи является обеспечение радио покрытия сети в зданиях и подземных парковках. Одним из способов улучшения радио покрытия сети внутри зданий является установка пико- и микросот. Но у этого способа есть несколько недостатков:

1. Требуется тщательная настройка системы для обеспечения максимально возможного коэффициента повторного использования каналов и минимизации интерференции между сотами.

2. В случае добавления или удаления пикосоты вся система подлежит реконфигурированию.

3. При обеспечении покрытия больших площадей возникают сложности с организацией трафика между пикосотами, поскольку список соседних пикосот ограничен.

Другим эффективным способом увеличения емкости сети и улучшения качества радиопокрытия являются распределенные [2] антенные системы (*Disctributed Antennas Systems,* DAS) – масштабные распределенные системы антенно-фидерных устройств, которые не только обеспечивают полное покрытие здания в сетях 2G/3G и Wi-Fi от одного оператора, но и позволяют подключиться к инфраструктуре DAS другим операторам сотовой связи. Возможности DAS еще более востребованы при переходе на сети WiMAX/4G, ориентированные на передачу больших объемов данных с большой скоростью. Основными преимуществами данных систем является легкая масштабируемость и простота развертывания.

Для обеспечения качественного покрытия в здании было принято решение реализовать Active DAS. Принцип ее работы основан на использовании разнесенных активных радиомодулей, которые способны усиливать сигнал, а также множества активных антенн, которые подключаются к радиомодулям при помощи обычного LAN кабеля.

На рисунке 1 представлена DAS система, покрывающая один этаж офисного здания.

Входящие сигналы различных операторов необходимо согласовывать входящие полосы частот и приводить уровни мощности сигнала к единому значению, для выполнения данной задачи устанавливается Signal Conditioner. Далее Комбайнеры объединяют сигналы разных операторов и частотных диапазонов. Затем объединенные сигналы передаются к радиомодулям, усиливающим их, преобразующим оптические сигналы в радиосигналы и передающим их к активным антеннам через делители мощности.

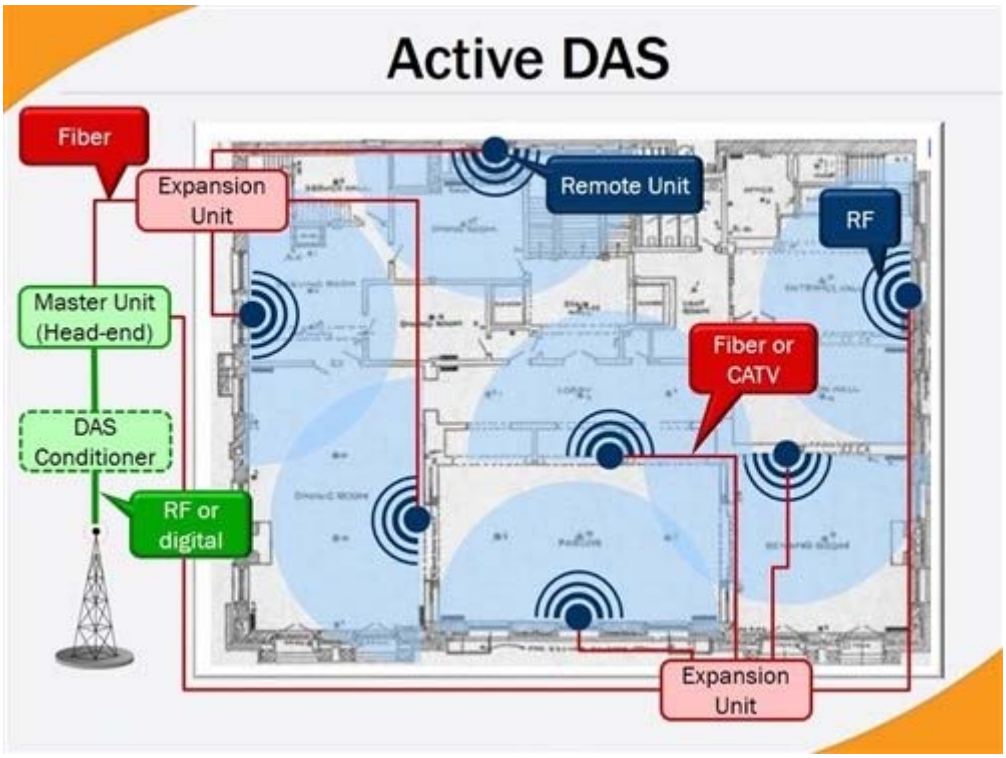


Рис. 1. Схема построения активной распределенной антенной системы

Достоинствами данной системы являются:

– возможность обеспечения качественным покрытием большой площади, за счет волоконно-оптических линий связи;

– неограниченно количество устанавливаемых антенн. Антенна – расширение одного источника сигнала, а значит, нет необходимости в конфигурации каждой антенны под конкретное место инсталляции;

– отсутствие интерференции между антеннами;

– на выходе каждой антенны, не зависимо от ее удаления от источника сигнала, будет гарантированный уровень сигнала;

– простое масштабирование;

– легкость монтажа. Тонкие волоконно-оптические линии и небольшие антенны можно установить, не нарушая отделку помещений;

– возможность локализации проблем с качеством связи, благодаря возможности дистанционного контроля и управления каждой антенной.

Существенным недостатком данной системы является ее высокая стоимость. Однако для обеспечения качественной связью и получения прибыли, администрация ТРК «ЛЕТО» согласилась дала согласие на реализацию этой дорогостоящей системы.

Для обеспечения покрытия в здании была использована платформа компании Mobile Access 1000, производства компании Corning (США).

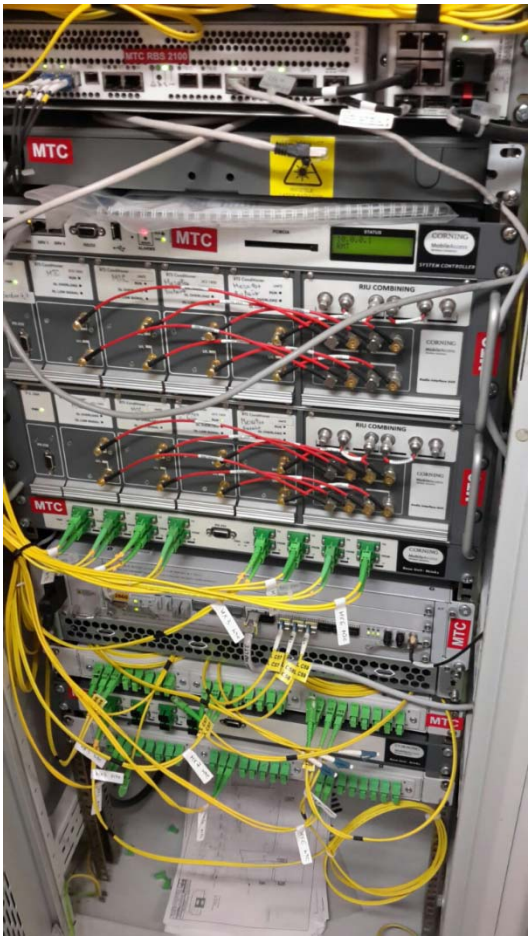


Рис. 2. Оборудование, расположенное в аппаратной ТРК «ЛЕТО»

На рисунке 2 представлена 19” стойка, располагающаяся в аппаратной в ТРК «ЛЕТО». На рисунке сверху-вниз представлены: контроллер SC-450, занимающий 2*U*, 2 блока SubRack, каждый из которых занимает по 8*U*, состоящий из четырех блоков RIU, 2 блока Base Unit на 8 и 4 выхода, которые занимают 4*U*. Таким образом, основное оборудование для развертывания

DAS системы занимает 22*U* в 19” стойке, что позволяет значительно сэкономить место в серверной.

В добавок к основному оборудованию расположенного в серверной, было задействовано 9 блоков MobileAccess HX Indoor, представленный на рисунке 3, расположенных на этажах ТРК «ЛЕТО», к которым подключено порядка 50 антенн. Для обеспечения коммуникации между блоками потребовалось не менее трех километров оптического кабеля.

Рис. 3. Радиомодуль Corning MobileAccess HX Indoor

В итоге покрытием было обеспечено порядка 98 % общей площади здания, без покрытия остались технические помещения ТРК; худший зафиксированный уровень сигнала – 89 дБм, что является отличным показателем.

Список используемых источников

1. Рыжков А. Е., Воробьев В. О., Слышков А. С., Сиверс М. А., Гусаров А. С., Шуньков Р. В. Стандарты и сети радиодоступа 4G. – СПб. : Линк, 2012. 226 с. ISBN 978-98595-032-8.

2. Фокин Г. А. Управление самоорганизующимися пакетными радиосетями на основе радиостанций с направленными антеннными: автореф. дис. … канд. техн. наук : 05.13.13 / Фокин Григорий Алексеевич. СПб., 2009, 17 с.

УДК 654.078

ВНЕДРЕНИЕ ОСНОВНЫХ ОПЕРАТОРОВ DAS В СИСТЕМУ ТРК «ЛЕТО»

Р. А. Андреев[1], Р. И. Гальчин[1], А. В. Качнов[2]

[1]Научно-производственная инновационная фирма «Гиперион»
[2]Научно-производственное предприятие «Авиационная и Морская Электроника»

Рассмотрены ключевые моменты внедрения дополнительных операторов в уже существующую DAS системы ТРК «Лето». Представлено решение поставленной задачи.

DAS, баланс мощностей, операторы сотовой связи, indoor покрытие.

Обеспечение связи внутри зданий (офисных центров, торговых комплексов, стадионов) является очень важной задачей как для операторов,

так и для арендодателей [1]. Одним из способов создания покрытия внутри зданий является использование самоорганизующихся сетей [2].

Рассмотрим вариант реализации indoor покрытия в ТРК «Лето» на основе DAS систем. Distributed Antenna Systems (распределенные антенные системы) – это сеть с пространственно разнесенными антеннами, которые подключены к общему источнику сигнала. Данная система имеет ряд преимуществ, таких как:

– возможность передачи широкополосного сигнала для одновременного обслуживания нескольких операторов, и возможности передачи по различным технологиям и стандартам сотовой связи;

– единая антенно-кабельная инфраструктура, поддерживающая любые стандарты беспроводной связи, исключающая необходимость развертывания наложенной сети для нового сервиса;

– возможность дистанционного контроля и управления системой;

– мониторинг и оптимизация по уровню мощности излучаемых радиосигналов.

– главное достоинство для владельцев комплекса – это то, что все оборудование операторов располагается только в одном помещении – аппаратной.

В ТРК «Лето» развернута DAS система, которая была рассчитана на двух операторов (рис. 1). Со временем возникла потребность в улучшении Indoor покрытия еще у двух операторов. В таком случае самый экономически выгодный вариант – это развертывание дополнительной DAS системы. Но данный метод влечет за собой проведение большого объема строительно-монтажных работ, а именно прокладку дополнительных линий оптики и установку новых блоков на этажах. Данный вариант не устроил администрацию ТРК «Лето». Поэтому был принят другой вариант улучшения покрытия уже через существующую DAS систему.

По договоренности с владельцем DAS системы было принято решение провести реконструкцию и выделить участникам по 2 модуля RIU 1800 и 2 модуля RIU 2100. В ходе выполнения работы возникла проблема подключения 8 блоков RRU 1800 и 4 блоков RRU 2100 к уже имеющимся 4 блокам RIU.

На рисунке 2 изображена схема подключения дополнительных операторов и C и D в существующую DAS. В случае с UMTS было принято решение подключить попарно RRU каждого оператора к собственному блоку RIU. Но с подключением других 8ми блоков LTE 1800 и 2G 1800 возникают сложности – их нужно привести к одному уровню мощности. Это требуется по причине того, что у производителей радиопередающих устройств выходные уровни мощности сигнала не стандартизированы и могут отличаться на довольно большую величину. В целях приведения си-

стемы к общему уровню мощности самый оптимальный вариант, это использование аттенюаторов. Но у этого метода есть минус, при сильных перегревах ВЧ аттенюатор может выйти из строя. В связи с этим было принято решение использовать симметричный делитель (сплиттер) и ВЧ нагрузку.

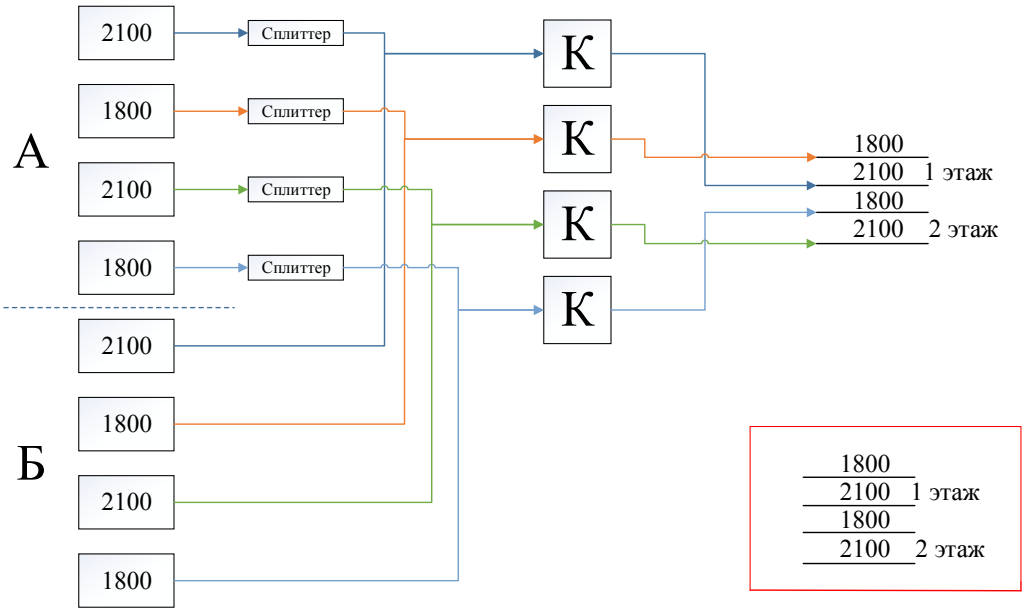


Рис. 1. Подключение двух операторов к DAS системе

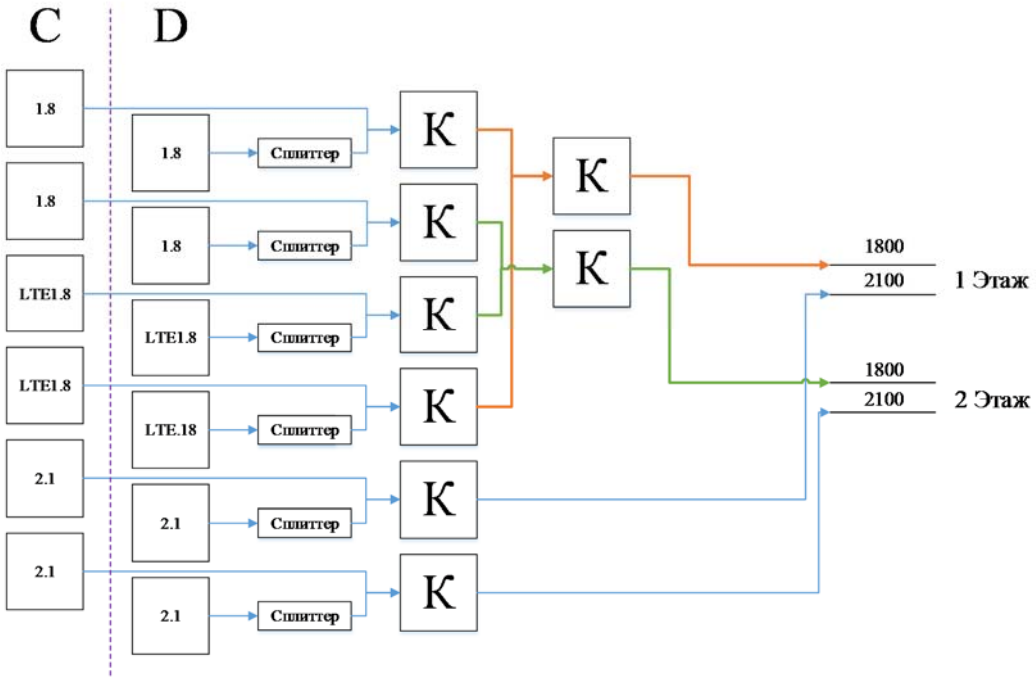


Рис. 2. Подключение дополнительных операторов

При таком варианте построения достигается возможность объединения до 4 блоков RRU с использованием гибридного комбайнера.

В ходе выполнения поставленной задачи была решена проблема подключения дополнительных операторов в уже развернутую DAS систему без

проведения дополнительных строительных работ. Результаты тестов покрытия показывают, что уровень сигнала всех операторов находится в зоне уверенного приема.

Список используемых источников

1. Рыжков А. Е., Воробьев В. О., Слышков А. С., Сиверс М. А., Гусаров А. С., Шуньков Р. В. Стандарты и сети радиодоступа 4G. – СПб. : Линк, 2012. 226 с. ISBN 978-98595-032-8.

2. Фокин Г. А. Управление самоорганизующимися пакетными радиосетями на основе радиостанций с направленными антенными: автореф. дис. … канд. техн. наук : 05.13.13 / Фокин Григорий Алексеевич. СПб., 2009, 17 с.

УДК 654.078

К ВОПРОСУ ОПРЕДЕЛЕНИЯ АЗИМУТА АНТЕННЫ БАЗОВОЙ СТАНЦИИ СОТОВОЙ СВЯЗИ

Р. А. Андреев[1], А. В. Качнов[2], Т. М. Морозова[1]

[1]Научно-производственная инновационная фирма «Гиперион»
[2]Научно-производственное предприятие «Авиационная и Морская Электроника»

Рассмотрены варианты определения азимута антенн базовых станций в реальных условиях эксплуатации с использованием различных методов. Предложены различные методики оценки правильности определения азимута антенны в полевых условиях.

определение азимута, антенны, геолокация.

Построение любой радиосистемы невозможно себе представить без применения антенно-фидерного тракта (АФУ). Частным случаем общего понятия радиосистемы является сотовая связь. базовые станции (БС) мобильной связи. Построение зон покрытия базовой станции является одной из задач, стоящих перед операторами для оценки качества оказываемых услуг, а также для планирования [1], оптимизации и улучшения качества обслуживания абонентов [2].

Правильная настройка АФУ БС является необходимым условием устойчивой работы. Ошибки при определении направления главного лепестка диаграммы направленности (ДН) АФУ могут приводить к очень серьезным последствиям, таким как: ухудшение электромагнитной совместимости в зоне излучения, создание помех соседним излучающим системам

и так далее. Также необходимо отметить, что существует ряд систем, например, станции радиорелейной связи, которые могут функционировать только при условии прямой видимости между антеннами двух станций [3].

Из вышесказанного становится очевидно, что определение направления излучения каждой антенны АФУ БС является крайне важно задачей, стоящей перед операторами [4, 5].

Рассмотрим более подробно различные варианты определения азимута излучающих антенн базовых станций мобильной связи.

Первый метод: с помощью компаса.

Как известно, азимут – это угол между направлением на север (для северного полушария) и направлением на какой-либо заданный объект

Определение азимута с использование компаса заключается в следующем: необходимо совместить северный конец стрелки с нулевой отметкой шкалы на компасе. Затем вращая кольцо с визиром добиться совпадения линии взгляда с направлением излучения ДН АФУ БС. Полученный угол и будет являться азимутом главного лепестка ДН БС. На рисунке 1 наглядно представлена реализация данного метода.

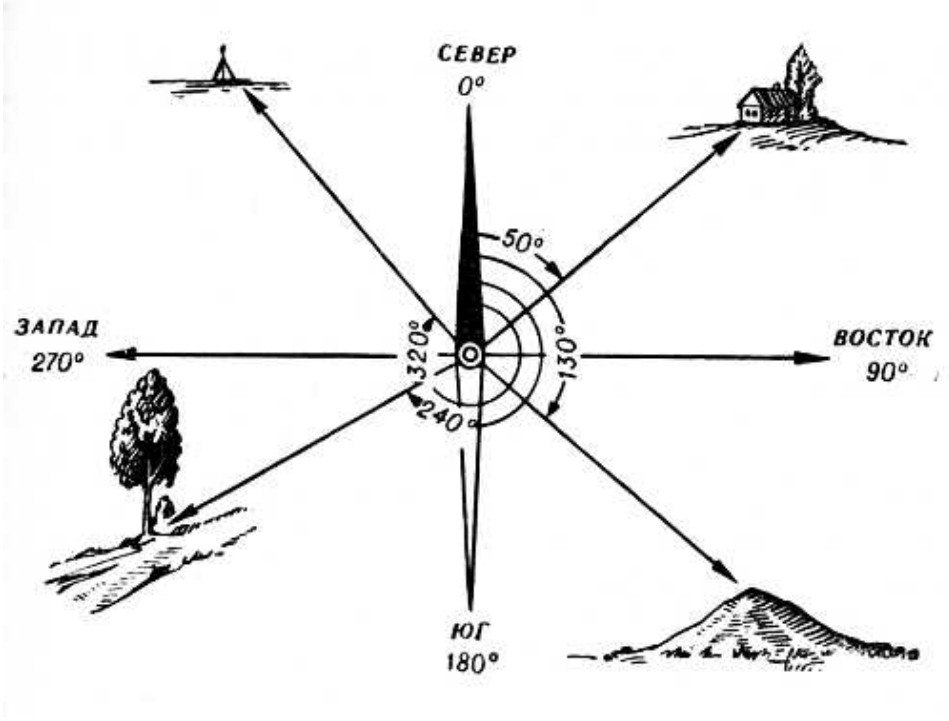


Рис. 1. Определение азимута с помощью компаса

Данный метод является исторически самым первым и простым для реализации, однако он является также самым неэффективным. Большое количество железа на антенно-мачтовых сооружениях и электромагнитные волны, излучаемые БС, существенно влияют на показания компаса, вплоть до физической невозможности определения севера. Другим недостатком

практического применения способа является неудобство его использования при работе монтажника на высоте порядка 130 м.

Как видно из вышесказанного, практическое применение данный метод находит в считанном количестве случаев и не является повсеместно применяемым.

Можно сказать, что данный метод используется для первоначальной оценки направления антенны и служит основой для последующих измерений.

Второй метод основан на использовании специального приложения или прибора – электронного транспортира.

Приложение работает следующим образом: на электронной карте находится точка расположения БС, в которой устанавливается ноль транспортира. В направлении излучения антенны на карте выбирается ориентир, и с помощью приложения определяется азимут. Погрешность такого измерения составляет примерно 10 градусов.

На рисунке 2 показан вариант использования приложения электронный транспортир. На рисунке 3 показано использование электронного транспортира в виде специального прибора при работе монтажника на объекте.

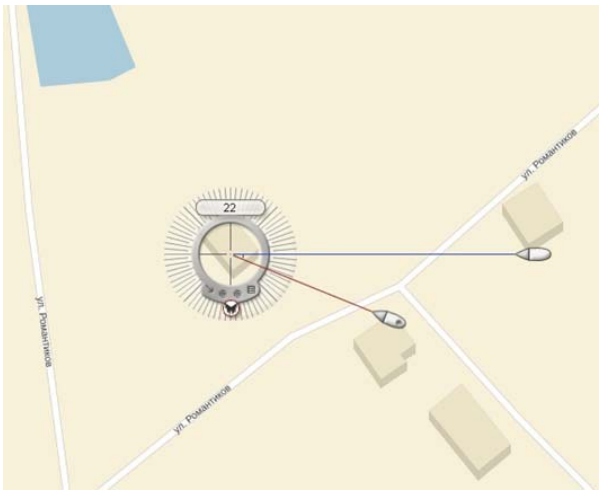


Рис. 2. Определение азимута с помощью приложения

Рис. 3. Определение азимута с помощью прибора

Использование прибора заключается в том, что монтажник прикладывает одну часть прибора к антенне, а вторую «на глаз» направляет на север,

на экране прибора или по шкале определяется азимут. Точность такого подхода больше, чем определение по компасу, но существенно зависит от того, как сотрудник определит направление на север.

Третий метод – координатный.

Этот метод использует GPS координаты двух точек, а именно, первая координата снимается с центра антенны, вторая координата определяется центром диаграммы направленности на расстоянии не менее 500 метров от антенны (рис. 4). Для вычисления азимута данным методом используется специальный географический калькулятор, который позволяет определить азимут с точностью до 1 градуса.

Погрешность данного метода измерения уменьшается с увеличением расстояния до ориентира. Стоит заметить, что данный метод является наиболее точным и более трудозатратным.

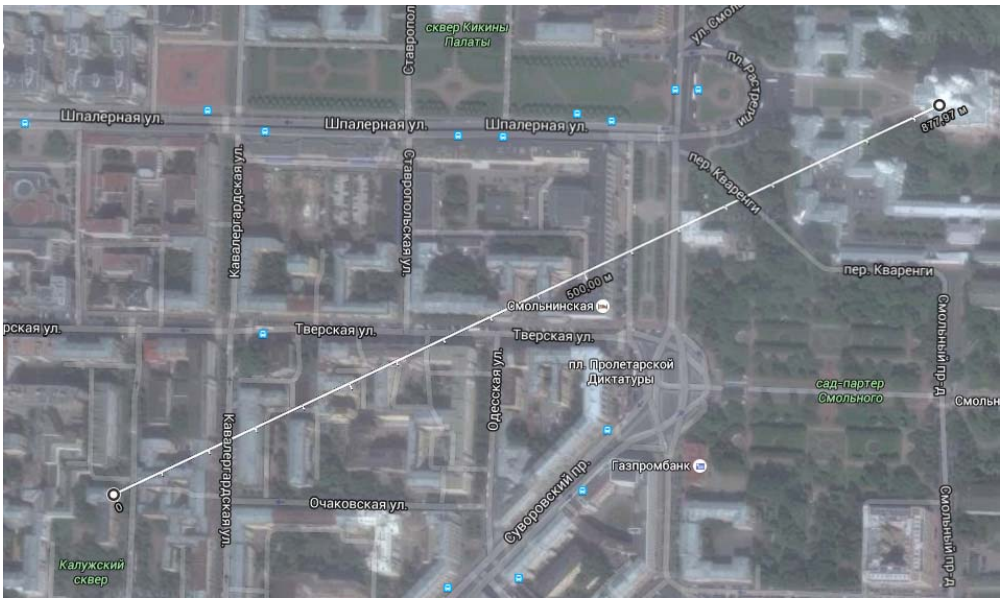


Рис.4. Определение азимута координатным методом

Список используемых источников

1. Бабков В. Ю., Стариков В. В. Планирование сотовой сети мобильной связи на основе технологии LTE [Электронный ресурс] // Актуальные проблемы инфотелекоммуникаций в науке и образовании. IV Международная научно-техническая и научно-методическая конференция: сб. науч. ст. в 2 т. / под ред. С. В. Бачевского, сост. А. Г. Владыко, Е. А. Аникевич, Л. М. Минаков. СПб. : Санкт-Петербургский государственный университет телекоммуникаций им. проф. М. А. Бонч-Бруевича, 2015. С. 33–37. URL: http://www.sut.ru/doci/nauka/4.apino.2015.sut.pdf (дата обращения 17.04.2016).

2. Рыжков А. Е., Сиверс М. А., Бабкин А. С., Пыленок А. М., Трофимов А. П. Сети стандарта LTE. Развитие технологий радиодоступа; СПбГУТ. СПб., 2015. 256 с. ISBN 978-5-89160-123-9.

3. Фокин Г. А. Методика идентификации прямой видимости в радиолиниях сетей мобильной связи 4-го поколения с пространственной обработкой сигналов // Труды научно-исследовательского института радио. М. : НИИР, 2013. Вып. 3. С. 78–82.

4. Киреев А. В., Фокин Г. А. Позиционирование базовой станции в сетях LTE средствами пространственной обработки сигналов [Электронный ресурс] // Актуальные проблемы инфотелекоммуникаций в науке и образовании. III Международная научно-техническая и научно-методическая конференция: сб. научных статей / под ред. С. М. Доценко, сост. А. Г. Владыко, Е. А. Аникевич, Л. М. Минаков. СПб. : Санкт-Петербургский государственный университет телекоммуникаций им. проф. М. А. Бонч-Бруевича, 2014. С. 124–128. URL: http://www.sut.ru/doci/nauka/iiiapino2014.pdf (дата обращения 17.04.2016).

5. Киреев А. В., Фокин Г. А. Пеленгация источников радиоизлучения LTE мобильным пунктом радиоконтроля с круговой антенной решеткой // Труды научно-исследовательского института радио. М. : НИИР, 2015. Вып. 2. С. 68–71.

УДК 621.396(075)

АНАЛИЗ ТРЕБОВАНИЙ К ОБОРУДОВАНИЮ РАДИОКОНТРОЛЯ ПРИ МОНИТОРИНГЕ РАДИОЧАСТОТНОГО СПЕКТРА ДЛЯ ОЦЕНКИ ЭЛЕКТРОМАГНИТНОЙ СОВМЕСТИМОСТИ

Б. М. Антипин, Е. М. Виноградов

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

Анализируются требования, предъявляемые к характеристикам радиоконтрольного оборудования, установленные в Положении о единой технической политике предприятий радиотехнической службы, и их влияние на качество оценки электромагнитной совместимости. Показано, что в целом измерительная аппаратура, удовлетворяющая требованиям единой технической политики, позволяет получать качественную информацию об электромагнитной обстановке, хотя требования к фазовому шуму гетеродина можно ужесточить, поскольку мощные радиочастотные помехи могут существенно снизить качество приема сигнала вследствие эффекта переноса шумов гетеродина.

радиоконтроль, электромагнитная совместимость, радиочастотный спектр, характеристики оборудования радиоконтроля, единая техническая политика.

Одной из задач, решаемых радиоконтролем, является задача обеспечения электромагнитной совместимости (ЭМС) радиоэлектронных средств (РЭС). На этапе эксплуатации РЭС эту задачу радиоконтроль решает посредством измерения параметров излучений и определения местоположения излучателей и сравнения измеренных значений параметров с разрешенными, представленными в базе данных частотных присвоений и РЭС. Однако первым этапом решения этой задачи, на котором должен принимать участие радиоконтроль, является этап частотно-территориального планирования размещения РЭС. На этом этапе радиоконтроль должен

предоставлять информацию об электромагнитной обстановке (ЭМО) в местах предполагаемого размещения антенных систем новых РЭС, которая позволит оценить качество функционирования РЭС, содержащих радиоприемные устройства, в этих местах. Описание ЭМО должно содержать сведения о частотах, на которых обнаружены излучения, значения напряженности поля и ширины спектра излучений на этих частотах, а также информацию о внешнем фоне [1, 2]. В докладе проведен анализ характеристик радиоконтрольного измерительного оборудования с точки зрения их влияния на качество оценки ЭМС РЭС.

Напряженность поля является объективной характеристикой электромагнитного поля, не зависящей от приемной аппаратуры. Однако уровень сигнала на входе приемника, по которому определяется значение напряженности поля, зависит от коэффициента преобразования напряженности поля в напряжение на нагрузке антенны (антенного фактора), потерь в антенно-фидерном тракте (АФТ) и степени согласования антенно-фидерного тракта с антенной и входом измерительного приемника или анализатора спектра. Кроме того, на значение напряженности поля, получаемое по результатам измерения уровня сигнала на входе приемника, влияет также погрешность измерения этого уровня. Высокая точность измерения напряженности поля позволяет при использовании измеренного значения для оценки ЭМС провести более качественный анализ совместимости. Погрешность измерения напряженности электромагнитного поля определяет погрешность оценки отношения сигнал/помеха и уровней мешающих сигналов, которые, в свою очередь, определяют качество работы РЭС, а, следовательно, и ЭМС РЭС в анализируемой ЭМО. И если для аналоговых систем, например систем передачи речи, небольшая погрешность в оценке отношения сигнал/помеха, когда помеха действует по линейным каналам приема, приводит к относительно небольшой погрешности в оценке качества приема речи (разборчивости или индекса артикуляции), то для цифровых систем зависимость качества работы от отношения сигнал/помеха носит пороговый характер, и небольшие погрешности в его оценке могут привести к неправильным выводам относительно наличия или отсутствия ЭМС. Более сложная зависимость между погрешностью измерения напряженности поля и погрешностью в оценке качества работы РЭС имеет место в случае нелинейных эффектов в приемнике, вызванных помехой, когда небольшие погрешности в оценке уровня мешающего сигнала могут приводить к значительным погрешностям в оценке качества работы даже аналоговых РЭС.

В Положении о единой технической политике (ЕТП) предприятий радиотехнической службы [3] установлено требование к погрешности измерения напряженности поля ±3 дБ. При этом погрешность измерения уровня немодулированного радиосигнала на частотах выше 30 МГц при отношении сигнал/шум не менее 20 дБ установлена в пределах ±2 дБ, а погрешности определения антенного фактора и потерь в АФТ не указаны. Учитывая,

что на практике погрешность определения антенного фактора может превышать 1 дБ и такого же порядка может быть погрешность определения потерь в АФТ, получить требуемую погрешность измерения напряженности поля достаточно трудно, а при наличии атмосферных или других внешних помех практически невозможно. Поэтому требование к погрешности измерения напряженности поля, представленное в [3], можно рассматривать как достаточно жесткое и трудно достижимое.

Достоверность информации, получаемой средствами радиоконтроля, которая может быть использована для оценки ЭМС, зависит от технически параметров измерительной аппаратуры, в первую очередь измерительных приемников и анализаторов спектра, а также от условий, в которых выполняются измерения.

Измерительные приемники должны обладать высокой линейностью и большим динамическим диапазоном по основному каналу приема (ОКП). Но и при этом внешняя ЭМО может влиять на результаты измерений.

Обращаясь снова к Положению о ЕТП, заметим, что параметрами, представленными в этом документе, которые определяют линейность приемной аппаратуры, являются точки пересечения по интермодуляции второго и третьего порядка, отнесенные к входу приемника. Точка пересечения третьего порядка, отнесенная к входу приемника, *IP*3, в [3] установлена +10 дБм. Учитывая, что она обычно находится на 10–15 дБ выше точки компрессии 1 дБ, $P_{1\text{дБ}}$, можно найти, что в большинстве случаев для измерительных приемников $P_{1\text{дБ}} \geq -5$ дБм. Чувствительность приемника зависит от используемой ширины полосы ОКП, *BW*. Уровень собственного шума приемника:

$$N[\text{дБм}] = -174 + 10\lg(BW[\text{Гц}]) + NF, \qquad (1)$$

где *NF* – коэффициент шума приемника, дБ.

Так как согласно [3] *NF* = 12 дБ, то (1) приобретает вид:

$$N[\text{дБм}] = -162 + 10\lg(BW[\text{Гц}]). \qquad (2)$$

Теперь из (2) при *BW* =25 кГц *N* = – 118 дБм, а при *BW* = 1 МГц *N* = –102 дБм.

Если чувствительность приемника P_R определяется при отношении сигнал/шум на выходе приемника *S/N* = 12 дБ, то, поскольку $P_R = N - (S/N)$, она будет составлять P_R = –106 дБм при *BW* =25 кГц и P_R = –90 дБм при *BW* = 1 МГц. Отсюда, в рассматриваемых условиях, динамический диапазон по ОКП:

$$D_{\text{ОКП}} = P_{1\text{д Б}} - P_R$$

будет колебаться от $D_{\text{ОКП}}$= –5 + 106 = 101 дБ при *BW* =25 кГц до $D_{\text{ОКП}}$ = –5+90 = 85 дБ при *BW* = 1 МГц.

Учитывая высокие требования к подавлению побочных каналов приема (80 дБ для каналов зеркальных и промежуточных частот), можно сделать вывод, что измерительный приемник, удовлетворяющий требованиям

Положения о ЕТП, обеспечивает измерение уровней сигналов в широком диапазоне их изменений при отсутствии помех за пределами ОКП. Тем не менее, наличие мощных излучений в месте измерений может привести к ошибкам в определении их уровней и соответственно к ошибкам в оценке напряженности поля от этих источников. В этих случаях необходимо обеспечить определенную удаленность измерительной антенны от антенны источника излучений, чтобы получить уровень измеряемого сигнала в пределах динамического диапазона ОКП приемника.

Например, если антенна измерительного приемника располагается на высоте h_R= 10 м, а антенна передатчика на высоте h_T= 30 м, то, используя модифицированную модель Хата для частоты f = 1000 МГц, можно получить, что развязка между антеннами составит, дБ:

$$\text{для города } L_{\text{грд}} = 105,7 + 35,2\lg(d),$$

$$\text{для пригорода } L_{\text{пгрд}} = 95,5 + 35,2\lg(d),$$

где d – расстояние между антеннами, км.

Отсюда, полагая развязку равной 60 дБ, найдем, что для городских условий расстояние между антеннами должно составлять d = 50 м, а для пригорода d = 98 м. Если коэффициент усиления приемной антенны равен 0 дБи и можно пренебречь потерями в антенно-фидерном тракте, то для передатчика с эффективной изотропно излучаемой мощностью P_T = 40 дБм уровень сигнала S на входе приемника на указанных расстояниях будет:

$$S = P_T - 60 = -20 \text{дБм}.$$

Этот уровень лежит ниже верхней границы динамического диапазона по ОКП (–5 дБм), и при измерениях недопустимые искажения отсутствуют. Однако, если данный сигнал не находится на частоте настройки приемника, но лежит в полосе преселектора, то он может создать помеху работе приемника и привести к ошибкам в результатах измерений, в частности, за счет переноса шумов гетеродина.

В [3] уровень фазового шума гетеродина приемника относительно уровня несущей гетеродина установлен L_N = –100 дБн/Гц при отстройке 10 кГц. С увеличением отстройки этот уровень падает и скорость падения может составлять 20 дБ/дек, так что при отстройке 100 кГц спектральная плотность фазового шума может составлять уже –120 дБн/Гц. Однако можно легко убедиться, что помеха указанного выше уровня I = –20 дБм, поступающая на смеситель, даже при полосе BW =25 кГц при отстройке 100 кГц существенно снизит качество работы приемника вследствие эффекта переноса шумов гетеродина, приращение которых составит:

$$\Delta N = I + L_N + 10\lg(BW[\text{Гц}]) = -20 - 120 + 10\lg(25 \cdot 10^3) = -96 \text{дБм}.$$

что на 22 дБ выше собственного шума приемника. Отсюда, в частности, следует, что требования к фазовому шуму приемника можно сделать более жесткими, чтобы уменьшить количество ситуаций, в которых будет проявляться рассмотренный выше эффект. Если обратиться к Справочнику по радиоконтролю, изданному МСЭ в 2011 г. [4], то в нем отсутствуют конкретные цифры, определяющие уровень фазового шума гетеродина измерительного приемника для радиоконтроля. Просто отмечается, что требования к фазовому шуму определяются видом сигналов, которые должны контролироваться, хотя в более ранних изданиях Справочника указывались цифры, совпадающие с цифрами, приведенными в Положении о ЕТП.

Что касается интермодуляционных искажений, то опасные интермодуляционные продукты появляются только при больших уровнях мешающих сигналов. В частности, если два мешающих сигнала имеют одинаковые уровни $I = -20$ дБм, то значение интермодуляционного продукта третьего порядка $PIM3$ составит:

$$PIM3 = 3I - 2IP3 = 3(-20) - 2 \cdot 10 = -80 \text{дБм},$$

что значительно превышает чувствительность приемника. Однако вероятность такой ситуации мала, и если, например, частота интермодуляционного продукта $f_{им} = 2f_1 - f_2$, а мощности мешающих сигналов, образующих этот продукт, составляют соответственно $I_1 = -35$ дБм, $I_2 = -20$ дБм, то

$$PIM3 = 2I_1 + I_2 - 2IP3 = 2(-35) + (-20) - 2 \cdot 10 = -110 \text{дБм},$$

что уже ниже чувствительности приемника.

Таким образом, проведенный анализ требований к техническим характеристикам измерительной аппаратуры, используемой для решения задач радиоконтроля, показывает, что характеристики аппаратуры в целом позволяют получать результаты измерений, которые могут быть использованы для анализа ЭМС. Более жесткие требования можно предъявить только к спектральной плотности фазового шума гетеродина. При наличии мощных излучений в окрестности предполагаемого размещения РЭС с целью проведения измерений, необходимых для анализа ЭМС, места проведения измерений следует выбирать, учитывая характеристики измерительной аппаратуры.

Список используемых источников

1. Антипин Б. М., Виноградов Е. М. Оценка электромагнитной совместимости по результатам радиоконтроля // Известия вузов России. Радиоэлектроника. 2012. Вып. 6. С. 97–104.

2. Антипин Б. М., Виноградов Е. М. Алгоритм оценки электромагнитной совместимости радиоэлектронных средств // Известия вузов России. Радиоэлектроника. 2013. Вып. 1. С. 102–110.

3. Положение о единой технической политике предприятий радиотехнической службы. Приложение к приказу Федеральной службы по надзору в сфере связи, информационных технологий и массовых коммуникаций от 19 декабря 2011 г. № 1131. 82 с.
4. Handbook. Spectrum Monitoring. ITU, 2011. 660 p.

УДК 621.396

ОЦЕНКА ОСНОВНЫХ ОШИБОК СЛЕДЯЩИХ ИЗМЕРЕНИЙ РАДИОЛОКАЦИОННЫХ КОМПЛЕКСОВ РАЗВЕДКИ И КОНТРОЛЯ СТРЕЛЬБЫ

Б. И. Ахмедов[1], А. В. Коряковцев[2], В. В. Смирнов[1]

[1]Балтийский государственный технический университет «ВОЕНМЕХ» им. Д. Ф. Устинова
[2]Военная академия связи им. Маршала Советского Союза С. М. Буденного

В настоящее время в связи с совершенствованием артиллерийских систем и ростом эффективности обычных и специальных боеприпасов актуальной является борьба с артиллерией противника. Эффективность этой борьбы в значительной мере зависит от многоцелевых радиолокационных комплексов разведки и контроля стрельбы, которые по засечкам снарядов и мин на траектории определяют координаты огневых позиций противника, а также корректируют огонь своей артиллерии. В данной статье рассмотрены основные источники ошибок следящих измерителей радиолокационных комплексов разведки, выявлены наиболее существенные из них, которые необходимо учитывать при оценке эффективности комплекса.

радиолокационный комплекс разведки, фазированная антенная решетка, следящие измерители, ошибки.

Сложность радиолокационных комплексов разведки (РКР), удовлетворяющих требованиям современных боевых действий, обусловлена, во-первых, тем, что эти комплексы должны обнаруживать, распознавать и определять с высокой точностью координаты множества малоразмерных целей в сложной обстановке (при наличии радиоэлектронного и огневого противодействия, многолучевого распространения радиоволн, значительной тропосферной рефракции, мощных пассивных помех и пр.). Во-вторых, РКР должен при минимуме затрат времени автоматически определять координаты огневых позиций противника с учётом данных о рельефе местности и передавать эти данные в систему управления огнём. В-третьих, комплекс должен обладать высокой боеготовностью, мобильностью, малым весом и габаритами.

Основным показателем РКР является точность. Точность комплекса определяется, в основном, следящим измерителем направления (СИН)

и дальности (СИД). У современных РКР она достигает нескольких десятков метров на дальностях до 30 км [1].

По источнику возникновения ошибки следящих измерителей классифицируются четыре группы.

1. Ошибки, вносимые целью:

– систематические (динамическое отставание);

– стохастические (вариации динамического отставания и ошибки, вызываемые шумами цели).

2. Ошибки, вносимые каналом передачи:

– систематические (из-за тропосферной рефракции);

– стохастические (обусловленные нерегулярностью тропосферной рефракции).

3. Ошибки, обусловленные несовершенством аппаратуры РКР:

– систематические (ошибки антенной системы, ошибки из-за не идеальности узлов приемного устройства, и т. д.);

– стохастические (тепловой шум приемника, многолучевое распространение радиоволн, аппаратурные нестабильности).

4. Ошибки, обусловленные помехами.

Ограниченный порядок астатизма следящего измерителя приводит к появлению динамической ошибки, которая при известной траектории цели и параметрах следящего измерителя может быть учтена [2].

Шумы цели также приводят к ошибкам СИН и СИД. Амплитудный шум (АШ) цели слабо влияет на работу СИД и моноимпульсных СИН. Но при наличии ошибки запаздывания в следящем измерителе приводит к дополнительной ошибке, величина которой существенно зависит от быстродействия схемы автоматической регулировки усиления (АРУ) и составляет единицы процентов от ошибки запаздывания [2]. АШ обычно учитывают на больших и средних дальностях.

На малых дальностях основной причиной ошибки СИН всех типов является угловой шум (УШ) цели. Среднеквадратическое значение угловой ошибки СИН, обусловленной УШ, определяется по формуле [2]:

$$\delta_y = \frac{Z_0}{R\sqrt{2}},$$

где Z_0 – эквивалентный радиус случайных перемещений распределенных отражающих участков цели по отношению к угловой координате геометрического центра цели; R – дальность до цели.

При априорно известных траекториях движения и матрицах рассеяния целей при использовании РКР на полигоне можно учесть ошибки, обусловленные шумами цели. При отсутствии этих априорных данных можно лишь оценить величину случайной составляющей ошибки РКР, обусловленной целью.

Канал передачи для РКР, работающих в нижнем слое тропосферы, является источником значительных ошибок. Наибольшее влияние при этом оказывает тропосферная рефракция. Для оценки ошибок, обусловленных рефракцией, необходимо знать значение преломления воздуха *n*, являющегося функцией географического положения пункта на земной поверхности, погоды, времени года и суток.

Для характерных условий работы РКР величина систематической ошибки измерения дальности, вызванной тропосферной рефракцией может достигать десятков метров и являться прямой функцией угла места цели и влажности воздуха [3]. Систематическая ошибка измерения угла места цели зависит от кажущегося угла места цели, её высоты, влажности воздуха и составляет десятые доли градуса. Азимутальной ошибкой, обусловленной рефракцией, можно пренебречь, т.к. величина этой ошибки не превышает 0,1 мрад в облачные дни и 0,03 мрад – в ясную погоду [3].

Систематические ошибки, обусловленные рефракцией, можно скорректировать путем применения рефракционных профилей, основанных на метеоданных. При этом ошибка по дальности может быть сведена до долей метра, но для этого необходимо знать параметры атмосферы на всех участках траектории цели [2]. В полном объеме эта задача может быть решена лишь в условиях полигона. Частичная компенсация ошибок может быть проведена путем использования метеоданных в месте расположения РКР.

В многоцелевых РКР в качестве антенных систем используются фазированные антенные решётки (ФАР). Характерной особенностью ФАР является расширение главного лепестка диаграммы направленности (ДН) при отклонении луча от нормали на угол θ по закону [2]:

$$\theta_{0,5}(\theta) = \theta_{0,5} / \cos(\theta),$$

где $\theta_{0,5}$ – ширина главного лепестка ДН на уровне половинной мощности. Влияние изменения ширины главного лепестка ДН ФАР при сканировании на точность измерений может быть легко учтено. Разработана обобщенная модель ФАР [4], позволяющая определить параметры ДА ФАР любого вида зависимости от погрешности работы элементов решетки. Это позволяет учесть влияние погрешностей элементов ФАР на точность СИН.

Одним из основных факторов, ограничивающих точность пеленгации в ФАР, является дискретное фазирование. Максимальная угловая ошибка при этом определяется формулой [5]:

$$\delta_{y\max} \cong (d / 2\pi)\theta_{0,5},$$

где *d* – дискрет фазирования. Обычно величина $d/2\pi = 0{,}125 - 0{,}25$, поэтому угловые ошибки могут быть недопустимо большими. В принципе, систематические угловые ошибки ФАР могут быть определены эмпирически

или вычислены для каждого углового направления и использованы для коррекции выходных данных СИН, но этот путь требует значительной ёмкости памяти ЭВМ.

Причиной угловых ошибок моноимпульсных СИН является также не идеальность характеристик радиоприемных устройств: не идентичность амплитудно-фазовых характеристик отдельных каналов, несовершенство работы АРУ и т. п. [6]. Для наиболее распространенных амплитудных суммарно-разностных СИН систематическая угловая в типичном случае равна 0,35°–1,27°. Для уменьшения ошибок пеленгации, вызванных несовершенством приемных устройств, используют разнообразные методы: конструктивные, технологические и эксплуатационные [6].

Систематические ошибки, обусловленные несовершенством аппаратуры РКР, могут быть определены методами полунатурного моделирования и натурных испытаний и использованы для коррекции выходных данных РКР.

Одной из основных причин случайных ошибок следящих измерителей на больших дальностях является шум приемника. Величина случайной угловой ошибки, вызванной шумом при $S/N > 1$, определяется формулой:

$$\delta_y = \frac{\theta_{0,5}}{\sqrt{(2S/N)(F_n/\beta_n)}},,$$

где δ_y измеряется в радианах. А величина случайной ошибки дальности определяется по формуле:

$$\delta_g = \frac{\tau_n}{\sqrt{(S/N)(F_n/\beta_n)}},$$

где *S/N* – отношение сигнал/шум по мощности, F_n – частота повторения, β_n – ширина полосы пропускания следящей системы, τ_n – длительность импульса, выраженная в эквивалентной дальности (1 мкс = 150 м) [3].

Характерными для РКР являются ошибки, обусловленные многопутным распространением радиоволн. Наиболее существенной является угломестная ошибка, определяемая выражением:

$$\delta_y = \frac{\rho \cdot \theta_{0,5}}{\sqrt{8A_S}},$$

где δ_y измеряется в радианах, ρ – коэффициент отражения от подстилающей поверхности (по напряжению), A_s – коэффициент ослабления боковых лепестков по мощности [3].

Анализ известных видов помех [7] показывает, что для РКР наиболее вероятным из организованных помех являются шумовые помехи, а из естественных помех – отражения от подстилающей поверхности.

Ошибка малоимпульсной станции по обобщенной координате Z, вызванная помехой, оценивается по формуле [8]:

$$\delta_Z = \frac{(\Delta/\Sigma)\cdot i\cdot\sqrt{\eta}}{K_Z\sqrt{(2S/I)n_e}},$$

где $(\Delta/\Sigma)i$ – отношение усиления разностного канала по координате Z к усилению суммарного канала при данном положении сигнала помехи, η – коэффициент эффективности суммарного канала, K_Z – крутизна разностного канала, (S/I) – отношение сигнал/помеха, n_e – количество независимых выборок помех. Для защиты РКР от пассивных помех широко используются СДЦ и цифровые карты помех [7]. Кроме того, в РКР возможно использование следящих адаптивных доплеровских фильтров для выделения сигналов.

Из этого следует, что:

1. Для обеспечения высокой точности РКР необходим учет ошибок следящих измерителей, корректировка результатов измерений и применение специальных конструктивных мер.

2. Могут быть вычислены или определены эмпирически следующие систематические ошибки: динамическое отставание (при априорно известной траектории), ошибки из-за тропосферной рефракции, ошибки ФАР и ошибки, вызванные аппаратурными погрешностями РКР.

3. Из случайных ошибок при оценке точности РКР необходимо учитывать: амплитудный и угловой шумы цели, тепловой шум приемника, многопутное распространение радиоволн, активные и пассивные помехи.

Список используемых источников

1. Бабий Б. РЛС засечки огневых позиций // Техника и вооружение. 1981. N 3. С. 36–37.

2. Справочник по радиолокации / под ред. М. Скольника: Т. 1–4. М. : Советское радио, 1976–78.

3. Современная радиолокация (анализ, расчет и проектирование систем) : пер. с англ. / ред. Ю. Б. Кобзарев. М. : Советское радио, 1969. 704 с.

4. Михеев С. М., Попов В. В. Исследование обобщенной модели фазируемой антенной решетки // Изв. вузов «Радиоэлектроника». 1978. Т. XXI. N 2. С. 62–68.

5. Зимин Д. Б., Лосев В. С., Седенков Е. Г., Унуков Л. В. О точностных характеристиках антенных решеток с дискретными фазовращателями // Радиотехника. 1975. Т. 30. N 6. С. 53–56.

6. Леонов А. И., Фомичев К. И. Моноимпульсная радиолокация. М. : Советское радио, 1970. 392 с.

7. Бобнев М. П., Кривицкий Б. Х., Максимов М. В. и др. Защита от радиопомех / под ред. М. В. Максимова. М. : Советское радио, 1976. 496 с.

8. Бартон Д., Вард Г. Справочник по радиолокационным измерениям / под ред. М. М. Вейсбейна. М. : Советское радио, 1976. 392 с.

УДК 621.397

ПОСТРОЕНИЕ СЕТИ НАЧАЛЬНОГО ПРИБЛИЖЕНИЯ СТАНДАРТА LTE НА ОСНОВЕ КЛАСТЕРНЫХ СТРУКТУР

В. Ю. Бабков, В. В. Стариков

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

Статья посвящена процессу синтеза сети начального приближения стандарта LTE. Сформулирована задача построения оптимальной сети начального приближения с точки зрения выполнения требований по пропускной способности и уровню внутрисистемной интерференции. Приведены результаты оценок внутрисистемной интерференции для кластеров с жестким и дробным повторным назначениями частотного ресурса.

планирование стандартов связи четвертого поколения, частотный кластер, пропускная способность, абонентская емкость, бюджет потерь.

Основную сложность в планировании сетей стандарта LTE составляет построение сети начального приближения [1]. Это обуславливается тем, что именно на данном этапе производится поиск такой сетевой структуры, где обеспечение требуемых абонентской емкости и пропускной способности будет решаться за счет размещения минимально-возможного количества базовых станций (БС) определенной конфигурации. Таким образом, для решения задачи построения сети начального приближения прежде всего следует выработать подходы получения максимально точных оценок сетевой емкости и пропускной способности.

Благодаря технологии внутрисотовой координации помех ICIC *(Inter-cell Interference Coordination)* сеть LTE обладает возможностью в режиме реального времени управлять выделенным частотно-временным ресурсом. В зависимости от сложившейся ситуации система способна производить координацию внутрисистемных помех и тем самым по факту реализовывать сценарии построения сети на основе адаптивных кластерных структур [2, 3]. Такой вариант управления сетевыми ресурсами также позволяет в определенных пределах производить балансировку нагрузки между соседними сотами. Однако следует отметить тот факт, что возможности такой адаптации весьма ограничены, т. к. результат будет определяться не только сложившимися на данный момент распределением абонентов и профилем трафика, но и заложенными при строительстве сети пространственно-техническими параметрами. Определение этих параметров начинается на этапе решения задачи построения сети начального приближения и уточняется на этапе сетевой оптимизации [4].

Оценить предполагаемую пропускной способность будущей сети можно с помощью бюджета потерь, рассчитав распределение скоростных зон в соте с учетом частотного диапазона, ширины полосы, параметров оборудования, типа местности и пр. Стоит отметить, что такой расчет практически не учитывает помеховую обстановку, поскольку ее учет ограничивается лишь добавлением некого рекомендуемого запаса.

Для учета внутрисистемной интерференции при расчете скоростных зон соты необходимо задаться окружением БС (т. е. фактически зафиксировать кластерную структуру), которая позволит оценить уровень внутрисистемных помех и получить второе распределение скоростей, только уже рассчитанное, исходя из помеховой обстановки. За оцениваемый критерий кластерных структур в условиях внутрисистемных помех будем принимать вероятность *P(C)* невыполнения требуемого отношения полезного сигнала к суммарной помехе и шуму приемника SINR *(Signal Interference + Noise Ratio)* для заданной модуляционно-кодирующей схемы MCS *(modulation and coding scheme)* в точке приема [5].

$$P(C) = \frac{1}{\sqrt{2\pi}} \int_{z'}^{\infty} e^{\frac{z^2}{2}} dz, \text{ где } z' = \frac{10\lg(\frac{1}{\beta e}) - (\frac{c}{n})_{thr}}{\sqrt{\sigma^2 + \sigma_e^2}},$$

где β_e – суммарная эквивалентная нормированная помеха в точке анализа от всех учитываемых в модели источников на данной частоте (полосе), σ – СКО логарифма сигнала, зависящее от условий распространения на местности, σ_e – СКО логарифма уровня эквивалентной помехи, $(c/n)_{thr}$ – граничное отношение с/п, [дБ]. При проведении расчетов примем $(c/n)_{thr} = 9$дБ, что не принципиально, т. к. методика расчета инвариантна типу MCS.

Вероятности *P(C)* в кластерных структурах будем оценивать в точках, соответствующих наихудшим условиям передачи/приема от обслуживающей БС до мобильного терминала: в точке А на границе «дальней» зоны соты (или просто на границе соты при жестком назначении частот) и в точке В на границе «ближней» зоны соты (в случае кластеров с дробным и мягким назначениями частот). На рисунке 1 изображено расположение точек анализа А и В на примере фрагмента сети, построенного на основе несекторированной кластерной структуры с дробным повторным назначением частот.

При рассмотрении помеховой обстановки ограничимся ближайшим помеховым окружением, под которым будем понимать только соты (сектора/зоны) соседних кластеров, работающих на той же частоте, что и сота (сектор/зона) анализа. На рисунке 2 изображена помеховая обстановка для «ближней» зоны одной из сот, где «жирным» и «пунктирным» стрелкам соответствуют помехи от «дальних» и «ближних» зон ближайшего помехового окружения соответственно.

Таким образом, задаваясь различными MCS с соответствующими им SINR, можно судить о их применимости на границе соты с точки зрения внутрисистемной интерференции в выбранной кластерной структуре размерностью *(C, M),* где *C* – число БС в кластере, а *M* – число секторов в кластере. В таблице 1 приведены результаты расчетов вероятностей *P(C)* при SINR = 9 дБ для кластеров с жестким и дробным повторным назначениями частотного ресурса. Расчеты проводились для сельской (σ = 4), пригородной (σ = 7) и городской (σ = 10) местностей.

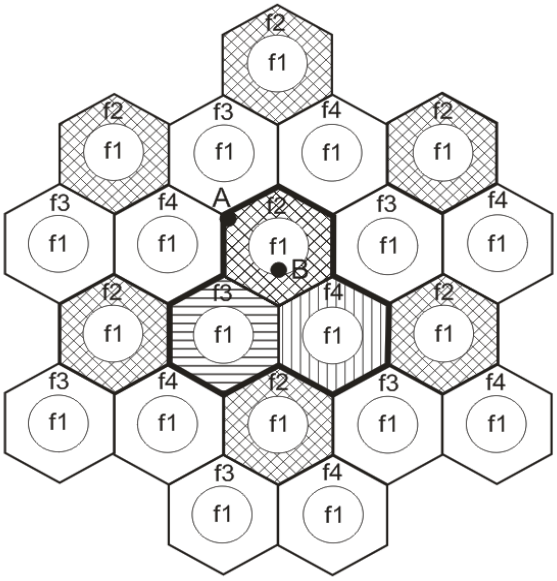


Рис. 1. Фрагмент сети на основе кластера с дробным повторным назначением частот

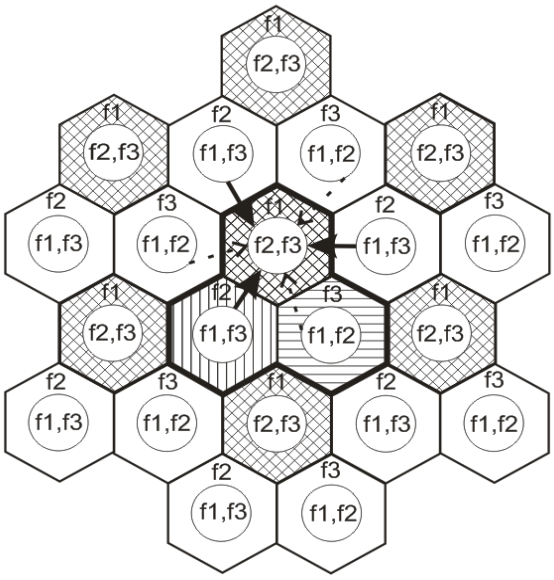


Рис. 2. Фрагмент сети на основе кластера с мягким повторным назначением частот

ТАБЛИЦА. Результаты расчетов вероятностей P(C) для кластеров с жестким и дробным повторным назначениями частотного ресурса

Отношение радиуса «ближней» зоны к *R*сот (*r0/R*)	σ, дБ	Точка анализа на границе «ближней» зоны (точка «А»)	Точка анализа на границе соты (точка «В»)
Кластер с жестким повторным назначением частотного ресурса (*C* = 3; *M* = 3)			
–	4	–	48,3
–	7	–	49,0
–	10	–	49,3
Кластер с дробным повторным назначением частотного ресурса (*C* = 3; *M* = 9)			
0,3	4	1,7 %	2,9 %
	7	11,2 %	15,6 %
	10	19,6 %	23,7 %

Изложенная выше модель оценки уровня внутрисистемных помех направлена на решение задачи синтеза (определение конфигурации по заданным параметрам *P(C)* и SINR) кластерной структуры сети начального приближения стандарта LTE и также позволяет определить радиус действия для любой MCS, выраженный в относительном расстоянии *r/R*. Таким образом, рассчитанный уровень внутрисистемных помех для различных конфигураций кластерных структур и процедура расчета бюджета потерь являются необходимыми условиями для максимально точной оценки пропускной способности сети LTE.

Список используемых источников

1. Бабков В. Ю., Цикин И. А. Сотовые системы мобильной радиосвязи: учеб. пособие. 2-е изд. перераб. и дополн. СПб. : БХВ-Петербург, 2013. 432 с. ISBN 978-5-9775-0877-3.

2. Рыжков А. Е., Воробьев В. О., Слышков А. С., Сиверс М. А., Гусаров А. С., Шуньков Р. В. Стандарты и сети радиодоступа 4G. – СПб. : Линк, 2012. 226 с. ISBN 978-98595-032-8.

3. Степутин А. Н., Ромашенков Н. О., Фокин Г. А. Разгрузка сетей LTE через сети Wi-Fi. // Научно-технический вестник информационных технологий, механики и оптики. 2015. Т. 15. № 6. С. 1139–1146.

4. Бабков В. Ю., Никитина А. В., Стариков В. В. Определение пространственно-технических параметров сотовой сети стандарта LTE // НТВ СПбГПУ. Информатика. Телекоммуникации. Управление. 2015. № 1 (212). С. 7–15.

5. Фокин Г. А., Стариков В. В. Оценка показателей функционирования радиосети LTE средствами имитационного моделирования // Неделя науки СПбПУ. Материалы научного форума с международным участием. Институт физики, нанотехнологий и телекоммуникаций; В. Э. Гасумянц, Д. Д. Каров – ответственные редакторы. 2015. С. 37–40.

УДК 621.391.25

ФОРМИРОВАНИЕ СИГНАЛЬНО-КОДОВЫХ КОНСТРУКЦИЙ ДЛЯ DVB-T2

П. А. Башмаков[1], Д. Д. Капралов[2], Д. И. Кирик[2]

[1]Холдинг РТ Electronics

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

Рассматриваются вопросы помехоустойчивости в многолучевом канале при передаче сигналов цифрового телевидения DVB-T2. Предлагается подход к решению задачи оптимизации формирования сигнально-кодовой конструкции.

стандарт DVB-T2, цифровое телевещание, сигнально-кодовые конструкции.

DVB-T2 – цифровая система эфирного вещания, разработанная в рамках проекта DVB [1]. Эта система использует новейшие методы модуляции и кодирования для обеспечения высокоэффективного использования ограниченного спектра с целью предоставления аудио и видео служб, а также служб передачи данных стационарным, портативным и мобильным устройствам. В DVB-T2 используется OFDM модуляция, предусматривается большое количество различных режимов, что обеспечивает устойчивый прием сигнала. Для выполнения коррекции ошибок в DVB-T2 применяется каскадное кодирование: внутренний код с низкой плотностью проверок на четность (LDPC) и внешний код – код Боуза-Чоудхури-Хоквингема (БЧХ), а также битовое перемежение, что обеспечивает устойчивый сигнал и высокое качество в условиях с высоким уровнем шумов и помех. Основные характеристики стандарта представлены в таблице.

ТАБЛИЦА. Основные характеристики DVB-T2

Параметр	Значение параметра
Первичная модуляция несущих	QPSK, 16-QAM, 64-QAM, 256-QAM
Скорость кода	1/2, 3/5, 2/3, 3/4, 4/5, 5/6
Защитный интервал	1/128, 1/32, 1/16, 19/256, 1/8, 19/128, 1/4
Количество несущих OFDM: – при нормальной полосе – при расширенной полосе	 1К, 2К, 4К, 8К, 16К, 32К 8К, 16К, 32К
Варианты размещения распределенных пилот сигналов	PP1, PP2, PP3, PP4, PP,5 PP6, PP7, PP8
Полоса канала	8 МГц
Поворот созвездия	Нормальный, Повернутый

При передаче сигналов цифрового телевидения возникают эффекты, характерные для распространения радиоволн: многолучевое распространение радиоволн в следствие наличия препятствий и формирования задержек между копиями сигнала в точке приема, медленные и быстрые замирания из-за кратковременного или длительного снижения уровня сигнала в точке приема. Для снижения влияния этих явлений и повышения помехоустойчивости системы передачи применяют сигнально-кодовые конструкции (СКК), в основе которых лежат операции отображения информационной последовательности в кодовую путем внесения избыточности и кодовой последовательности в канальную заданием манипуляционного кода. Получаемый при этом энергетический выигрыш от кодирования зависит от степени увеличения минимального сигнального расстояния между разрешенными кодовыми блоками.

В стандарте DVB-T2 изменена методика канального кодирования, что обеспечивает лучшую помехоустойчивость, в сравнении с предыдущей версией стандарта, в многолучевых каналах, характерных для городской застройки. В стандарте определены 8 новых режимов распределения пилот-сигналов для различных комбинаций длительности защитного интервала и видов первичной модуляции поднесущих, что позволило адаптивно перестраивать режимы вещания под специфику канала связи и гибко решать проблемы частотного планирования сети. В части борьбы с пик-фактором используются две новые методики – расширение активного созвездия и резервирование пилот-тона, позволяющие снизить пик-фактор без увеличения ошибок и внеполосного излучения.

Для борьбы с многолучевостью в сигналах используются различные методы. В результате, если сигналы, пришедшие по разным путям, перекрываются во времени, то между ними возникает интерференция, которая в свою очередь вызывает глубокие замирания результирующего сигнала. В стандарте DVB-T2 используется техника поворота сигнального созвездия на определенный круговой угол. Эта процедура означает, что сформированный модуляционный символ поворачивается в комплексной плоскости на определенный угол, зависящий от числа уровней модуляции (29° для QPSK16; 8° для 16-QAM; 8,6° для 64-QAM и arctg(1/16) для 256-QAM). Более того, перед началом вращения квадратурная (*U*2) координата каждого модуляционного символа циклически сдвигается в рамках одного кодового слова (т. е. берется из предыдущего символа этого слова, *U2*-компонента первого символа становится равной *U2*-компоненте последнего).

После поворота сигнального созвездия (рис.) у каждой точки – уникальные *U2* и *U1* координаты. Некоторые из координат оказываются достаточно близко друг к другу, но по одной координате точки всегда можно восстановить другую ее координату. А механизм сдвига *U2* координаты приводит к тому, что исходные координаты сигнальной точки оказываются в разных модуляционных символах (т. е. заведомо на разных поднесущих), что существенно снижает вероятность их одновременной деградации как из-за случайных импульсных помех, так и по причине селективных затуханий в канале.

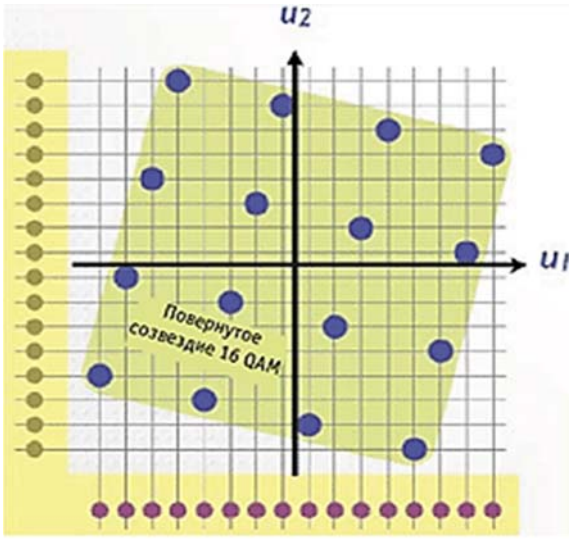


Рисунок. Сигнальное созвездие 16-QAM после поворота

Такой поворот может существенно повысить устойчивость сигнала при типичных проблемах эфира [3, 4]. За счет поворота диаграммы на точно подобранный угол каждая точка созвездия приобретает уникальные координаты (*U1* и *U2*), не повторяемые остальными точками.

Каждая координата точки обрабатывается в модуляторе отдельно, и они передаются в OFDM-сигнале отдельно друг от друга, замешиваясь с *U2* и *U1* другого символа (т. е. *U2* и *U1* могут передаваться на разных OFDM_несущих и в разных OFDM_символах). В приемнике *U2* и *U1* опять объединяются, формируя исходное созвездие сигналов, сдвинутое по кругу. Таким образом, если одна несущая или символ будут потеряны в результате интерференции, сохранится информация о другой координате, это позволит восстановить символ, хотя и с более низким уровнем сигнал/шум. При использовании симметричного (не повернутого) сигнального созвездия разнесение *U2* и *U1* смысла не имеет потому, что символ может быть распознан только по сочетанию двух координат. Каждая из них в отдельности имеет двойников, и уникально только их сочетание.

Поворот созвездия сигналов на угол θ является линейным изометрическим преобразованием, при котором сохраняется евклидово расстояние. Однако при повороте созвездия может меняться расстояние между проекциями на оси абсциссы и ординаты. В работе [2] показано, что в условиях воздействия аддитивного белого гауссовского шума (АБГШ) поворот сигнального созвездия на угол θ приводит к снижению помехоустойчивости сигнальной конструкции. Воздействие АБГШ на входе приемника исключить невозможно, поэтому шумовая составляющая будет, очевидно, влиять на принятие решения о значении проекций сигнала на оси координат.

Пусть задано созвездие сигналов QAM-N, тогда число точек на осях координат будет $K = log_2 N$. Обозначим расстояние между соседними проекциями сигнала на ось x как $Dx_{i,i+1}$, где $i = 1,..K-1$, обозначим расстояние между соседними проекциями сигнала на ось y как $Dy_{i,i+1}$, где $i = 1,..K-1$, тогда задачу определения оптимального угла поворота сигнального созвездия можно представить в виде следующего выражения:

$$\max_{\Theta \epsilon [0,\frac{\pi}{2}]} \min(Dx_{i,i+1}, Dy_{i,i+1}, i = 1,..K-1).$$

Таким образом, задача определения оптимального угла поворота созвездия сигналов сводится к максимизации минимального расстояния между соседними координатами точки пространства сигналов. Решение данной задачи позволит вычислять оптимальный угол поворота θ пространства сигналов для различных видов модуляции и не использовать эмпирические значения, а в перспективе применять адаптивную систему передачи цифрового телевидения в зависимости от помеховой обстановки.

Список используемых источников

1. ETSI EN 302 755 V1.4.1 (2015-07) Структура кадра, канальное кодирование и модуляция для системы цифрового наземного ТВ вещания второго поколения (DVB-T2). URL: http://www.etsi.org/deliver/etsi_en/302700_302799/302755/01.04.01_60/en_ 302755v 010401p.pdf (дата обращения: 18.01.16).

2. Савищенко Н. В. Специальные интегральные функции, применяемые в теории связи. СПб. : Изд-во Политехн. ун-та. 2011. 560 с.

3. Polak L., Kratochvil T. Performance of the Rotated Constellation in DVB-T2 // The Seventh International Conference on Digital Telecommunications ICDT 2012. Brno, Czech Republic. PP. 84–87.

4. Perez-Calderon D., Oria C., Garcia J., Lopez P., Baena V., Lacadena L. Rotated Constellations for DVB-T2 // XXIV Design of Circuits and Integrated Systems Conference. Zaragoza, Nov. 18–20, 2009. PP. 187–191.

УДК 621.376

ПРИНЦИП ФОРМИРОВАНИЯ РАДИОСИГНАЛА НА ОСНОВЕ ПРОГРАММНО УПРАВЛЯЕМОГО МОДУЛЯ ФОРМИРОВАНИЯ С ПРИМЕНЕНИЕМ МЕЖКАНАЛЬНЫХ КВАДРАТУРНЫХ СВЯЗЕЙ

Г. С. Боголепов, А. А. Михеев

Военная академия связи им. Маршала Советского Союза С. М. Буденного

В последнее время стало актуальным использование спутниковых систем связи для обеспечения передачи информации в труднодоступных районах, где сегмент GSM развит слабо или не развит вообще. Существует проблема обеспечения электромагнитной совместимости, с работающими в соседних диапазонах частот, РЭС. Предложено использовать универсальный способ формирования радиосигнала, на основе квадратурного формирователя с применением спектрально эффективных видов цифровой модуляции.

радиочастотный ресурс, комплексная огибающая, элементарный импульс.

В системах спутниковой связи, системах связи с космическими аппаратами (КА), а также системах спутникового геопозиционирования остро стоит вопрос об эффективном использовании выделенной полосы частот, при строгом дефиците частотного ресурса (РЧР). А также обеспечение электромагнитной совместимости с другими радиоэлектронными средствами (РЭС), работающими в соседних диапазонах частот, при сохранении необходимого уровня мощности сигнала и скорости передачи данных.

Для решения актуальных проблем рассматривается подход использования спектрально-эффективных сигналов специальной формы, таких как

GMSK и FQPSK. При использовании таких сигналов, уровень флуктуации огибающей сигнала является постоянным, либо максимально к нему приближенным, что обеспечивает высокую устойчивость к воздействиям нелинейных искажений в оконечных каскадах передающего устройства, снижая мощность взаимных помех путем подавления первого бокового лепестка спектральной плотности мощности радиосигнала. Основой идеи является реализация универсального квадратурного модулятора, на основе теории комплексной огибающей радиосигнала.

Так как в радиосвязи для передачи информации используются полосовые сигналы, то будем оперировать несколькими необходимыми понятиями. Информационный сигнал – цифровая информация, изображение, речь. Полосовой сигнал – сигнал, спектр которого сосредоточен в районе несущей частоты.

Таким образом полосовой сигнал имеет следующее математическое представление (1):

$$s(t)=a(t)\cdot\cos(\Phi(t))=a(t)\cdot\cos(\omega_0 t+\varphi(t))\,. \qquad (1)$$

При рассмотрении понятия комплексной огибающей и представлении сигнала в векторном виде, выражение принимает вид (2):

$$z(t)=a(t)\cdot\cos(\omega_0 t+\varphi(t))+j\cdot a(t)\cdot\sin(\omega_0 t+\varphi(t))\,. \qquad (2)$$

Из выражения (2) следует, что $R[z(t)]=s(t)$ реальная часть комплексного сигнала соответствует полосовому радиосигналу. По формуле Эйлера выражение (2) имеет вид (3):

$$z(t)=a(t)\cdot\exp(j(\omega_0 t+\varphi(t)))=a(t)\cdot\exp(j\varphi(t))\cdot\exp(j\omega_0 t)\,. \qquad (3)$$

Сигнал $z(t)=z_m(t)\cdot\exp(j\cdot\omega_0\cdot t)$ носит название комплексной огибающей сигнала $z(t)$, а $z_m(t)$ можно представить в виде реальной и мнимой частей (4):

$$z_m(t)=a(t)\cdot\exp(j\cdot\varphi(t))=a(t)\cdot\cos(\varphi(t))+j\cdot a(t)\cdot\sin(\varphi(t))\,, \qquad (4)$$

где $I(t)=a(t)\cdot\cos(\varphi(t))$ – синфазная составляющая комплексной огибающей, а $Q(t)=a(t)\cdot\sin(\varphi(t))$ – квадратурная составляющая.

На основе того, что исходный модулирующий сигнал является низкочастотным, формирование комплексной огибающей можно производить в цифровом виде. Способ формирования комплексной огибающей в зависимости от модулирующего сигнала определяет вид модуляции. Схема, представленная на рисунке, подходит для всех цифровых видов модуляций.

При анализе современных систем связи с космическими аппаратами, выявлен ряд спектрально-эффективных видов модуляции на основе QPSK.

Хотя QPSK можно считать квадратурной манипуляцией (QAM-4), иногда её проще рассматривать в виде двух независимых модулированных не-

сущих, сдвинутых на 90°. При таком подходе чётные (нечётные) биты используются для модуляции синфазной составляющей I, а нечётные (чётные) – квадратурной составляющей, несущей Q. Так как BPSK используется для обеих составляющих несущей, то они могут быть демодулированы независимо.

Рисунок. Универсальный квадратурный модулятор

Существует ряд работ, где показана возможность объединения схем формирования перечисленных выше спектрально-эффективных радиосигналов в одном устройстве, в том числе сигналов с фазовой и частотной манипуляцией.

Анализ известных источников показывает, что подобное объединение реализуемо на основе схемы генерации T-OQPSK-сигналов, из-за того, что T-OQPSK сам по себе не спектрально-эффективный вид манипуляции. Изменение формы элементарного импульса на импульс вида:

$$p_1 = \sin^2\left(\frac{\pi t}{2T_s}\right) \cdot \mathrm{rect}\left(\frac{t}{2T_s}\right), \qquad (5)$$

где rect(t) = 1 при $0 \le t \le 1$ и rect(t) = 0 при $t \ge 1$. Однако подобный подход приводит к увеличению уровня флуктуации огибающей, что вызывает нелинейные искажения радиосигнала. Более эффективным механизмом сокращения уровня флуктуаций огибающей при сохранении высокой спектральной эффективности и помехоустойчивости является внесение взаимосвязи между синфазной и квадратурной составляющими комплексной огибающей OQPSK-радиосигнала посредством нелинейного преобразования. Данный вид модуляции получил название FQPSK [1, 2].

Применяя проектирование на ПЭВМ с использованием пакета Matlab, получены результаты моделирования. В моделировании основными параметрами являлись коэффициенты усиления глубины квадратурных связей A_1 и A_2, n – пик-фактор сигнала, ΔF_{99} – ширина полосы занимаемых частот (ШПЗЧ), γ – ослабление первого бокового лепестка, J – джиттер-эффект (нежелательное частотное или фазовое дрожание цифрового сигнала), R – раскрыв глазковой диаграммы. Результаты эксперимента сведены в таблицу.

В рамках работы выполнены исследования эффективности сигналов, получены их временные диаграммы, сигнальные созвездия, спектры плотности мощности, «глазковые» диаграммы.

Произведён расчёт полос нормированных частот относительно длительности бита (1,4–2,04), пик-фактора сигналов (1,006–1,16), ослабление первого бокового лепестка (28–31 дБ), раскрытие «глазковой» диаграммы (0,68–1) и полученный нулевой джиттер J [3, 4].

ТАБЛИЦА. Параметры экспериментальных сигналов

Сигнал	A_1	A_2	n	ΔF_{99}	γ, дБ	J	R
T-OQPSK	1	1	1,16	1,4	31	0	1
FQPSK	0,7104	0,6873	1,019	1,6	28	0	0,68
GMSK(BT = 0,3)	0,5209	0,8536	1,006	1,8	38	0	0,85
GMSK(BT = 0,5)	0,3261	0,9454	1,025	2,04	39	0	0,95

Список используемых источников

1. Прокис Д. Цифровая связь: пер. с англ. / под ред. Д. Д. Кловского. М. : Радио и связь. 2000. 800 с.: ил.

2. Феер К. Беспроводная цифровая связь. Методы модуляции и расширения спектра. М. : Радио и связь, 2000. 520 с. ISBN 5-256-01444-7.

3. Сергиенко А. Б. Цифровая обработка сигналов : учеб. для вузов. СПб. : Питер, 2002. 608 с.: ил. ISBN 5-318-00666-3.

4. Потемкин В. Г. MatLab 5 для студентов : справ. пособие. М. : АО «Диалог-МИФИ», 1998. 314 с.: ил.

Статья представлена старшим научным сотрудником Военной академии связи, кандидатом технических наук А. С. Дворниковым.

УДК 621.396.96

ИССЛЕДОВАНИЕ МНОГОЛУЧЕВОГО ПЕЛЕНГАТОРА

Е. Г. Борисов, О. С. Голод, С. Г. Егоров

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

Рассмотрен метод определения азимута и дальности до судовой радиолокационной станции по нескольким последовательным измерениям угла и доплеровской частоты. Приведены приближенные оценки точности определения координат, полученные путем имитационного моделирования.

многолучевой пеленгатор; обнаружение целей; измерение координат; доплеровская частота, радиолокационная станция, точность.

Задача определения местоположения источника радиоизлучения пеленгатором представляет значительный интерес для радиоразведки, навигации и др. Рассмотрим задачу определения координат судовой радиолокационной станции (РЛС) пассивным многолучевым пеленгатором (МП) [1]. Если априорно принять, что курс и скорость судна – носителя пеленгуемой когерентной РЛС не меняются в течение всего интервала измерений, то по принимаемому антенной МП сигналу можно определить курс судна, скорость, азимут и дальность.

Рассмотрим методику измерений. Зондирующие импульсы судовой РЛС периодически, с периодом, определяемым скоростью вращения антенны РЛС, принимаются соответствующими парами лучей МП, реализующими моноимпульсный метод пеленгации. При этом непрерывно измеряются:

– $\beta_0, \beta_1, \beta_2, \ldots, \beta_i, \ldots, \beta_N$ – азимуты судна, соответствующие последовательным оборотам антенны РЛС в моменты приема зондирующих сигналов антенной МП;

– f_{np} – частота принимаемого импульсного сигнала РЛС;

– T_n – интервал времени между началом наблюдения $t_0 = 0$ и текущим циклом наблюдения за судном-носителем РЛС.

Геометрическая интерпретация задачи иллюстрируется рисунком 1, где судно в момент времени $t_0 = 0$ находится в точке А.

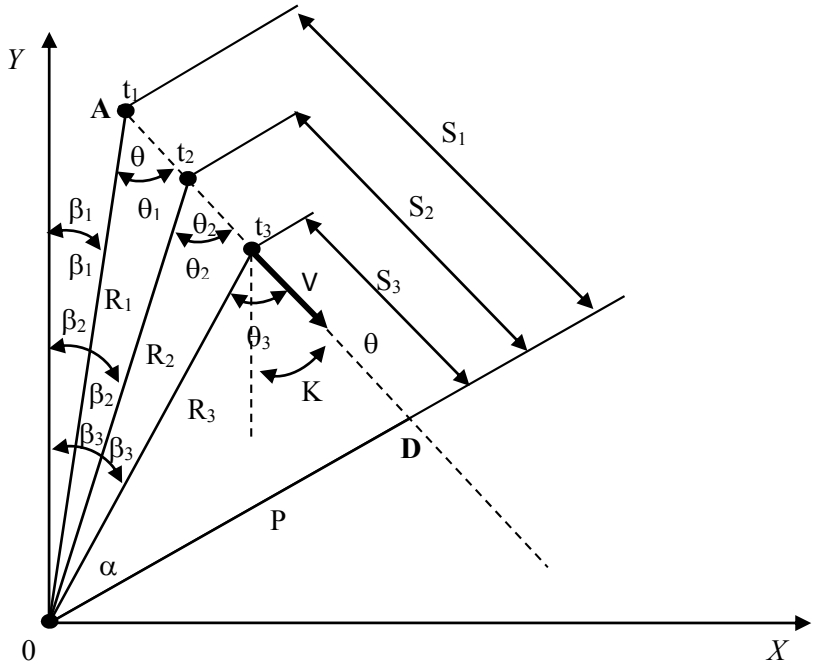


Рис. 1. Геометрическая интерпретация задачи определения угломерных параметров движения судна пассивным моностатическим пеленгатором АПРЛ

Из геометрии рисунка 1 выразим разности углов азимута β_i, измеряемые моноимпульсным методом, как

$$\Delta\beta_{21}=\beta_2-\beta_1,\ \Delta\beta_{31}=\beta_3-\beta_1,\ \Delta\beta_{32}=\beta_3-\beta_2,$$

а также их связь с углом θ:

$$\theta_2-\theta_1=\beta_2-\beta_1=\Delta\beta_{21},\ \theta_3-\theta_1=\beta_3-\beta_1=\Delta\beta_{31};\ \theta_3-\theta_2=\beta_3-\beta_2=\Delta\beta_{32}.$$

Учитывая гипотезу о прямолинейном и равномерном движении объекта для трех моментов времени получим:

$$ctg\theta_1=\frac{S_1}{P},\ ctg\theta_2=\frac{S_2}{P},\ ctg\theta_3=\frac{S_3}{P},$$

$$\text{или } ctg\theta_1=\frac{S_3+V\left(T_{12}+T_{23}\right)}{P},\ ctg\theta_2=\frac{S_3+VT_{23}}{P},\ ctg\theta_3=\frac{S_3}{P}.$$

Выразим величину $\frac{ctg\theta_2-ctg\theta_3}{T_{23}}=\frac{V}{P}$, где $P = OD$,

тогда:

$$ctg\theta_1-ctg\theta_3-\left(ctg\theta_2-ctg\theta_3\right)\frac{\left(T_{12}+T_{23}\right)}{T_{23}}=0 \text{ или}$$

$$\frac{\cos\theta_1}{\sin\theta_1}-\frac{\cos\theta_3}{\sin\theta_3}-\left(\frac{\cos\theta_2}{\sin\theta_2}-\frac{\cos\theta_3}{\sin\theta_3}\right)\frac{\left(T_{12}+T_{23}\right)}{T_{23}}=0$$

$$\frac{\cos\theta_1}{\sin\theta_1}-\frac{\cos\theta_3}{\sin\theta_3}-\left(\frac{\cos\theta_2}{\sin\theta_2}-\frac{\cos\theta_3}{\sin\theta_3}\right)\frac{\left(T_{12}+T_{23}\right)}{T_{23}}=0$$

опуская промежуточные выкладки, запишем

$$\cos\theta_1\sin\theta_2\sin\theta_3-\cos\theta_3\sin\theta_1\sin\theta_2-k_T\sin\theta_1\left(\cos\theta_2\sin\theta_3-\cos\theta_3\sin\theta_2\right)=0,$$

учитывая, что

$$\theta_2-\theta_1=\beta_2-\beta_1=\Delta\beta_{21},\ \theta_3-\theta_1=\beta_3-\beta_1=\Delta\beta_{31};\ \theta_3-\theta_2=\beta_3-\beta_2=\Delta\beta_{32},$$

Учитывая, что $T_{12} = T_{23} = T$ получим:

$$\theta_3=arctg\left[\frac{\sin\left(\Delta\beta_{32}\right)\sin\left(\Delta\beta_{31}\right)}{2\sin\left(\Delta\beta_{32}\right)\cos\left(\Delta\beta_{31}\right)-\sin\left(\Delta\beta_{31}\right)\cos\left(\Delta\beta_{32}\right)}\right]. \quad (1)$$

Рассмотрим способ измерения скорости судна. Частота $f_{пр}$ сигнала принимаемого антенной МП, описывается соотношением

$$f_{\text{пр}}=f_{\text{И}}\left[1+\left(v/c\right)\cos\theta_i\right], \quad (2)$$

где: $f_И$ – частота излученного РЛС сигнала; $f_{пр}$ – частота принимаемого сигнала при i-ом измерении; Θ_i – угол между вектором скорости и линией визирования судна.

По соотношению (1) определяем угол между вектором скорости движения судна и линией визирования судна.

В формуле (2) неизвестны частота $f_И$ сигнала, излучаемого РЛС, и скорость v судна. Следовательно, проведя, как минимум три измерения, β_1, β_2, β_3 азимута судна и два измерения $f_{пр}$ – частоты принимаемого сигнала можно определить скорость судна. Решив систему уравнений, составленных для различных значений Θ_i и f_{np}, получим

$$v = c\frac{f_{пр2} - f_{пр1}}{f_{пр1}\cos\Theta_2 - f_{пр2}\cos\Theta_1} \qquad (3)$$

Для обеспечения достаточной точности измерений частоты $f_{пр}$ принимаемого сигнала необходимо использовать систему фазовой автоподстройки частоты, которая должна успевать входить в режим синхронизма за время пачки импульсов, принимаемых в течение времени прохождения антенной РЛС направления на МП [2]. Измерив интервал T времени между использованными измерениями, определим дальность R_3 до РЛС из треугольника Ot_2t_3 по теореме синусов

$$R_3 = \frac{vT_{23}\sin(\Theta_3 - \Delta\beta_{32})}{\sin\Delta\beta_{32}}. \qquad (4)$$

Рассмотренная методика позволяет определить координаты движущейся судовой РЛС кругового обзора посредством пассивного многолучевого пеленгатора всего за три оборота антенны РЛС. Результаты моделирования приведены ниже.

Рассмотри линейное движение ИРИ при различном начальном положении цели. Пусть цель движется прямолинейно со скоростью v = 10 м/с, курсовой угол K = 5, период измерений T = 10 с. Начальная точка движения цели имеет координаты X_0= –50 км, Y_0 = 50, 30 и 10 км. СКО определения азимута $\sigma\beta$ = 1 град. Цифрами на рисунке 2 и рисунке 3 обозначены траектории движения цели для 1 – Y_0 = 10 км, 2 – Y_0 = 20 км, 3 – Y_0 = 30 км, 4 – Y_0 = 40 км, 5 – Y_0 = 50 км.

СКО определения относительной дальности R_3 до цели при использовании процедур (1)–(4) и различных начальных положениях цели представлены на рисунке 3. Цифрами отмечены траектории цели согласно рисунка 2.

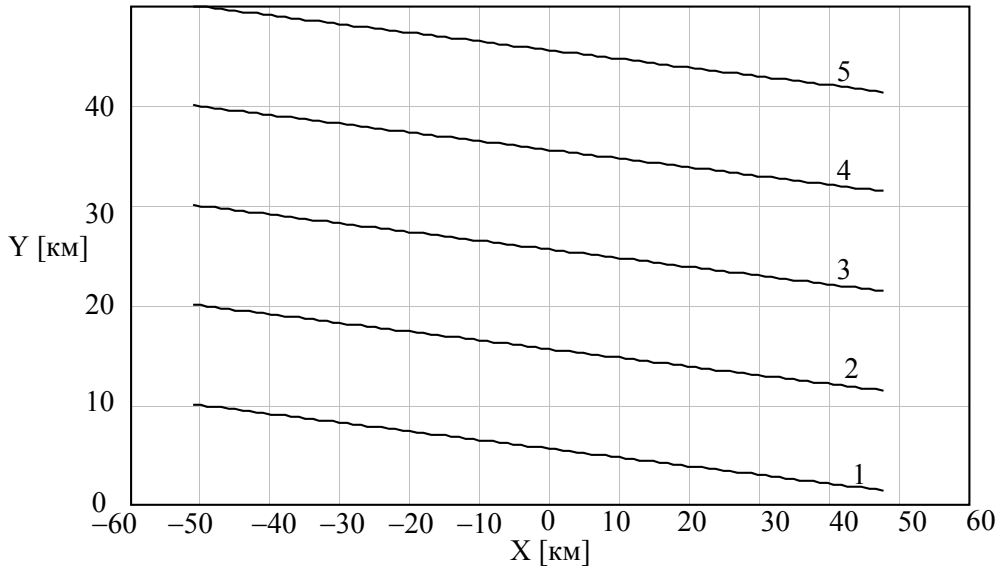


Рис. 2. Геометрическая интерпретация задачи моделирования

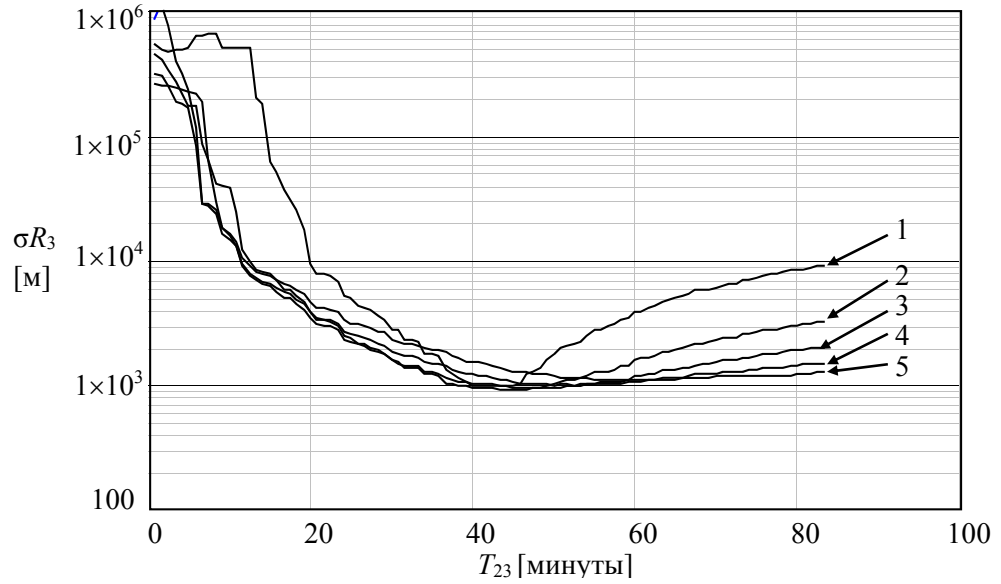


Рис. 3 СКО определения дальности R_3

Список используемых источников

1. Меньшаков Ю. К. Теоретические основы технических разведок: учеб. пособие / под ред. Ю. Н. Лаврухина. М. : Изд-во МГТУ им. Н. Э. Баумана, 2008. 536 с.: ил. ISBN 978-5-7038-3019-2.

2. Прусс Е. Ш., Голод О. С. Устройство фазовой автоподстройки частоты. А. с. 145359 Б СССР, МПК: H03L 7/00. № 47725/14; заявл. 23.01.86; ОПУБЛ. 23.01.89. Бюл. № 3.

УДК 621.396.96

ЭКСПЕРИМЕНТАЛЬНЫЙ СТЕНД ОЦЕНКИ ТОЧНОСТИ ПОЗИЦИОНИРОВАНИЯ ИСТОЧНИКОВ РАДИОИЗЛУЧЕНИЯ НА ОСНОВЕ ПРОГРАММНО-КОНФИГУРИРУЕМОГО РАДИО

Е. Г. Борисов, Г. М. Машков, Г. А. Фокин

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

В статье представлена экспериментальная оценка точности позиционирования источников радиоизлучения на основе алгоритма многопозиционной кооперативной обработки дальномерных измерений с накоплением. Экспериментальный стенд выполнен средствами программно-конфигурируемого радио на аппаратной платформе NI USRP в программной среде LabVIEW, где реализована передача, прием и обработка сигналов. Эксперимент проводился в стационарных условиях и показал точность в единицы метров в зависимости от числа накоплений.

кооперативная обработка в многопозиционной системе, дальномерные измерения, программно-конфигурируемое радио, испытательный стенд, среднеквадратическая ошибка, USRP, LabVIEW.

Задача позиционирования возникает в радиолокационных и радионавигационных системах, а также системах мобильной связи, когда измерению и оцениванию подлежат дальномерные параметры. Разностно-дальномерный метод используется для позиционирования абонентских станций в сетях мобильной связи LTE и оценка показателей его функционирования позволяет сделать вывод о точности в единицы-десятки метров [1, 2, 3]. В радиолокационных и радионавигационных системах, когда объект позиционирования переизлучает навигационные сигналы, возможна организация суммарно-дальномерных измерений с последующим их накоплением и комплексированием.

Исследование путей повышения точности позиционирования в многопозиционной радиотехнической системе за процедур кооперативной обработки избыточных измерений представлено в работах [4, 5, 6, 7, 8] и позволяет сделать следующие выводы: 1. При организации кооперативной обработки дальномерных и суммарно – дальномерных измерений в формировании результирующих оценок наклонных дальностей участвуют все отсчеты, взятые с определенным весом. 2. Накопление данных на одной позиции приводит к естественному увеличению точности определения параметров, точность оценивания дальностей на других улучшается с меньшим приростом в зависимости от способа обработки измерений. 3. Накопление данных на всех позициях приводит к пропорциональному увеличению точности всех оцениваемых параметров.

Для экспериментальной верификации полученных аналитических результатов был разработан испытательный стенд сбора и обработки навигационных измерений для трех приемопередающих станций, каждая из которых принимает ретранслированные собственные зондирующие сигналы и сигналы, излучаемые другими станциями системы. Функции станций и объекта наблюдения реализованы на основе модельно-ориентированного проектирования средствами программно-конфигурируемого радио [9, 10, 11] на платах NI USRP-2932 [12]: три платы работают в режиме приемо-передающих позиций, а одна плата – в режиме объекта наблюдения. Для организации кооперативной обработки измерений устройства, входящие в состав стенда сбора и обработки измерений, соединены в локальную сеть по схеме, представленной на рисунке 1.

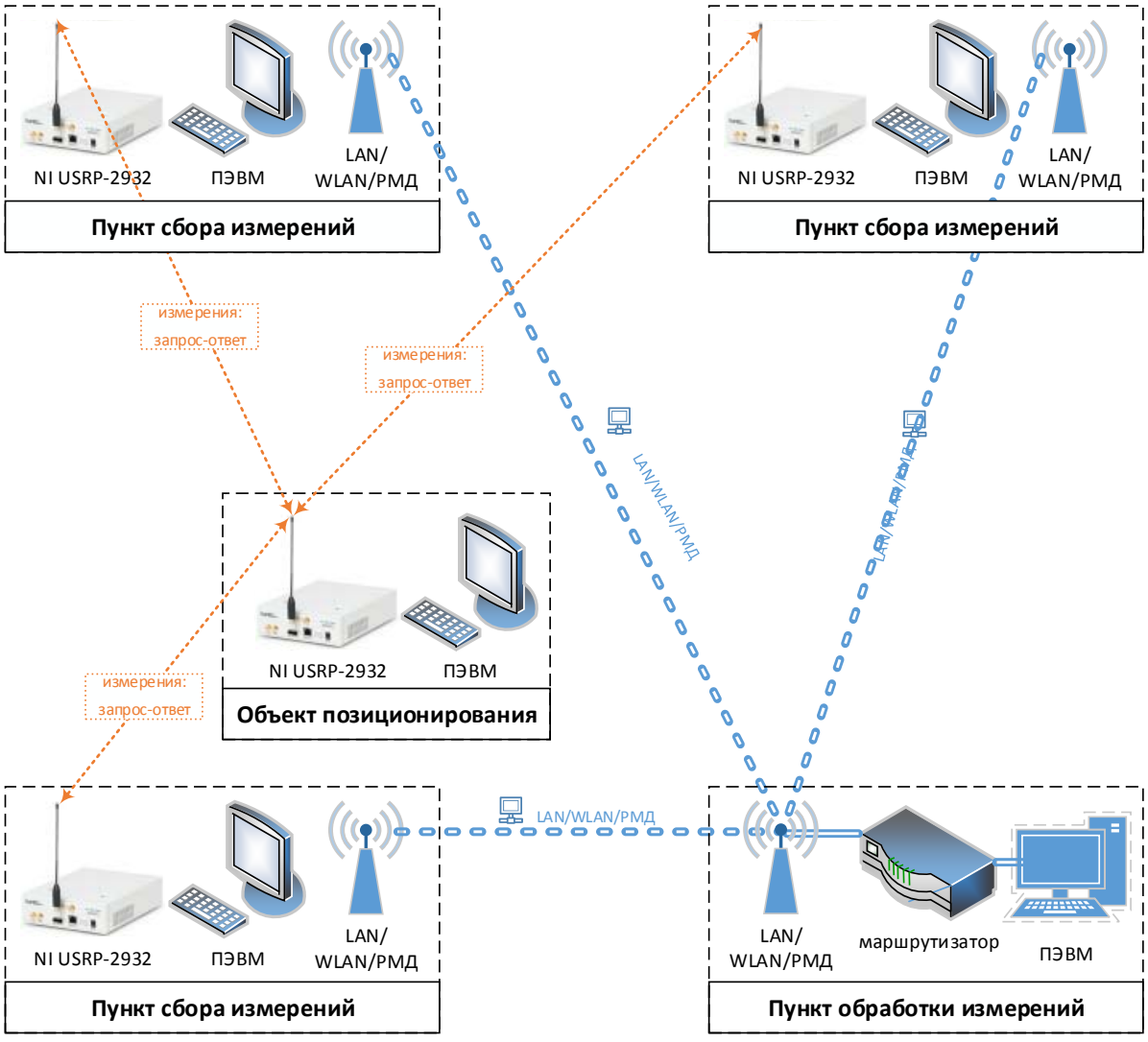


Рис. 1. Сетевая организация устройств испытательного стенда сбора и обработки навигационных измерений

Пользователь работает на компьютере с установленной библиотекой драйверов Act_Pos: этот компьютер называется Клиентом и является пунктом обработки измерений. На удаленных компьютерах работают Серверы (*Server*), которые являются пунктами сбора измерений (три USRP устройства). Состав программно-аппаратного обеспечения стенда сбора и обработки навигационных измерений представлен в таблице. Программное обеспечение (ПО) для реализации всех процедур обработки реализовано в среде LabVIEW [13].

Аппаратный состав пункта сбора измерений включает SDR-плату NI USRP-2932, ПЭВМ и сетевой интерфейс для организации связи с пунктом обработки измерений. В качестве сетевого интерфейса может использоваться беспроводной Radio Ethernet Wi-Fi. В состав программного обеспечения (ПО) пункта сбора измерений входит специальное программное обеспечение (СПО) Server. Аппаратный состав пункта обработки измерений включает ПЭВМ и сетевой интерфейс для организации связи с тремя пунктами сбора измерений. В состав ПО пункта обработки измерений входит СПО Active Positioning. Аппаратный состав объекта позиционирования включает ПЭВМ и SDR-плату NI USRP-2932. В состав ПО объекта позиционирования входит СПО Repeater. При проведении отладочных испытаний допускается использовать СПО Active Positioning и Repeater на одной ПЭВМ.

ТАБЛИЦА. Состав программно-аппаратного обеспечения испытательного стенда сбора и обработки навигационных измерений

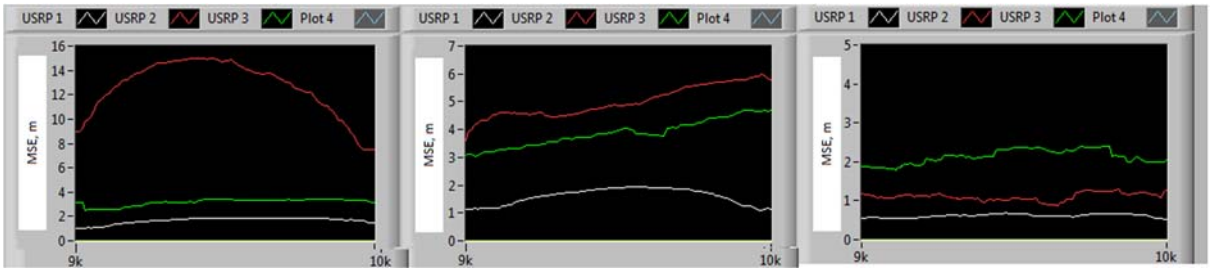
	Состав аппаратного обеспечения	Состав СПО	Реализуемые функции
Пункт сбора измерений	NI USRP-2932, ПЭВМ, LAN/WLAN интерфейс	Server	Запрос-ответ на измерения по командам СПО Active Positioning
Пункт обработки измерений (клиент)	LAN/WLAN интерфейс, маршрутизатор, ПЭВМ	Active Positioning	Кооперативная обработка измерений
Объект позиционирования	NI USRP-2932, ПЭВМ	Repeater	Запрос-ответ на измерения по командам СПО Server

СПО Active Positioning – это инструмент для нахождения местоположения объекта. В данном случае объектом позиционирования является Active Repeater (активный повторитель), который переизлучает сигнал с известным временем запаздывания.

Система работает следующим образом. Первый USRP излучает сигнал, принимаемый и переизлучаемый повторителем. Ретранслированный сигнал принимается первой и другими двумя позициями, что позволяет получить

одно измерение дальности и два измерения суммы расстояний. Одновременно этот сигнал принимается другими позициями, что приводит к генерации запросных сигналов с этих блоков. Процессы излучения и приема сигналов второй и третьей позицией аналогичны, что позволяет получить дополнительно два измерения наклонной дальности и четыре измерения суммы расстояний. Когда сигналы от всех USRP приняты, пункт обработки измерений (СПО Server) оценивает местоположение ретранслятора (СПО Repeater). Эксперимент проводился следующим образом: три станции были территориально разнесены на расстояние в десятки метров.

На рисунке 2 приведены СКО определения дальности дальномерных и суммарно-дальномерных измерений при различных способах их кооперативной обработки.



а) б) в)

Рис. 2. СКО определения дальности по результатам эксперимента:
а) каждой из позиций; б) каждой из позиций при кооперативной обработке всей совокупности полученных однократных измерений; в) при кооперативной обработке этой же совокупности из десяти измерений каждое

Измерения проведены при средней мощности излучения 100 мВт, несущей частоте 433 МГц, с модуляцией по фазе псевдослучайной последовательностью на основе кодов Голда с 1024 дискретами. Расстояние между преимо–передающим позициями выбрано 100 м, а геометрия их расположения близка к равностороннему треугольнику. Устройство имитирующее бортовой ответчик в точке пересечения медиан. На рисунке 5 обозначено: а) СКО определения дальности относительно каждой из позиций, б) СКО определения дальностей относительно каждой из позиций при кооперативной обработке всей совокупности полученных однократных измерений; в) СКО определения дальностей при кооперативной обработке этой же совокупности из десяти измерений каждое.

Анализ графиков, представленных на рисунке 2 позволяет сделать вывод о том, что кооперативная обработка всей совокупности полученных однократных измерений позволяет повысить точность измерений по сравнению со случаем определения дальности относительно каждой из позиций,

а повышение числа измерений до 10 при кооперативной обработке позволяет еще больше уточнить полученные результаты для случая однократных измерений.

Для уточнения выводов конкретными количественными показателями необходимо оценить вклад погрешности, вносимой асинхронной сетевой организацией испытательного стенда, что представляется крайне затруднительным, однако даже при такой организации трех станций получаемый выигрыш очевиден.

Работа выполнена при финансовой поддержке Минобрнауки России в рамках федеральной целевой программы «Исследования и разработки по приоритетным направлениям развития научно-технологического комплекса России на 2014–2020 годы» по проекту «Разработка экспериментального образца многопозиционной автономной радио-технической быстроразворачиваемой системы наземной инфраструктуры воздушного транспорта для посадки летательных аппаратов на неподготовленные площадки» (уникальный идентификатор проекта – RFMEF160714X0057).

Список используемых источников

1. Sivers M., Fokin G. LTE Positioning Accuracy Performance Evaluation // Lecture Notes in Computer Science. 2015. Vol. 9247. pp. 393–406.

2. Сиверс М. А., Фокин Г. А. Духовницкий О. Г., Позиционирование абонентских станций в сетях мобильной связи LTE разностно-дальномерным методом // Системы управления и информационные технологии. 2015. Т. 59. № 1. С. 55–61.

3. Фокин Г. А. Оценка точности позиционирования абонентских станций в сетях LTE разностно-дальномерным методом //Актуальные проблемы инфотелекоммуникаций в науке и образовании. IV Международная научно-техническая и научно-методическая конференция: сборник научных статей в 2 томах. 2015. Т. 1. С. 170–173.

4. Борисов Е. Г., Машков Г. М., Турнецкий Л. С. Повышение точности определения координат цели при реализации кооперативной обработки в многопозиционной радиолокационной системе // Радиотехника. 2013. № 5. С. 4–9.

5. Борисов Е. Г., Машков Г. М. Получение максимально правдоподобных оценок координат целей при кооперативной обработке дальномерно-угломерной информации // Известия вузов России. Радиоэлектроника. 2012. Вып. 3. С. 84–92.

6. Борисов Е. Г., Анцев Г. В., Лебедев И. А. Потенциальная точность оценивания дальности в многопозиционной радиолокационной системе при реализации процедур кооперативной обработки информации // Наукоемкие технологии. 2015. Том 16. № 5. С. 31–37.

7. Mashkov G. M., Borisov E. G., Vladyko A. G., Gomonova A. I. The Use of Software-Defined Radio Systems in Multilateral Navigation Radio Systems // Infocommunications Journal. 2015. Vol. VII. N. 2. pp. 26–31.

8. Mashkov G., Borisov E., Fokin G. Experimental Validation of Multipoint Joint Processing of Range Measurements via Software-Defined Radio Testbed // 18th International Conference on Advanced Communication Technology (ICACT) 2016. pp. 268–273.

9. Фокин Г. А., Буланов Д. В., Волгушев Д. Б. Модельно-ориентированное проектирование систем радиосвязи на основе ПКР // Вестник связи. 2015. № 6. С. 26–31.

10. Фокин Г. А., Лаврухин В. А., Волгушев Д. А., Киреев А. В. Модельно-ориентированное проектирование на основе SDR // Системы управления и информационные технологии. 2015. Т. 60. № 2. С. 94–99.

11. Волгушев Д. Б., Киреев А. В., Фокин Г. А. Модельно-ориентированный синтез систем радиосвязи на основе программно-конфигурируемого радио // Актуальные проблемы инфотелекоммуникаций в науке и образовании. IV Международная научно-техническая и научно-методическая конференция: сборник научных статей в 2 т. 2015. Т. 1. С. 50–53.

12. NI USRP-2932 Datasheet. URL: http://www.ni.com/datasheet/pdf/en/ds-355 (дата обращения 14.04.2016).

13. LabVIEW. URL: http://www.labview.ru (дата обращения 14.04.2016).

УДК 621.396.96

ПРИМЕНЕНИЕ ПРОСТРАНСТВЕННО-ВРЕМЕННЫХ ИЗЛУЧЕННЫХ СИГНАЛОВ ДЛЯ ОПРЕДЕЛЕНИЯ КООРДИНАТ ЦЕЛЕЙ В БИСТАТИЧЕСКОЙ ЛОКАЦИОННОЙ СИСТЕМЕ

Е. Г. Борисов, С. С. Поддубный

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

В статье рассматривается вариант пространственно-временной обработки сигналов в бистатической радиолокационной системе позволяющий реализовать дополнительные измерения угловых координат и повысить точность определения местоположения объектов

бистатическая радиолокационная система, пространственно-временной сигнал, угломерная информация, суммарно-дальномерно-угломерный, триангуляция, точность определения координат.

Интенсивное развитие миниатюрных беспилотных летательных аппаратов (МБПЛА) вызванное технологическим прорывом в области микродвигателей различного типа, мехатроники, микросистемотехники, совершенствование систем управления и передачи данных, разработки энергоемких источников энергопитания позволяет создать аппараты способные выполнять полеты на значительное расстояние. Такие МБПЛА могут легко попасть в руки различных группировок и могут создать определенные проблемы объектам государственной инфраструктуры и по своей сути прямо или косвенно являться объектами террористических угроз [1].

Серьезную опасность для воздушных судов (ВС) представляют МБПЛА находящиеся в зоне аэропорта, поскольку могут создать серьезные проблемы при взлете или посадке авиалайнеров. Для функционирования

всех типов гражданских ВС требуются аэродромы, оснащённые необходимой службой с информационными датчиками, обеспечивающими диспетчера необходимой информацией для безопасного управления транспортными потоками, как в воздухе, так и на лётном поле [2].

Технические требования к вновь разрабатываемым системам обзора летного поля и управлением воздушных судов и транспортных средств по аэродрому регламентировано [3].

Целью статьи анализ точности определения координат воздушных объектов (ВО) в бистатических РЛС с использованием дополнительной линии положения основанной на измерении угла облучения цели с передающей позиции излучающей пространственно-временной сигнал. Рассматриваемая бистатическая система может являться дополнительным средством контроля воздушного пространства в зоне аэродрома.

Анализ литературы. Важной особенностью бистатических радиолокационных станций (БРЛС) является высокая вероятность обнаружения ВО за счет увеличения эффективной площади рассеяния целей (ЭПР) вблизи линии передатчик – приемник называемой базой. Размер области где наблюдается явление резкого увеличения величины бистатической ЭПР ВО (до 40 дБ) происходит при значениях бистатических углов, лежащих в диапазоне 150–180 град. Пояснение физической природы этого эффекта обосновано в [4, 5, 6, 7].

В работах [8, 9] рассмотрены варианты радиолокационных способов определения параметров движения объекта БРЛС использующих монохроматический зондирующий сигнал. Рассмотренные методы измерения координат ВО имеют ряд характерных недостатков, а именно:

отсутствие возможности определения местоположения цели до пересечения ею линии базы без применения специальных алгоритмов;

низкая точность определения координат, вызванная необходимостью экстраполяции доплеровской частоты на значительное время, что при малом времени наблюдения вызывает рост ошибок, особенно при следовании воздушного объекта вдоль линии базы или при совершении им маневра;

неоднозначность определения траекторных параметров, связанная с симметрией поверхностей положения (эллипсоидов) относительно перпендикулярной к линии базы плоскости, проведенной через ее середину, т. е. две различные траектории, симметричные относительно упомянутой плоскости, порождают одинаковые и неразличимые интерференционные сигналы биений;

высокая чувствительность измерений к отклонениям угловой координаты и отклонениям поверхности положения в непосредственной близости от линии базы.

В работах [10, 11, 12, 13] рассмотрены способы определения координат ВО лишенные данных недостатков, а определение координат объекта осно-

вано на использовании двухчастотного фазового способа или с использованием информации об угле, под которым облучается цель с использованием частотного «окрашивания» угловых направлений зондирования.

Недостатком данных способов является использование монохроматического сигнала предопределяет низкую скрытность системы и возможность постановки уводящих по частоте помех, что подразумевает сложность измерения дальности.

Рассмотрим способ определения местоположения цели за счет использования сложных пространственно – временных излученных сигналов модулированных псевдослучайной последовательностью (ПСП). Это позволит решить следующие задачи: повысить скрытность системы, а, следовательно, ее помехозащищенность и живучесть, а также измерить координаты цели различными способами, обеспечив кроме измерения угловых координат цели и разности расстояний на приемной позиции, а также угла под которым облучается цель с передающей позиции.

В бистатических РЛС параметры зоны обзора зависят от дальности обнаружения, которая определяется соотношением [6]:

$$R_1^2 R_2^2 = \frac{P_{\text{изл}} G_T G_R F_T^2 F_R^2 \lambda^2}{(4\pi)^3 q_{\text{пор}} \eta_T \eta_R k T_0 N_0} \sigma_b(\beta_b) = K^2,$$

где: $P_{\text{изл}}$ – излученная мощность; G_T, G_R – коэффициенты усиления антенн передающей и приемной позиции; F_T^2, F_R^2 – множители учитывающие направленные свойства антенных систем на передачу и прием; $\sigma_b(\beta_b)$ – бистатическая ЭПР; η_T, η_R – потери в трактах излучения и приема соответственно; $q_{\text{пор}}$ – пороговое отношение сигнал/шум; k – постоянная Больцмана ($k = 1{,}3806488 \cdot 10^{-23}$ Дж/К); T_0 – шумовая температура; N_0 – спектральная плотность мощности шумов; R_1 и R_2 – расстояния облучатель – цель и цель – приемная позиция.

В [4] для приближенной оценки ЭПР как функции угла β_b предложена формула $\sigma(\beta_b) = \sigma\{1 + exp[n|\beta_b| - (2,4n+1)]\}$, причем $\beta_b = \arccos\left[\frac{1}{2R_1R_2}\left(R_1^2 + R_2^2 - L^2\right)\right]$, где L – база РРС; n = 7–10-эмпирический коэффициент, определяемый конфигурацией и сложностью отражающего объекта.

Дальность до цели в бистатических системах (рис. 1) определяется формулой:

$$R_1 = \frac{\Delta R^2 + 2\Delta R L}{2(\Delta R + L(1 - \cos\varepsilon_1 \cos\beta_1))}.$$

где: $\Delta R = R_1 + R_2 - L$.

Вероятность правильного обнаружения цели D при фиксированном уровне ложной тревоги F определяется как $D = F^{\frac{1}{1+0,5q^2}}$ [14].

На рисунке 1 БРЛС контроля летного поля имеет зону обзора в пределах которой расположена взлетно-посадочная полоса (ВПП) смещённая на некоторое расстояние от базы. Такое расположение вызвано компромиссом точностью измерения координат, которые измеряются с худшей точностью в окрестности линии базы [7, 8], но при этом достигается наибольшее значение отношения сигнал/шум [4, 5, 6], а, следовательно, и наивысшая вероятность обнаружения.

На рисунке 2 приведена упрощенная структурная схема бистатической РЛС, где определение траекторных параметров основано на дополнительной информации получаемой за счет знания угла, под которым облучается ВО.

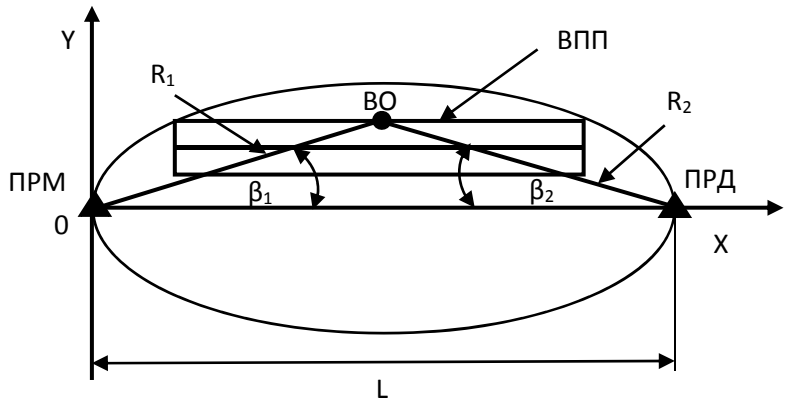


Рис. 1. Геометрия бистатической радиолокационной системы

На рисунке 2 обозначено: БОСВП – блок обработки сигналов вертикальной поляризации, БРК – блок расчета координат, БОСГП – блок обработки сигналов горизонтальной поляризации.

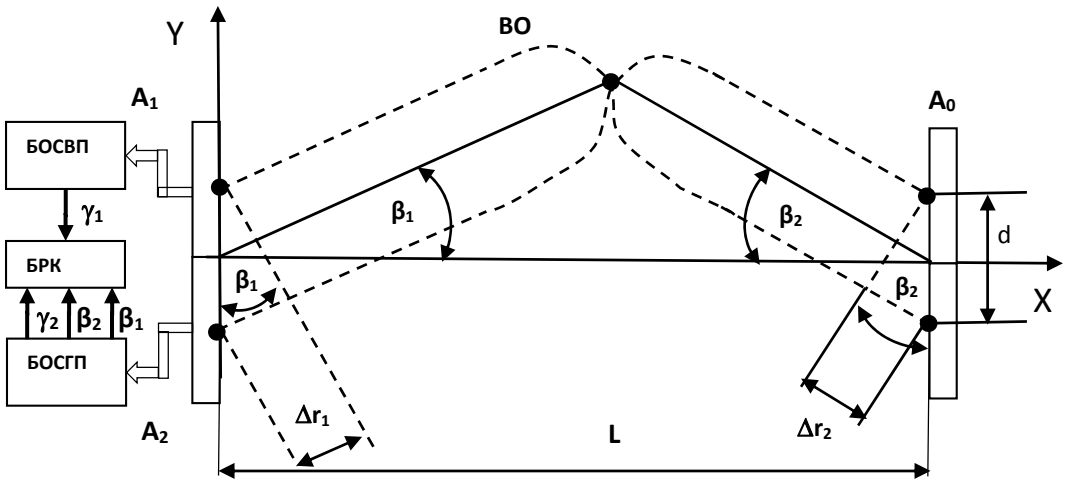


Рис. 2. Упрощенная схема бистатической радиолокационной системы

Сигнал модулированный ПСП изучается антенной A_0 и в зависимости от расположения цели сигналы, излучаемые из точек апертуры антенны

находящихся на расстоянии d будут проходить различные расстояния. Различие в проходимых радиосигналами расстояний будет приводить к дополнительным фазовым набегам $\Delta\varphi = \pi\frac{d}{\lambda}\sin(\beta_2)$ в которых и заключена информация об угле под которым облучается ВО.

В БОСВП производится обнаружение сигналов вертикальной поляризации и при формировании признака обнаружения γ_1, в БОСГП производится обнаружение сигналов горизонтальной поляризации и формируется признак обнаружения γ_2. Моменты формирования меток обнаружения формируют разность времен $\Delta t = t_1 + t_2 - t_L$, которая пропорциональна величине ΔR и вычисляется в БРК.

В БОСГП реализуется обнаружитель переотраженного ВО сигнала имеющего неизвестные значения фазовой модуляции «0 + $\varphi(\beta_2)$» и «$\pi - \varphi(\beta_2)$» и строится по схеме набора фильтров согласованных с набором точек настройки по углам зондирования перекрывающих весть сектор $\Delta\beta$ от β_{min} до β_{max} с шагом $\delta\beta$. В каждой точке угловой дискреты β_i формируется набор доплеровских фильтров, перекрывающих диапазон ожидаемых доплеровских сдвигов частот. По сути это многоканальный обнаружитель с числом фильтров K = NM, где:

$$N = \frac{\Delta\beta}{\delta\beta} = \frac{\beta_{max} - \beta_{min}}{\delta\beta},\ N = \frac{F_{R\max} - F_{R\min}}{\Delta F},$$

$F_{R\max}, F_{R\min}$ – максимальное и минимальное значение доплеровского сдвига частот; ΔF – ширина полосы пропускания фильтра.

С выхода БОСГП формируется значение оценок углов β_2 и известными методами [16] измеряются углы ε_1 и β_1, что позволяет определить местоположение ВО.

Наличие измеренного значения угла β_2 позволяет реализовать ряд методов определения координат, таких как триангуляционный и различные модификации суммарно – дальномерно – угломерного. Точность определения местоположения цели различными методами для чего используем формулу [5]:

$$\sigma = \sqrt{tr\left(B^T W^{-1} B\right)^{-1}},$$

где соответствующие матрицы имеют форму записи:

$$B = \begin{Vmatrix} \frac{\partial S_i}{\partial X} & \frac{\partial S_i}{\partial Y} & \frac{\partial S_i}{\partial H} \\ \frac{\partial S_j}{\partial X} & \frac{\partial S_j}{\partial Y} & \frac{\partial S_j}{\partial H} \\ \vdots & \vdots & \vdots \\ \frac{\partial S_k}{\partial X} & \frac{\partial S_k}{\partial Y} & \frac{\partial S_k}{\partial H} \end{Vmatrix},\ W = \begin{Vmatrix} \sigma_S^2 & 0 & 0 & 0 \\ 0 & \sigma_S^2 & 0 & 0 \\ 0 & 0 & \ddots & 0 \\ 0 & 0 & 0 & \sigma_S^2 \end{Vmatrix},$$

где: σ_S^2 – дисперсии измерения соответствующего параметра.

Значения частных производных в матрице B равны:

$$\frac{\partial\beta_1}{\partial X}=-\frac{Y}{X^2+Y^2},\ \frac{\partial\beta_1}{\partial Y}=\frac{X}{X^2+Y^2},\ \frac{\partial\beta_1}{\partial H}=0,\ \frac{\partial\beta_2}{\partial X}=\frac{Y}{(L-X)^2+Y^2},\ \frac{\partial\beta_2}{\partial Y}=\frac{L-X}{(L-X)^2+Y^2},$$

$$\frac{\partial\beta_2}{\partial H}=0,\ \frac{\partial\varepsilon_1}{\partial X}=-\frac{X(H-h_1)}{\sqrt{X^2+Y^2}\left(X^2+Y^2+(H-h_1)^2\right)},$$

$$\frac{\partial\varepsilon_1}{\partial Y}=-\frac{Y(H-h_1)}{\sqrt{X^2+Y^2}\left(X^2+Y^2+(H-h_1)^2\right)},\ \frac{\partial\varepsilon_1}{\partial H}=\frac{\sqrt{X^2+Y^2}}{X^2+Y^2+(H-h_1)^2},$$

$$\frac{\partial\varepsilon_2}{\partial X}=\frac{(L-X)(H-h_2)\left((L-X)^2+Y^2\right)}{\sqrt{\left((L-X)^2+Y^2\right)^3}\left((L-X)^2+Y^2+(H-h_2)^2\right)},$$

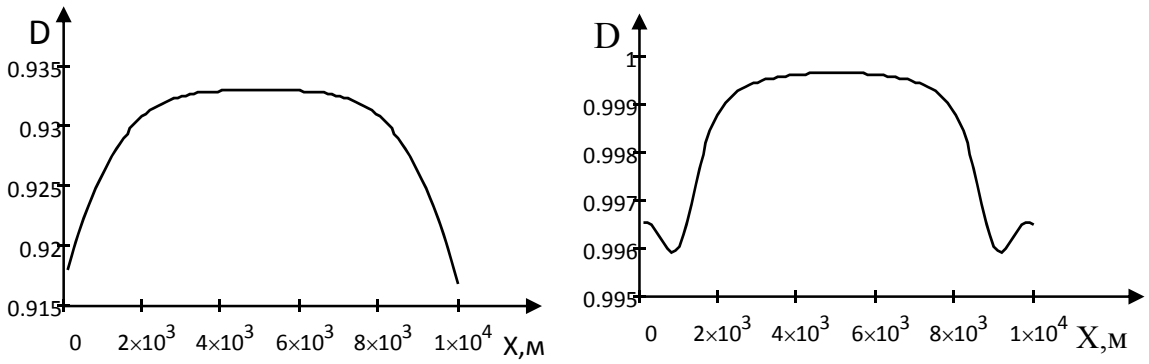
$$\frac{\partial\varepsilon_2}{\partial Y}=-\frac{Y(H-h_2)\left((L-X)^2+Y^2\right)}{\sqrt{\left((L-X)^2+Y^2\right)^3}\left((L-X)^2+Y^2+(H-h_2)^2\right)},\ \frac{\partial\varepsilon_2}{\partial H}=-\frac{\sqrt{(L-X)^2+Y^2}}{(L-X)^2+Y^2+(H-h_2)^2},$$

$$\frac{\partial\Delta R}{\partial X}=\frac{X}{\sqrt{X^2+Y^2+(H-h_1)^2}}-\frac{L-X}{\sqrt{X^2+Y^2+(H-h_2)^2}},$$

$$\frac{\partial\Delta R}{\partial Y}=\frac{Y}{\sqrt{(L-X)^2+Y^2+(H-h_2)^2}}+\frac{Y}{\sqrt{X^2+Y^2+(H-h_1)^2}},$$

$$\frac{\partial\Delta R}{\partial H}=\frac{H-h_2}{\sqrt{(L-X)^2+Y^2+(H-h_2)^2}}+\frac{H-h_1}{\sqrt{X^2+Y^2+(H-h_1)^2}}.$$

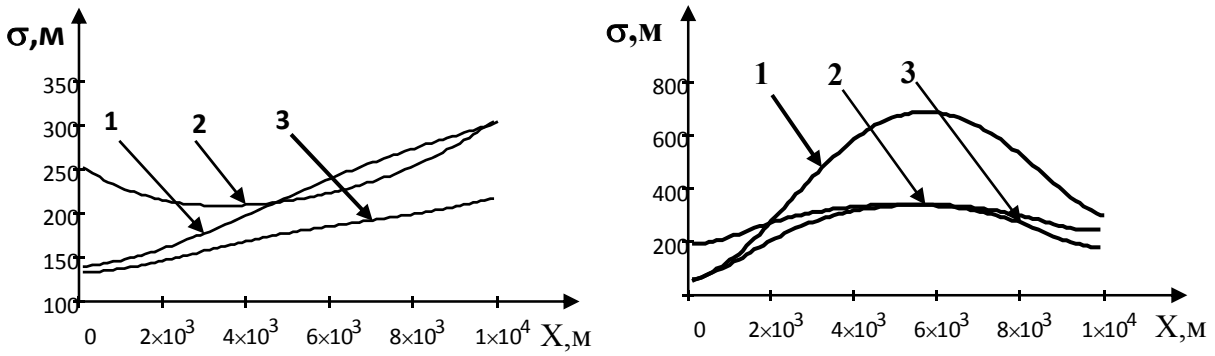
На рисунке 3 приведены вероятности обнаружения целей для случая ее движения параллельно оси X с начальными координатами а) $-Y = 5000$ м, б) $Y = 1000$ м. Высота полета ВО $H = 500$ м, значение моностатической ЭПР $\sigma = 0{,}1$ м^2, вероятность ложной тревоги на элемент разрешения $F = 10^{-6}$. Как следует из рисунка 3 при выбранном потенциале РЛС обеспечивается высокая вероятность обнаружения ВО в пределах всей зоны обзора.



а) б)

Рис. 3. Вероятности обнаружения ВО БРЛС

На рисунке 4 приведены СКО определения координат различными способами для тех же траекторий ВО, цифрами обозначено: 1 – СКО определения местоположения ВО суммарно-дальномерно-угломерным способом; 2 – СКО определения местоположения ВО триангуляционным способом; 3 – СКО определения местоположения ВО суммарно-дальномерно-угломерным способом при измерении угла облучения ВО с передающей позиции.



а) б)

Рис. 4. СКО определения местоположения для случая определения координат цели различными способами

Заключение

1. Рассмотрен способ определения местоположения ВО с использованием дополнительной информации об угле облучения с передающей позиции, обладающей выигрышем в точности от 0 до 30 % в зависимости от положения ВО в пространстве.

2. Предложенный способ измерения подразумевает применение РЛС со сложным зондирующим сигналом обладающей повышенной скрытностью и помехозащищенностью.

3. Зона контроля ВПП расположена области, где вероятность обнаружения близка к единице, а отсутствие сканирования антенны подразумевает высокий темп обновления информации.

Список используемых источников

1. Воронков Ю. С., Воронков О. Ю. Миниатюрные беспилотные летательные аппараты и особенности их создания // Современные наукоемкие технологии. 2013. № 10-1. С. 144–147.

2. Федоров И. Б., Слукин Г. П., Нефедов С. И., Скосырев В. Н., Ананенков А. Е., Нуждин В. М. Многофункциональная РЛС малой дальности для удалённой диспетчеризации региональных аэропортов // Наука и Образование. МГТУ им. Н. Э. Баумана. Электрон. журн. 2014. № 12. С. 633–644.

3. ГОСТ Р 51505-99. Система обзора летного поля и управления движением воздушных судов и транспортных средств по аэродрому. Основные параметры и технические требования. М. : Изд-во стандартов, 2000.

4. Аверьянов В. Я. Разнесенные радиолокационные станции и системы. Минск : Техника, 1978. 148 с.

5. Черняк В. С. Многопозиционная радиолокация: пер. с англ. М. : Радио и связь. 1993. 416 с.

6. Willis N. J. Bistatic Radar // Artech House, Inc. 1991.

7. Бляхман А. Б., Рунова И. А. Бистатическая эффективная площадь рассеяния и обнаружение объектов при радиолокации на просвет // Радиотехника и электроника. 2001. Т. 46. № 4. С. 424–432.

8. Бляхман А. Б., Мякиньков А. В., Рындык А. Г. Измерение координат целей в трехкоординатных бистатических радиолокационных системах с обнаружением на просвет // Радиотехника и электроника. 2006. Т. 51. № 4. С. 422–427.

9. Ковалев А. Н., Ковалев Ф. Н. Точность определения параметров траектории цели в просветной бистатической радиолокационной системе // Вестник Рязанского государственного радиотехнического университета. 2014. № 47. С. 58–62.

10. Ковалев Ф. Н. Определение координат движущихся целей по измерениям доплеровской частоты в радиолокационных системах с обнаружением «на просвет» // Радиотехника и электроника. 2007. Т. 52. № 3. С. 331–339.

11. Ковалев Ф. Н., Кондратьев В. В. Фазовая пеленгация в системах радиолокации на просвет // Доклады Академии наук. 2014. Т. 455. № 4. С. 401–403.

12. Борисов Е. Г., Анцев Г. В., Турнецкий Л. С., Машков Г. М. Пат. на полезную модель № 107370 Российская Федерация, МПК, G01S13/06. Устройство определения параметров движения цели / Е. Г. Борисов, Г. В. Анцев, Л. С. Турнецкий, Г. М. Машков; – № 2011111250/09 ; заявл. 24.03.2011 ; опубл. 10.08.2011, Бюл. № 22.

13. Борисов Е. Г., Иванов А. А., Турнецкий Л. С., Машков Г. М. Пат. на полезную модель № 109869 Российская Федерация, МПК G01S3/46. Устройство для определения параметров движения целей / Е. Г. Борисов, А. А. Иванов, Л. С. Турнецкий, Г. М. Машков; – 2011107665/07 ; заявл. 28.02.2011 ; опубл. 27.10.2011, Бюл. № 30.

14. Ширман Я. Д. Теоретические основы радиолокации. М. : Советское радио, 1970. 560 с.

УДК 621.396

ПЕРСПЕКТИВЫ ИСПОЛЬЗОВАНИЯ ЛИТИЕВЫХ АККУМУЛЯТОРОВ В СИСТЕМАХ ЭЛЕКТРОПИТАНИЯ ДЛЯ ТЕЛЕКОММУНИКАЦИЙ

П. Ю. Виноградов

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

Повышение надежности систем связи приводит к более жестким требованиям, предъявляемым к электропитанию. Решение этой задачи возможно путем применения различных источников энергии в качестве агрегатов бесперебойного и гарантированного электропитания. Расширение зоны эксплуатации телекоммуникационных

устройств в сторону Крайнего Севера приводит к необходимости применять оборудование, способное надежно работать в широком диапазоне температур. Этим условиям отвечают разрабатываемые аккумуляторные батареи на основе лития.

электропитающая установка, агрегат бесперебойного питания, литиевая аккумуляторная батарея.

Литий самый легкий щелочной металл, открытый в 1817 г. занимает третью позицию в периодической таблице Д. И. Менделеева. Месторождения лития находятся в ряде стран. В России более 50 % в Мурманской области. Первые научные попытки создать источник питания на основе лития были в начале XX века. Начиная с 1990-х годов, литиевые аккумуляторы вытесняют Ni-Cd и NiMH элементы питания в портативных инфокоммуникационных устройствах (мобильные телефоны, ноутбуки).

Преимущества Li-ионных аккумуляторных батарей (АБ) заключаются в:

– продолжительном сроке службы (до 20 лет);

– большом количестве (несколько тысяч) полных циклов заряда-разряда;

– широком диапазоне рабочих температур (от –40° до +60°);

– полной герметичности;

– самой высокой плотности энергии (до 180 Втч/кг и до 400 Втч/л, что в 5 раз выше чем свинцово-кислотных и в два раза выше чем у NiMH);

– способности работать при повышенном атмосферном давлении, влажности, воздействии магнитных полей, при любом пространственном положении;

– высоком значении зарядного тока (в 5–10 раз выше, чем свинцово-кислотных), и, следовательно, малом времени заряда.

До недавнего времени основным недостатком литиевых элементов питания была их потенциальная пожароопасность, что существенно снижало область применения.

Сейчас, благодаря развитию технологии производства аккумуляторов, вопрос пажаробезопасности можно считать решенным [1]. Основные технологические решения следующие:

– создание аккумулятора без применения чистого Li, но с использованием его ионов;

– применение в качестве активного материала положительного электрода оксиды кобальта;

– построение отрицательного электрода из углеродных материалов;

– использования встроенных электронных ключей, позволяющих отключать АБ при полном разряде и полном заряде;

– снабжение аккумуляторов клапанами для выпуска газов при повышенном давлении, что предотвращает разрыв.

В конструкциях Li-ионных аккумуляторов предусмотрены система контроля, управления и защиты от перегрева, перезаряда, короткого замыкания.

Перечисленные преимущества привели к широкому развитию производства литиевых аккумуляторов. Несколько лет назад выпускались аккумуляторы для переносных устройств емкостью единицы ампер-часов. Сейчас практически нет ограничения по емкости. Li-ионные аккумуляторы следует считать наиболее перспективными для широкого круга потребителей таких как атомная энергетика, автомобильный и железнодорожный транспорт, промышленность и др. Основным двигателем развития таких АБ является производство гибридных и электрических автомобилей.

Сегодня в мире работает более 40 крупных производителей Li-ионных аккумуляторов. Это быстро растущий и многообещающий сегмент рынка. На последней международной выставке источников тока в Китае более 70 % экспонатов были связаны именно с литием.

Рассмотрим возможность применения Li-ионных аккумуляторов в телекоммуникациях. Последние 70 лет в подавляющем числе электропитающих установок (ЭПУ) в связи в качестве агрегата бесперебойного питания применяется свинцово-кислотная АБ.

Начиная с 1994, европейские и международные стандарты и рекомендации, касающиеся электропитания телекоммуникационных устройств, прописаны под разрядно-зарядные характеристики свинцово-кислотного аккумулятора, включенного между выходом ЭПУ и питаемым оборудование. Напряжение питания постоянным током лежит в пределах от 40,5 В до 57 В. Это позволяет обеспечивать максимальную надежность, т. к. не требует регулировок, подключения дополнительных элементов аккумулятора по мере его разряда. АБ напрямую подключена к питаемому оборудованию без дополнительных коммутаций, обеспечивая энергией это оборудование при любых аварийных ситуациях, возникших в ЭПУ до батареи. Условное напряжение данного стандарта – 48 В, что соответствует последовательно включенным 24 двухволтовым элементам батареи.

Щелочные аккумуляторы требуют значительного более широкого диапазона напряжений от минимального при разряде до максимального при заряде. Поэтому они не используются в составе ЭПУ.

Единственным аккумулятором, подходящим по стандарт 48 В, является Li-ионный. У него среднее напряжение – 3,6 В, минимальное при разряде – 3,2 В, максимальное при заряде – 4,2 В. Таким образом при 13 последовательно включенных в батарею элементах напряжение ЭПУ укладывается в требования стандарта.

На сегодня стоимость литиевых АБ выше, чем традиционных свинцово-кислотных, но она заметно падает с развитием производства.

Главным препятствием на пути использования Li-ионных аккумуляторов АБ в составе ЭТУ телекоммуникационного оборудования является

невозможность их использование в режиме постоянного подключения (буферный режим) между ЭПУ и питаемым оборудованием из-за возможного перезаряда и как следствие пожарно-взрывоопасности. Встроенная электроника современных литиевых батарей отключит аккумулятор при полном заряде, предотвращая опасность пожара. Но это противоречит всей идеологии построения ЭПУ последних 20 лет – высокая надежность путем минимума коммутаций.

Разработчики Li-ионных аккумуляторов уверяют в очень высокой надежности встроенных электронных силовых ключей. Опыта эксплуатации мало. В нашей стране единицы объектов связи, которые используют Li-ионные аккумуляторы в течение нескольких лет. Нареканий пока нет. Возможно за ними будущее. Время покажет.

Список используемых источников

1. Варнавский С. А., Мельников В. А., Якушкин В. А. Применение литий-ионных аккумуляторов Saft в гибридных системах электропитания // Состояние и перспективы развития энергетики связи: материалы XVI всерос. науч. конф., Санкт-Петербург, 6–8 июня 2015 г. СПб.: СПбГУТ, 2015. С. 68–70.

УДК 654.165

ПРИМЕНЕНИЕ ПЕРСПЕКТИВНЫХ МЕТОДОВ МОДУЛЯЦИИ В СОВРЕМЕННЫХ СИСТЕМАХ МОБИЛЬНОЙ СВЯЗИ

Р. В. Глазков

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

Развитие мультимедийных технологий, внедрение новых услуг и повышение объемов, передаваемых данных, требует повышения эффективности работы существующих перспективных сетей мобильной связи. На данный момент появление новых стандартов (семейство 5G) и постоянное совершенствование технологий беспроводной передачи привело к экспоненциальному росту частотных и программно-аппаратных ресурсов, необходимых для обслуживания абонентов. Однако данные ресурсы ограничены, а их использование требует значительного финансирования.

В связи с этим, крайне актуальной задачей является оптимизация работы систем мобильной связи пятого поколения на физическом уровне. Исследования, направленные на внедрение новых перспективных методов модуляции, позволят изменить характеристики передаваемых радиосигналов, и обеспечить значительную экономию сетевых ресурсов. Это, в свою очередь, сможет повысить эффективность работы сети в целом. В данной работе приведен анализ возможности применения в сетях 5G таких методов модуляции как FBMC, а также других технологий, в которых используется цифровой метод модуляции N-OFDM.

модуляция, частотное мультиплексирование, N-OFDM, FBMC, UFMC, 5G.

Основными задачами в сетях 5G на физическом уровне являются: повышение спектральной эффективности, достигнутой в сетях четвертого поколения, расширение частотного диапазона сетей 4G, повышение помехоустойчивости и электромагнитной совместимости, обеспечение взаимодействия между абонентскими устройствами напрямую (M2M), повышение эффективности утилизации радиочастотного спектра [1]. Данные требования продиктованы экспоненциальным ростом абонентской нагрузки на сети [2], наличию проблем в используемых сетях мобильной связи [3], а также специфичностью некоторых технологий [4].

Актуальной на данный момент является технология мультиплексирования с ортогональным частотным разделением каналов (OFDM). Основными достоинствами OFDM являются: эффективность использования спектра, помехоустойчивость и относительная простота реализации. Недостатками являются: наличие высокого уровня внеполосного излучения, подверженность доплеровскому сдвигу и циклический префикс[5].

Особенностью OFDM является ортогональное разнесение поднесущих частот таким образом, чтобы сигнальные отклики в приемнике приходились на максимумы амплитудно-частотных характеристик (АЧХ), синтезированных в результате быстрого преобразования Фурье (БПФ) частотных фильтров (рис. 1) [5].

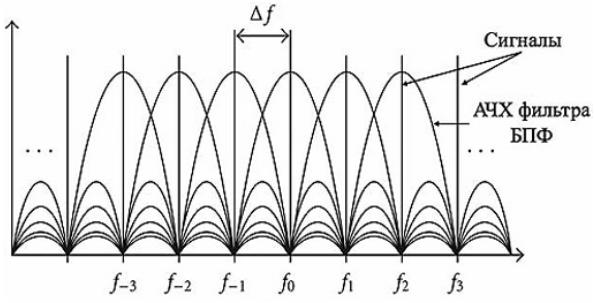


Рис. 1. OFDM-пакет

Условие ортогональности поднесущих частот обуславливает равенство нулю коэффициента корреляции сигналов двух соседних поднесущих (1).

$$\rho = \frac{1}{T}\int_0^T e^{j2\pi f_1 t} e^{j2\pi f_2 t} dt, \quad (1)$$

где T – длительность сигнальной выборки, над которой выполняется операция БПФ (символьный интервал), f_1, f_2– две соседние поднесущие частоты, t – время, e, π – математические постоянные.

Для повышения спектральной эффективности OFDM была предложена схема модуляции Fast OFDM, в которой частотный интервал между поднесущими уменьшен в два раза (2), (3).

$$\Delta f_{OFDM} = \frac{1}{T}, \quad (2)$$

$$\Delta f_{Fast\ OFDM} = \frac{1}{2T}, \quad (3)$$

где Δf – частотный интервал между соседними поднесущими, T – длительность сигнальной выборки.

Данная схема модуляции позволила повысить спектральную эффективность сигнала вдвое и при этом снизить уровень внеполосных излучений (рис. 2). Однако проблема данного метода модуляции состоит в том, что реализовать демодуляторы для декодирования сигнала Fast OFDM возможно только при использовании амплитудной и ФМ-2 (фазовая модуляция) модуляции поднесущих [5].

Альтернативой является метод произвольной расстановки поднесущих относительно АЧХ частотных фильтров, который получил название мультиплексирования с неортогональным частотным разделением (N-OFDM) [5]. Демодуляция сигнала N-OFDM производится с помощью ортогонализирования, при этом самыми распространенными являются методы Лёвдина и Грамма-Шмидта (4).

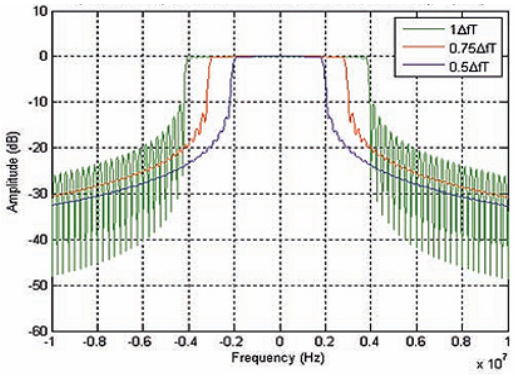


Рис. 2. Сопоставление ширины полосы частот сигналов *OFDM* ($\Delta f_x T = 1$) и Fast-OFDM ($\Delta f_x T = 0{,}5$) для пакета из 32 поднесущих

$$\begin{cases} U_1 = \sum_{m=1}^{2} \dot{a}_m \times f_1(w_m), \\ U_2 = \sum_{m=1}^{2} \dot{a}_m \times f_2(w_m), \end{cases} \quad f_1(w_m) = \frac{\sin S \times \left[n \times \frac{\pi}{S} - w_m\right]}{S \times sin\left[n \times \frac{\pi}{S} - w_m\right]}, \quad (4)$$

где $f_1(w_m)$ – значение нормированной АЧХ n-го БПФ-фильтра на частоте m-й поднесущей w_m, S – размерность (количество точек) операции БПФ, $\dot{a}_m$ – комплексная амплитуда m-й поднесущей, U_r – выходное напряжение r-го частотного фильтра.

Одним из вариантов N-OFDM является метод универсального фильтруемого многочастотного сигнала (UFMC) [6], который заключается в особом способе фильтрации многочастотной выборки (5).

$$\underset{[(N+L-1)\times 1]}{\boldsymbol{X}_k} = \sum_{i=1}^{B} \underset{[(N+L-1)\times N]}{\boldsymbol{F}_{ik}} \underset{[N\times n_i]}{\boldsymbol{V}_{ik}} \underset{[n_i\times 1]}{\boldsymbol{S}_{ik}}, \quad (5)$$

где X_k – суммарный сигнал *UFMC*, k – номер абонента, L – длина фильтра, N – размерность *БПФ*, B – число поднесущих. N_i – промодулированные КАМ сигналы, трансформированные в матрицу V_i. F_i – матрица импульсных характеристик частотных фильтров.

На рисунке 3 представлен график сравнения помехоустойчивости сигнала UFMC и OFDM.

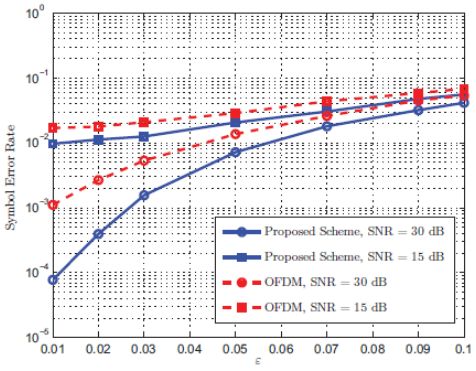


Рис. 3. Помехоустойчивость UFMC и OFDM

Другим перспективным методом модуляции с неоргональным частотным разделением является метод частотного мультиплексирования с множеством несущих, использующий банк (гребенку) частотных фильтров (FBMC) [7]. Данный метод отличается фильтрацией с высокой степенью избирательности по всему банку фильтров БПФ, это позволяет снизить внеполосное излучение, повысить спектральную эффективность, а также обеспечить одновременное сосуществование в одном частотном диапазоне широкополосных и узкополосных сигналов, что важно для обеспечения связи в сетях пятого поколения (такой как M2M).

На рисунке 4 представлен график сравнения уровня внеполосного излучения OFDM и FBMC, смоделированных в среде MATLAB.

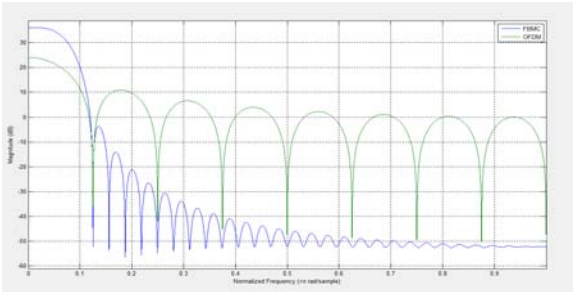


Рис. 4. Результат моделирования OFDM и FBMC сигналов в MATLAB

На основе полученных данных можно сделать вывод, что новые перспективные методы модуляции позволяют повысить спектральную эффективность и помехоустойчивость существующих сетей связи, а также улуч-

шить возможности сосуществования широкополосных и узкополосных систем передачи данных. Сравнение перспективных методов модуляции по результатам проведенного анализа приведено в таблице.

В статье исследованы цифровые методы модуляции, в которых используется мультиплексирование с ортогональным и неортогональным частотным разделением. По результатам работы можно сделать вывод, что проанализированные методы являются перспективными и требуются их всестороннего сравнение для выявления наиболее подходящих сценариев применения каждой из технологий. Более глубокое изучение технологий неортогонального мультиплексирования в дальнейшем будет проведен посредством оборудования программно-конфигурируемого радио и по методикам, представленным в работах [8, 9, 10].

ТАБЛИЦА. Сравнение перспективных методов модуляции и их возможность применения в сетях пятого поколения

Вид модуляции	Достоинства	Недостатки	Возможность применения в 5G
Fast-OFDM	Спектральная эффективность	Только AM и ФМ-2	Маловероятна
Семейство N-OFDM	Спектральная эффективность, помехоустойчивость	Сложнее, чем OFDM	Есть
UFMC	Спектральная эффективность, помехоустойчивость, внеполосное излучение	Сложность построения передатчиков	Есть
FBMC	Спектральная эффективность, внеполосное излучение	Сложность реализации	Есть

Список используемых источников

1. Jaakko Vihriälä, Natalia Ermolova, Eeva Lähetkangas, Olav Tirkkonen, Kari Pajukoski. On the Waveforms for 5G Mobile Broadband Communications [Электронный ресурс]. URL: https://www.metis2020.com/wp-content/uploads/publications/IEEE_VTC_Spring_2015_Vihri%C3%A4l%C3%A4_etal_On-the-Waveforms-for-5G.pdf (дата обращения 12.01.2016).

2. Cisco Visual Networking Index: Global Mobile Data Traffic Forecast Update, 2015 – 2020 [Электронный ресурс] // Whitepaper – 03.02.2016. URL: http://www.cisco.com/c/en/us/solutions/collateral/service-provider/visual-networking-index-vni/mobile-white-paper-c11-520862.pdf (дата обращения 12.01.2016).

3. Глазков Р. В. Анализ существующих методов обнаружения «спящих» сот в сетях LTE // Актуальные проблемы инфотелекоммуникаций в науке и образовании. III Международная научно-техническая и научно-методическая конференция: сб. научных статей. СПб. : СПбГУТ, 2014. – С. 72–77.

4. Гельгор А. Л., Павленко И. И., Горлов А. И., Фокин Г. А., Попов Е. А., Лаврухин В. А., Сиверс М. А. Первичная синхронизация с базовыми станциями LTE // Электромагнитные волны и электронные системы. 2014. № 7. С. 54–62.

5. Слюсар В. И. Неортогональное частотное мультиплексирование (N-OFDM) сигналов. Часть 1 // Технологии и средства связи. 2013. № 5 (98). С. 61–65.

6. Vida Vakilian, Thorsten Wild, Frank Schaich, Stephan ten Brink, Jean-Francois Frigon. Universal-Filtered Multi-Carrier Technique for Wireless Systems Beyond LTE // IEEE Globecom Workshop, Atlanta, USA, Feb. 9, 2013.

7. Malte Schellmann, Zhao Zhao. FBMC-based air interface for 5G Mobile: Challenges and proposed solutions // 9th International Conference on Cognitive Radio Oriented Wireless Networks, Оулу, Finland, June 2–4, 2014.

8. Волгушев Д. Б., Киреев А. В., Фокин Г. А. Модельно-ориентированный синтез систем радиосвязи на основе программно-конфигурируемого радио // Актуальные проблемы инфотелекоммуникаций в науке и образовании. IV Международная научно-техническая и научно-методическая конференция: сб. научных статей в 2 т. СПб. : СПбГУТ, 2015. Т. 1. С. 50–53.

9. Фокин Г. А., Буланов Д. В., Волгушев Д. Б. Модельно-ориентированное проектирование систем радиосвязи на основе ПКР // Вестник связи. 2015. № 6. С. 26–30.

10. Фокин Г. А., Лаврухин В. А., Волгушев Д. А., Киреев А. В. Модельно-ориентированное проектирование на основе SDR // Системы управления и информационные технологии. 2015. № 2. С 94–99.

Статья представлена научным руководителем, кандидатом технических наук, профессором О. В. Воробьевым.

УДК 621.397.13

ПАРАМЕТРЫ ОЦЕНКИ КАЧЕСТВА ИЗОБРАЖЕНИЙ ВЫСОКОЙ ЧЕТКОСТИ И ОБЪЕМНЫХ ИЗОБРАЖЕНИЙ ДОПОЛНЕННОЙ И ВИРТУАЛЬНОЙ РЕАЛЬНОСТИ

А. А. Гоголь, Е. И. Туманова

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

Рассматриваются основные параметры оценки качества изображений виртуальной и дополненной реальности. Проведен анализ влияния на реалистичность восприятия виртуального трехмерного пространства таких параметров как: глубина изображения, разрешающая способность, частота обновления кадров форматов 4K, 8K и объемных изображений.

оценка качества, изображение высокой четкости, объемное изображение, дополненная и виртуальная реальность.

В связи с развитием сетевых технологий в последние годы доступ к сети Интернет и соответствующим услугам стал общедоступным. Это в свою очередь повлияло на рост интереса к виртуальной реальности и новым возможностям применения данной технологии. Все чаще виртуальную реальность используют в образовательной сфере, науке и бизнесе. В связи с этим возникает вопрос о качестве предоставляемой технологии.

Как следует из названия виртуальная реальность (*virtual reality* – VR) – это имитация трёхмерного мира, созданная с использованием специальных технических средств, субъектом которого является человек [1]. Другим видом применения виртуальных технологий является дополненная реальность (*augmented reality* – AR). Она позволяет в режиме реального времени совмещать существующее физическое изображение цифровыми данными. Примером дополненной реальности может служить выводимые на экран монитора схемы размера поля при телевизионной трансляции спортивного матча.

Для погружения в мир виртуальной реальности используются соответствующие устройства: стереоскопические очки, шлемы, аппаратные средства, сферы виртуальной реальности.

Качество воспринимаемого изображения, а также реалистичность восприятия виртуального трехмерного пространства зависят от следующих факторов: глубина сцены, сложность графики окружающей среды, реалистичность моделирования взаимодействия пользователя с трехмерной средой, звуковое сопровождение и т. д.

В виртуальной реальности происходит имитация трехмерной среды через наблюдение воспроизводимого видео изображения. От того насколько качественно данное изображение будет зависеть эффект погружения в виртуальную среду. Под качеством изображения в данном случае понимается реалистичность и глубина воспроизводимой среды с наиболее высоким ощущением реализма.

Признаки восприятия глубины человеком делятся на два основных типа: физиологические и психологические [2]. Физиологические признаки, в свою очередь, делятся на монокулярные (аккомодация, параллакс движения) и бинокулярные признаки (вергенция, диспарантность). Психологические признаки восприятия глубины основаны на полученном в течение жизни опыте наблюдения окружающего мира: тени и блики, относительный размер, градиент текстуры, линейная перспектива и т. д.

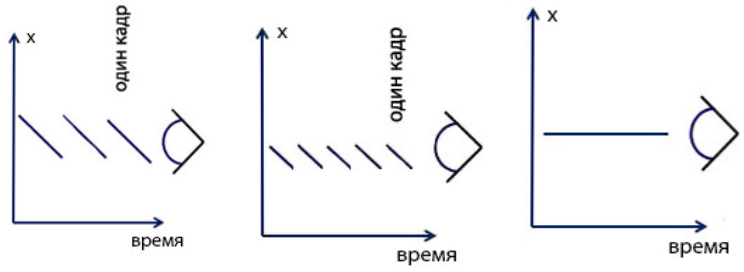
Следующим параметром, влияющим на различие в восприятии между реальной и виртуальной средой является поле зрения.

Поле зрения человека в горизонтальной плоскости (рис. 1), в отличие от вертикальной, где оно постоянно и равно 135°, может принимать различные значения. При восприятии окружающего мира одним глазом поле зрения человека в горизонтальной плоскости равно 160°, а при бинокулярном обзоре – 200°. Из этого можно следует, что

Рис. 1. Поле зрения человека

даже существующие виртуальные шлемы со 180° обзора не смогут обеспечить полное совпадение с реальным миром. При использовании виртуального шлема возникает визуальный феномен, который имеет название туннельное зрение [3]. Оно характерно ограничением поля зрения, в том числе периферийного зрения. Периферийное зрение передает в мозг информацию о скорости движения и расстоянии до объектов, в то время как центральное зрение даёт лишь приблизительную оценку скорости движущегося объекта на основе изменения размера или угла параллакса между глазами. По этой причине разработчики виртуальных сред стараются расположить основные объекты сцены в центре, удаляя дополнительную информацию, которая будет попадать на периферийное зрение.

Еще одним параметров влияющим на качество воспроизводимого изображения является количество воспринимаемой информации. Добиться его увеличения можно двумя способами: увеличением разрешающей способности воспроизводимого изображения или увеличением частоты обновления кадров (рис. 2).



а) б) в)

Рис. 2. Упрощенная иллюстрация наблюдения глазом изображений на мониторе при: а) 60 Гц, б) 120 Гц; в) в реальной жизни

При воспроизведении изображений в последних форматах Ultra HD 4K (3840 × 2160, 16:9) и 8K UHD (7 680 × 4 320, 16:9) [4] зритель будет воспринимать плоские изображения высокой четкости, как объемные. Данное явление хорошо известно в фотографии. Однако для этого необходимо, чтобы исходный контент и все звенья системы передачи и воспроизведения поддерживали соответствующие технические параметры.

Частота обновления кадров зависит от различных параметров: тип дисплея, скорость движения и характеристики глаз, содержание сцены, световая подсветка экрана, заполнения пикселя и т. д. [5]. На сегодняшний день основные производители телевизоров и компьютерных дисплеев заявляют частоту обновления кадров от 1000 до 3500 Гц. На практике оказывается, что данные цифры не являются физическим значением частоты обновления кадров, а представляют собой имитацию воспроизведения и ощущений

у зрителя наблюдения изображения с данным значением частоты обновления.

Развитие технологий виртуальной и дополненной реальности привело к распространению их применения в таких сферах как: здравоохранение, образование, военная промышленность и т. д. Наибольшую эффективность данные технологии будут представлять при высоком качестве воспроизводимой виртуальной среды. Обеспечить высокое качество изображений и необходимую глубину сцены способны современные форматы 4K и 8K, а также многоракурсное или объемное видео.

Список используемых источников

1. Красильников Н. Н. Цифровая обработка 2D- и 3D-изображений: учеб. пособие. СПб. : БХВ-Петербург, 2011. 608 с. ISBN 978-5-9775-0700-4.

2. Bernard Mendiburu. 3D Movie Making Stereoscopic Digital Cinema from Script to Screen. Oxford, UK, Elsevier Inc., 2009. pp. 13–24.

3. Alan B. Craig, William R. Sherman, Jeffrey D. Will. Developing Virtual Reality Applications: Foundations of Effective Design. Oxford, UK, Elsevier Inc., 2009. p. 284.

4. Кривошеев М. И. О стратегии развития ТВ вещания в России после 2015 г. // Труды НИИР. 2014. № 3. 50 с.

5. Гоголь А. А., Туманова Е. И. Анализ влияния частоты кадров современных телевизоров на качество воспроизводимого изображения в видеоинформационных системах // Вопросы радиоэлектроники. Серия техника телевидения. 2015. Вып. 1. С. 3–9.

УДК 621.396.67

МЕТОДЫ ПРОЕКТИРОВАНИЯ ПОЛОСКОВЫХ СТРУКТУР С ПОЛЮСАМИ ЗАТУХАНИЯ НА КОНЕЧНЫХ ЧАСТОТАХ

Н. О. Дёшина, А. Р. Кубалова, Т. А. Рыжикова

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

Рассмотрены основные типы структур с полюсами затухания. Приведены: полосковой структуры с инвертирующими отрезками линий и параллельными шлейфами; полосковой структуры, состоящей из параллельного соединения двух решёток, связанных многопроводных линий одинаковой длины; полосковой структуры, состоящей из параллельного соединения двух короткозамкнутых решеток, связанных многопроводных линий; полосковой структуры, состоящей из параллельного соединения двух разомкнутых решеток связанных линий; полосковой структуры на полусосредаточенных элементах.

полосковая структура, многопроводная линия, короткозамкнутые решётки, полусосредаточенные элементы, инвертирующие отрезки, параллельные решётки, полюса затухания, разомкнутые решетки.

Основные типы структур с полюсами затухания

Оптимизация параметров узлов СВЧ модулей на основе применения перспективных типов полосковых линий тесно связана с проектированием пассивных частотно-селективных цепей, имеющих нули передачи на конечных частотах. Такие цепи по сравнению с обычными полиномиальными цепями имеют ряд существенных преимуществ, связанных с тем, что крутизна АЧХ в них определяется не только числом элементов, но и положением полюсов затухания. В результате этого свойства фильтрующие, корректирующие и согласующие цепи становятся более компактными и имеют характеристики ближе к оптимальным. Улучшение практически по всем параметрам особенно заметно для цепей с узкой переходной областью. Так для фильтров с ненагруженной добротностью резонаторов порядка 2000 с высокой крутизной АЧХ в полосе расфильтрации полосковые структуры с нулями передачи на конечных частотах имеют почти на 40 % выше уровень затухания в полосе эффективного задерживания.

Полосковые структуры с нулями передачи на произвольных частотах в основном реализуются на СПЛ. Это объясняется тем, что для получения удовлетворительного совпадения теоретических и экспериментальных характеристик требуется точная реализация нулей (полюсов) цепи. А это приводит к тому, что влияние любых неоднородностей в рассматриваемых структурах сказываются более резко, чем в полиномиальных. При реализации на СПЛ в настоящее время существуют отработанные методики учета почти всех неоднородностей, что нельзя сказать о структурах на НПЛ. Это объясняется более сложными физическими процессами в этих линиях и более сложными математическими методами. Поэтому можно утверждать, что удовлетворительные результаты при реализации рассматриваемых структур на НПЛ получаются лишь для цепей с небольшим числом резонаторов.

Полосковые структуры с нулями передачи на конечных частотах можно разбить на пять основных типов:

– структуры с инвертирующими отрезками линий и с параллельными или последовательными шлейфами (рис. 1*а*);

– структуры, состоящие из параллельно соединенных двух решеток, связанных многопроводных линий одинаковой длины (рис. 1*б*);

– структуры, состоящие из параллельно соединенных двух короткозамкнутых решеток, связанных многопроводных линий (рис. 1*в*);

– структуры, состоящие из параллельно соединенных двух разомкнутых решеток, связанных многопроводных линий (рис. 1*г*);

– структуры на полусосредоточенных элементах (рис. 1*д*).

Все эти полосковые структуры реализуются на НПЛ, имеют свои достоинства и недостатки, и поэтому оптимальный выбор цепи представляет собой, как правило, сложную и творческую задачу.

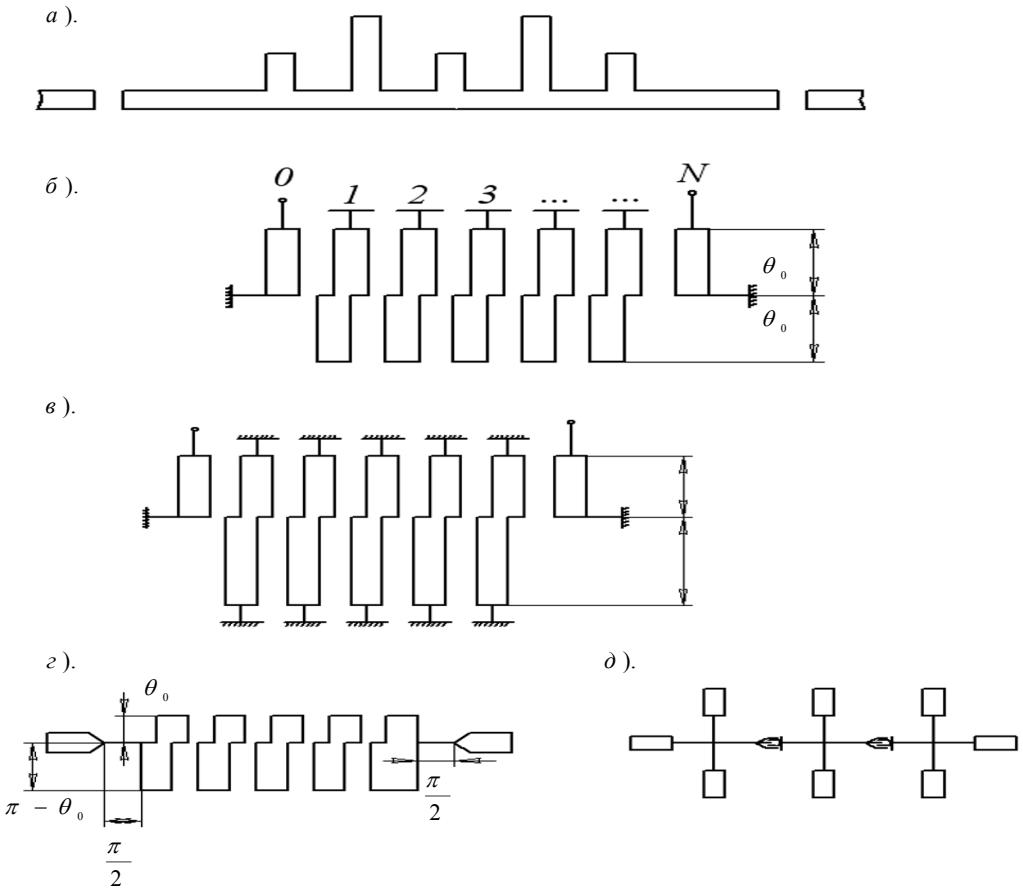
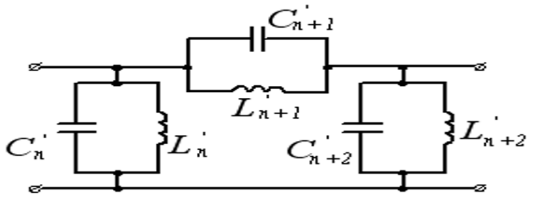


Рис. 1. Основные типы фильтрующих полосковых структур с полюсами затухания на конечных частотах

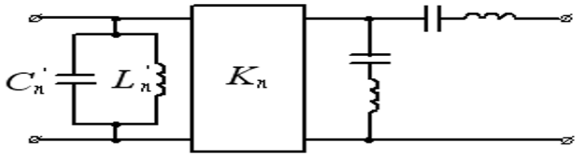
Шлейфные структуры используются при реализации простых прототипов с небольшим числом резонаторов, так как они содержат отрезки линий длиною кратных $\lambda/4$, а поэтому характеризуются большой площадью. Несомненным достоинством таких структур является отсутствие (при желании) заземленных резонаторов и достаточная точность воспроизведений теоретических характеристик. Последнее объясняется тем, что частоты полюсов АЧХ определяются только длиною шлейфов.

Известны многие разновидности этих структур [1, 2, 3]. Почти все они используются для реализации достаточно узкополосных характеристик – (2–10) %, так как в них вводятся идеальные инверторы, которые в реальных структурах заменяются четвертьволновыми отрезками линий (рис. 2).

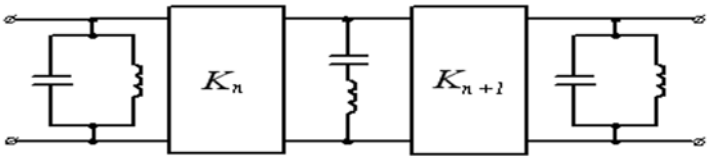
Как правило, затруднение при проектировании шлейфных структур вызывает реализация входного и выходного контуров. Из нескольких приближенных способов решения этой задачи следует выделить реализацию, предложенную в [2]. Суть ее заключается в ведении дополнительных инверторов, реализуемых зазорами в НПЛ.



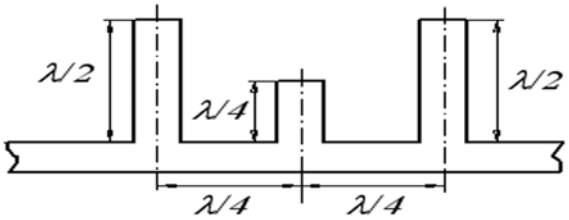
а).



б).



в).



г).

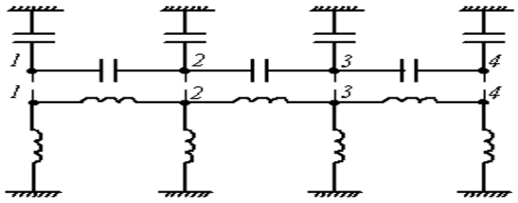
Рис. 2. Переход от прототипа к полосковой структуре со шлейфами

Шлейфные структуры имеют первую паразитную полосу пропускания на частоте $3\omega_0$, где ω_0 – центральная частота основной ПЭП. Однако при незначительной расстройке могут появиться узкие паразитные полосы пропускания вблизи частоты $2\omega_0$. Методика расчета рассматриваемой структуры приведена в [2].

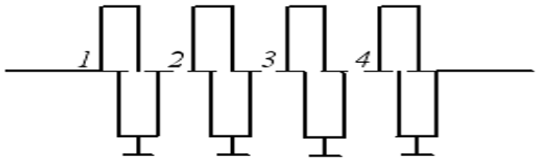
Одной из самых компактных структур с нулями передачи на конечных частотах является структура на связанных многопроводных линиях (рис. 1*б*).

Известно, что решетка связанных резонаторов реализует полиномиальные характеристики (гребенчатые и встречно-стрежневые цепи). Для получения нулей передачи было предложено параллельное соединение двух решеток [4]. На рис. 3*а* показан прототип, в котором резонансные контуры разделены так, что получилось две лестничные цепи из элементов L и элементов C. Они имеют общие узлы 1 – 4. Известно, что индуктивная лестничная цепь реализуется решеткой закороченных отрезков связанных ли-

ний, а емкостная – решеткой разомкнутых линий. Если теперь эти две решетки соединить параллельно в узлах 1 – 4, то получится структура, показанная на рис. 3*б*.



а).



б).

Рис. 3. Реализация прототипа с полюсами затухания параллельным соединением двух решеток, связанных многопроводных лини

Эта структура имеет реализуемые геометрические размеры только при высоких нагрузках. Поэтому в закороченной решетке добавляются трансформирующие входные линии.

Приведенная структура используется для реализации характеристик ППФ с полосой пропускания выше 5 %. Для более узких полос начинают резко связываться сосредоточенные емкости разомкнутых концов линий решетки, коррекция которых, как правило, удовлетворительных результатов не дает.

При проектировании структуры, показанной на рис. 3*б*, возможно проведение линейного преобразования матриц нормированных статических емкостей решеток, которое позволяется в достаточно широких пределах изменить геометрию связанных линий.

Недостатком этой структуры при реализации на НПЛ является наличие заземленных линий, что усложняет технологию изготовления. Методика расчета рассматриваемой структуры приведена в [3].

Второй структурой на связанных линиях с полюсами затухания на конечных частотах является структура без разомкнутых резонаторов (рис. 1*в*). Она позволяет достаточно удовлетворительно реализовать узкополосные характеристики – (1–5) %. Выше 8 % характеристика затухания становится резко несимметричной относительно центральной частоты. При этом происходит значительное уменьшение крутизны в нижней переходной области.

Рассматриваемая структура по сравнению с предыдущей имеет большие габариты, дополнительно заземленные резонаторы, но она позволяет реализовать более узкие полосы пропускания. Как и в первом случае, здесь

возможно варьировать геометрией связанных линий путем линейного преобразования емкостных матриц решеток. Методика расчета этой структуры приведена в [4].

Третья структура на связанных многопроводных линиях (рис. 1*г*) выгодно отличается от предыдущих отсутствием заземленных резонаторов, что во многих практических случаях является решающим фактором. Несмотря на то, что в структуре имеются разомкнутые резонаторы и при узких полосах пропускания должны сказываться сосредоточенные емкости, этого не наблюдается, как, например, в цепи на рис. 1*б*. Дело в том, что сосредоточенные емкости одновременно влияют на обе решетки, тем самым в значительной степени компенсируя друг друга. Эксперимент показывает, что рассматриваемая структура может использоваться, примерно, начиная с полос пропускания 2 %. Верхний предел, как и в структуре, рис. 1*в*, зависит от узкополосного приближения и приблизительно равен (8–10) %.

В рассматриваемой структуре узкие паразитные полосы появляются обычно несколько выше $2\omega_0$, однако их положение определяется трудно учитываемыми неоднородностями. Как и предыдущие структуры на связанных линиях, здесь возможно линейным преобразованием емкостных матриц варьировать геометрическими размерами резонаторов. Методика расчета этой структуры приведена в [5].

Реализация малогабаритных частотно-селективных цепей на печати в метровом диапазоне волн вызывает серьезные затруднения, так как сосредоточенные элементы уже не применимы из-за низкой добротности, а обычные структуры из отрезков линий имеют совершенно неприемлемые геометрические размеры даже на подложках с высоким ε. Именно поэтому были разработаны фильтрующие полосковые структуры, состоящие из отрезкой линий с длиною много меньше $\lambda/4$. Обычно эти цепи называют «цепями на полусосредоточенных элементах». Такие структуры достаточно компактны, практически не имеют ограничений на полосу пропускания реализуемой характеристики и могут быть без заземленных элементов (рис. 1*д*).

Серьезные затруднения при проектировании таких структур возникают из-за крайне малых значений реализуемых индуктивностей (десятки наногенри), которые определяются технологическими возможностями изготовления высокоомных линий. В последние годы в таких цепях стали применять индуктивности в виде спирали полосковой линии, которая реализует индуктивности порядка сотни наногенри [6].

Второе ограничение возникает при реализации последовательной емкости. Зазор в полосковой линии на печати имеет ничтожную емкость, и поэтому, как правило, приходится использовать гребенчатые зазоры, которыми можно реализовать емкости в пределах до 10 пФ [7].

В рассматриваемой структуре существует несколько способов коррекции паразитных параметров. Один из них рассмотрен в [3].

Методика расчета структур на полусосредоточенных элементах с нулями передачи на конечных частотах рассмотрена в книге Л. И. Чикунова «Эллиптический фильтр без заземленных резонаторов» 1980 г. выпуска.

Список используемых источников

1. Справочник по элементам полосковой техники / Под ред. А. Л. Фельдштейна. М. : Связь, 1979. 336 с.

2. Rubinstein J. Narrow-Band with Elliptic Function Filters // IEEE Trans. MTT-17, 1969, № 12.

3. Маттей Д. Л., Янг Л., Джонс Е. М. Т., Фильтры СВЧ согласующие цепи и цепи связи. Т. I. М. : Связь, 1971. 495 с.

4. Rodes J. D. The stepped digital elliptic filter // IEEE Trans. MTT-17, 1969, № 4.

5. Rodes J. D. The half-wave stepped digital elliptic filter // IEEE Trans. MTT-17, 1969, № 4.

6. Sobol H. Application of integrated circuit technology to microwave frequencies // Proc. IEEE, 1971, № 8.

7. Binotto L. Piacentin G. F. Analysis of interdigitated thin-film capasitors // Yhin solid Films, 1972, № 12.

УДК 621.396.67

ПРОЕКТИРОВАНИЕ АНТЕНН И СВЧ СТРУКТУР С ПОМОЩЬЮ ПРОГРАММЫ HFSS

Н. О. Дёшина, А. Р. Кубалова, Т. А. Рыжикова

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

Программа HFSS предназначена для проектирования трехмерных СВЧ устройств и использует несколько методов расчёта. Рассмотрен ряд фильтров и современных антенн, с линейной и круговой поляризацией, анализируемых с помощью HFSS. Даны методы расчёта и установка опций программы HFSS в ходе построения трехмерных моделей волноводных, и антенных структур. Рассматривается оптимизация СВЧ структур, значительно усиливающая скорость проектирования.

программа HFSS, СВЧ устройства, фильтры, антенны, линейная и круговая поляризация, трехмерная модель, волноводные структуры.

HFSS – High Frequency System Simulation компании Ansoft – это пакет программ автоматизированного проектирования, моделирования и анализа трехмерных СВЧ структур. В разработке программы участвовали фирмы Hewlett Packard, Agilent и Ansoft. Программа HFSS использует возможности строгого электродинамического моделирования и применяется при проектировании СВЧ устройств для решения широкого круга задач.

В основе электродинамического моделирования в программе HFSS лежит метод конечных элементов (МКЭ). Программа HFSS позволяет с высокой точностью рассчитывать матрицы рассеяния и матрицы импедансов СВЧ многополюсников. Решение граничной задачи ищется в частотной области. Программа HFSS получила распространение и признание во всем мире.

Однако, следует заметить, что программа HFSS представляет собой лишь совокупность команд и требует от разработчика понимания возможностей программы и творческого подхода для решения конкретной электродинамической задачи. Для точного решения требуется разработка 3-D модели с черчением всех форм, правильное задание граничных условий на границе раздела между трехмерной моделью и окружающим пространством, волновых портов, их интегральных линий и установка параметров решения задачи. Необходимо выбрать параметры адаптивного измельчения сетки для обеспечения сходимости результатов и параметры частотной развертки для получения решения в диапазоне частот

Пакет HFSS позволяет рассчитать основные характеристики антенн, в том числе коэффициент усиления, коэффициент эллиптичности, трехмерные диаграммы направленности в дальней зоне, сечения диаграммы направленности, ширину луча по уровню 3 дБ, поляризационные характеристики и т. д. HFSS вычисляет также характеристические импедансы порта и постоянные распространения в регулярных линиях передачи, подключенных к портам, одномодовые и многомодовые матрицы рассеяния СВЧ устройств, собственные волны и собственные колебания различных волноведущих и резонансных СВЧ структур.

Перед решением электродинамической задачи необходимо начертить анализируемую структуру, задать материалы для каждого объекта, указать порты и задать граничные условия на поверхностях. Затем HFSS рассчитает электромагнитное поле в каждой точке исследуемой структуры и найдет по этим данным *S*-параметры и другие характеристики. При расчете *S*-параметров HFSS предполагает, что структура возбуждена типами волн (модами), связанными с геометрией сечения порта. Решения двумерного поля, сгенерированные для каждого волнового порта, служат граничными условиями на этих портах для трехмерной задачи. Окончательное решение поля должно соответствовать двумерному распределению поля в каждом порту [1].

HFSS генерирует решение, возбуждая каждый волновой порт отдельно. Каждая падающая мода на порте несет один ватт усредненной во времени мощности. Порт 1 возбужден сигналом, равным одному ватту, а на другие порты мощность не подается. После того, как решение получено, на порт 2 назначается мощность в один ватт, а на другие порты мощности не подаются и т. д.

Перед тем, как задать порт, нужно перевести выделение в режим поверхность. Затем выделить цветом внешнюю поверхность порта, как показана на рисунке 1 и задать волновой порт командой HFSS → Excitations→ Assign→ Wave Port.

Кроме того, нужно задать линию интегрирования. Линия интегрирования – это вектор, который представляет линию калибровки, определяющий направление распределения поля возбуждения в порте или импедансную линию, вдоль который вычисляется импедансы порта [2].

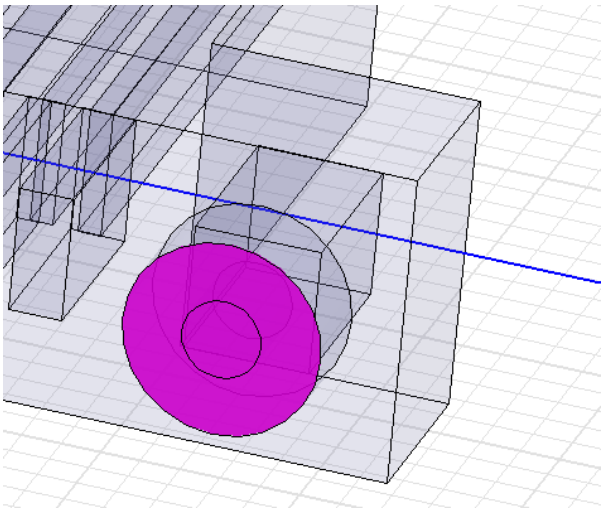


Рис. 1. Выделение внешней поверхности волнового порта (*Wave Port*)

Перед проведением анализа требуется задать параметры разбиения конструкции на тетраэдры. Для этого используются последовательность команд HFSS → Analysis Setup → Add Solution Setup. Появится окно Solution Setup (рис. 2), в котором нужно указать:

Setup Name – имя установки разбиения, так как для одной модели можно задать несколько вариантов установок;

Solution Frequency – частота решения. Это частота, на которой происходит разбиение структуры на тетраэдры. Для фильтра она равна центральной частоте.

На рисунке Maximum Number of Passes – максимальное число уплотнений ячеек, которое будет выполниться в процессе решения. Рекомендуется устанавливать 8–15. Если максимальное число проходов не завершено, адаптивный анализ будет продолжаться, пока не будет достигнут критерий остановки. Когда выполнено заданное число проходов, анализ останавливается. Maximum Delta S per Pass – критерий остановки для адаптивного решения. Если величина и фаза всех S-параметров изменяется на величину меньшую указанной, то процесс адаптации завершается, и программа приступает к решению в диапазоне частот. Чем меньше заданная величина критерия остановки, тем выше точность вычислений. Однако рекомендуется

устанавливать не менее 0,02. Необходимо заметить, что установка максимального числа проходов более 20 и критерия остановки менее 0,005 ведет к увеличению затрачиваемого времени и ресурсов компьютера, а в некоторых случаях и к зависанию системы. Остальные закладки окна Solution Setup можно принять без изменения [3].

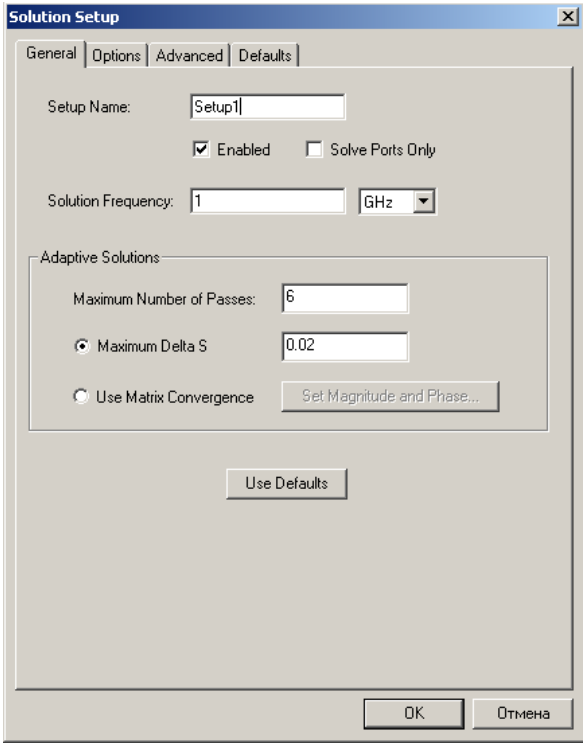


Рис. 2. Установка параметров анализа

Постановка задачи также включает установку частотного диапазона для анализа и определение условий сходимости решения. HFSS может получить решение электродинамической задачи как для фиксированной частоты, так и для ряда частот.

Если построенная модель обладает геометрической симметрией, то ее можно рассечь плоскостями симметрии, в полученных сечениях задать граничные условия и решать задачу лишь для части структуры. Если разбиение произведено корректно, то полученные результаты будут справедливы и для полной модели. Использование свойств симметрии позволяет значительно сократить объем вычислений, что приводит к заметному уменьшению времени расчета и повышению точности результатов.

Данная функция пакета HFSS особенно полезна при расчете параметров антенных многолучевых систем, состоящих из определенного числа одинаковых, не взаимодействующих между собой излучателей. В данном случае для определения суммарного поля системы достаточно рассчитать поле одного излучателя.

После черчения объектов, анализируемых в задаче, придания материальных свойств и создания необходимых поверхностей необходимо задать на них граничные условия. Электромагнитное поле фиксировано задается на этих границах, а на остальном пространстве поле находится в процессе решения, исходя из уравнений Максвелла. Граничные условия определяют поле на гранях объектов в области анализа и поверхностях объектов.

При анализе антенн необходимо решить открытую задачу, в которой волны излучаются бесконечно далеко в пространство. В этом случае необходимо выбрать специальную границу излучения Radiation. HFSS поглощает волну на границе Radiation, по существу на сферической границе, расположенной бесконечно далеко от структуры. Поверхность излучения может быть не сферической, но она должна быть выпуклой по отношению к земляной поверхности и источнику излучения и находиться, по крайней мере, на четверть длины волны от источника излучения. В некоторых случаях граница излучения может быть ближе, чем четверть длины волны, например, для части границы Radiation, где ожидается небольшое излучение.

В HFSS имеется альтернатива границе Radiation – слои PML. Идеально согласованные слои PML являются виртуальными объектами, которые полностью поглощают падающие на них электромагнитные поля.

Есть два способа применения слоя PML: замыкание его на свободное пространство и на нагрузку, в которой отражение отсутствует. При замыкании на свободное пространство PML связывается с поверхностью, которая излучает в свободное пространство одинаково в каждом направлении.

PML как граница излучения лучше, чем граница Radiation, потому что применение PML дает возможность установить поверхности излучения ближе к излучаемым объектам, уменьшая область расчета.

Слой PML смоделирован так, что с учетом отсутствия отражения направленных волн структура продлевается, что постепенно увеличивает толщину отдельных слоев к бесконечности. Поверхности, на которые она нагружена излучают в направлении, в котором распространяется волна. PML с отсутствием отражения применяется, например, для моделирования фазированной антенной решетки.

Важным моментом при анализе антенн и СВЧ-устройств в HFSS является этап разбиения исследуемой структуры на элементарные ячейки.

Разбиение объекта на элементарные ячейки – тетраэдры – является достаточно сложной самостоятельной задачей. В пакете HFSS она решается с помощью специальной программы Mesher.

Появление ячеек с размерами, большими $\lambda / 10$ (λ – длина волны в среде, в которой ищется решение), нежелательно.

На рисунках 3–5 показаны примеры разбиения пространства на ячейки, выполненные в HFSS. Рисунки 4 и 5 иллюстрируют также зависимость решения для электромагнитного поля от плотности разбиения.

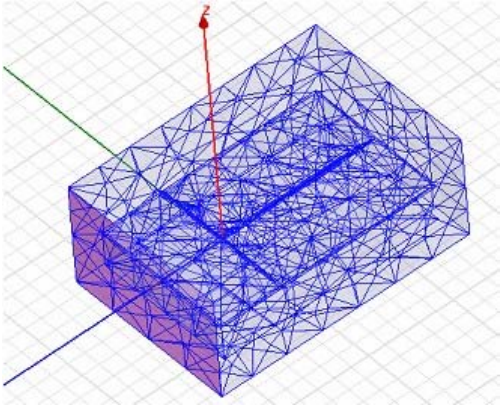


Рис. 3. Пример разбиения пространства в HFSS

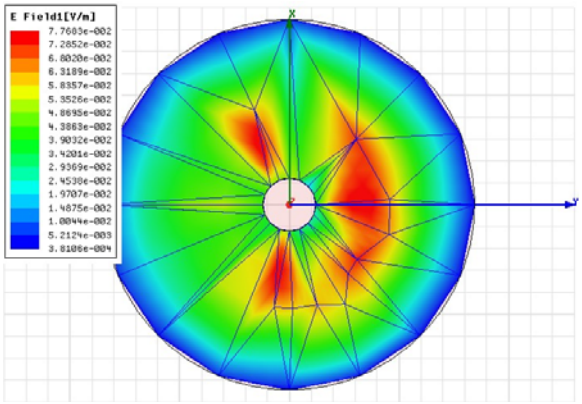


Рис. 4. Распределение поля в резонаторе при уплотнении плотности разбиения

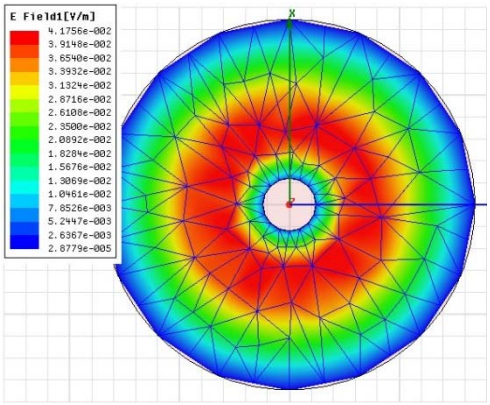


Рис. 5. Распределение поля в резонаторе при не достаточной сетки разбиения

Разбиение пространства на ячейки нарушает исходную структуру объекта таким образом, что его свойства могут исказиться. Безусловно, что по мере уменьшения размеров ячеек и увеличения их числа, поле, которое находится методом конечных элементов, стремится к истинному полю в структуре, т. е. имеется сходимость итерационного процесса. Однако очень часто в электродинамике даже небольшие искажения структуры могут вызывать существенные отклонения в электромагнитном поле и основных характеристиках. Например, при недостаточной плотности разбиения модели круглого резонатора (рис. 4) рассчитанная резонансная частота составила 2,116 ГГц. После применения уплотненной сетки разбиения существенно изменилось распределение поля в резонаторе (рис. 5), а рассчитанная резонансная частота стала равна 2,1349 ГГц.

Главный плюс программы HFSS – ее полная совместимость с другими программами проектирования, такими как Microwave Office, Serenade Ansoft, решающие другой спектр задач и являющиеся на данный момент высоко востребованными в среде инженеров, работающих с СВЧ устройствами, а также относительная простота и наглядность.

Список используемых источников

1. Банков С. Е., Курушин А. А. Проектирование СВЧ устройств и антенн с Ansoft HFSS. М. : Научное издательство: самиздат, 2009. 736 с.
2. Банков С. Е., Гутцайт Э. М., Курушин А. А. Расчет антенн и СВЧ структур с помощью HFSS. М. : ЗАО «НПП Родник», 2009. 256 с.
3. Банков С. Е., Гутцайт Э. М., Курушин А. А. Анализ и оптимизация трехмерных СВЧ-структур с помощью HFSS. М. : Солон-Пресс, 2012. 215 с. ISBN 5-98003-226-6.

УДК 57.087

ИСПОЛЬЗОВАНИЕ ДАННЫХ О СЕРДЕЧНОМ РИТМЕ ДЛЯ КОНТРОЛЯ СОСТОЯНИЯ ОБУЧАЕМОГО

П. Д. Дмитриев

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

В настоящей статье предлагается подход к решению задачи выделения «критерия обучаемости» и психофизиологического состояния человека на основе вариабельности сердечного ритма. Проанализированы возможные способы решения поднимаемой задачи. В качестве главного инструмента выбран индекс вагосимпатического взаимодействия, который строится посредством спектрального анализа длительностей кардиоинтервалов в режиме реального времени.

Рассмотрена и обоснована возможность применимости предлагаемого подхода для тренажеров и комплексов обучения персонала. Статья содержит результаты экспериментальных данных проведенных на добровольцах. Данный материал следует рассматривать как задел для последующих исследований.

обучение, тренажер, безопасность труда, оценка состояния человека, сердечный ритм.

В современном мире человеческий фактор играет все большую и большую роль. Это справедливо для профессий, которые связанны с экстремальными и опасными для жизни условиями. Кроме того, для операторов, эксплуатирующих сложные добывающие, транспортные или технические системы и комплексы. Ярким примером служат шахтеры, службы спасения, пилоты, водители, машинисты.

К сожалению, отнюдь не редким случаем являются аварии на шахтах, столкновения автомобилей, крушение поездов, по причине человеческой ошибки. Причем можно выделить, как банальное недомогание, так и фатальные ошибки, которые могут возникнуть из-за множества явлений, повседневно влияющих на человека.

Одним из вариантов сокращения нештатных ситуаций является наблюдение за человеком (оператором) с помощью видеокамер, однако суще-

ствует ряд недостатков, при которых данный подход не может быть использован повсеместно. Тяжело представить видеонаблюдение в штреках шахты или в горящем здании. Да и организация видеонаблюдения представляется задачей не из дешевых.

Другой вариант, это отслеживать физиологические параметры организма: температуру, сердечный ритм, количество вдыхаемого кислорода и выдыхаемого углекислого газа и многое другое. Однако, в рамках настоящей статьи будет рассмотрен подход, основанный на данных о сердечном ритме. Такой показатель был выбран по причине его информативности, аппаратная часть довольно дешева, модульна и развиваема.

В статье представлены 2 способа измерения сердечного ритма, наиболее популярные на сегодняшний день. Первый из них – это измерение электрической работы сердца – электрокардиография, (ЭКГ); второй – плетизмография.

По сути, сердце является электрическим органом. Электрические сигналы, генерируемые сердцем, организуют последовательность мышечного сокращения в каждом сердечном цикле, оптимизируя таким образом насосную функцию сердца. Кроме того, форма и продолжительность электрических сигналов сердца определяют сердечный ритм. Сутью данного метода является регистрация электрических потенциалов, возникающих во время работы сердца [1]. Среди всех составных частей электрокардиограммы стоит выделить зубец R, так как он является основным зубцом в ЭКГ, а время между пиками основной информацией о сердечном ритме. Время между зубцами R носит название R-R интервал (кардиоинтервал).

Дальнейшая обработка производится следующим образом: по значениям кардиоинтервалов формируется неравномерная шкала времени:

$$T = \begin{cases} t_0 = 0 \\ \dots \\ t_i = t_{i-1} + RR_i \end{cases},$$

где, RR – это значение кардиоинтервала.

После чего производится сплайн-интерполяция на равномерную шкалу времени с шагом 0,25 сек, которая позволяет прейти к следующему шагу обработки: быстрому преобразованию Фурье (БПФ). Осуществляется спектральный анализ динамического ряда кардиоинтервалов и измеряется спектральная мощность сигнала в низкочастотной (LF) и высокочастотной (HF) областях спектра. Низкочастотный диапазон – 0,04÷0,15 Гц; высокочастотный – 0,15÷0,4 Гц. Искомый показатель носит название индекс вагосимпатического взаимодействия (ИВВ), показывает отношение мощностей низкочастотной области к высокочастотной, или с физиологической точки зрения – отношение состояния симпатического отдела нервной системы к парасимпатическому [2, 3].

Второй метод – плетизмография. Он основан на регистрации изменения объемов кровенаполнения. Клинические возможности плетизмографии выходят далеко за рамки простого определения пульса, но в рамках данной статьи интересен именно он. Кроме того, из разновидностей данного метода, рассматривается оптический вариант или фотоплетизмография (ФПГ), так как один из самых популярных и показательных [4]. Метод довольно прост: производится просвет тканей световым потоком. Сужение и расширение сосуда под действием артериальной пульсации вызывают соответствующее изменение амплитуды сигнала, получаемого с выхода фотоприемника. ФПГ является наиболее универсальным, так как мест для съема сердечного ритма возможно использовать очень много, например, концевые фаланги пальцев рук и ног, запястья, лоб, мочки ушей. Детектирование *r*-пиков осуществляется по быстро нарастающему переднему фронту пульсовой волны, который является типичным для всех основных форм ФПГ. Дальнейшая обработка аналогична уже описанной.

Данная тематика нашла отражение в мире, например, компания HP занимается сбором и анализом физиологических данных в процессе вождения для определения уровня стресса водителя. В качестве биосигналов используются электрокардиограмма, электромиограмма, кожная проводимость, и дыхательная активность [5].

Определением уровня стресса водителя занимается и институт технологии и науки Бирлы в Пилани (*Birla Institute of Technology and Science*). В основе метода лежит фотоплетизмография и кожно-гальваническая реакция [6].

Автором статьи был проведен ряд экспериментов. Использовался спортивный нагрудный датчик сердечного ритма и профессиональная медицинская беговая дорожка. База испытуемых насчитывала 10 человек. Все испытуемые подвергались физической нагрузке по одному сценарию. Некоторые результаты эксперимента приведены на рисунке.

Стоит отметить, что был выделен факт понижения значения ИВВ при повторном экспериментальном исследовании. Однако выявленный критерий понижения справедлив только для человека, на котором проводился эксперимент.

Далее встают вопросы о дальнейшем использовании и вариантах развития. Областей применения действительно очень много, от контроля на производствах и выработках, контроля водителей подвижного состава. Но одну область стоит отметить отдельно. Это контроль при обучении персонала, например, при обучении пилотов или выработке навыка дыхания в средствах индивидуальной защиты органов дыхания (СИЗОД). При использовании на процедурных тренажерах вполне допустимо имитировать чрезвычайные ситуации и посредством предложенной методики следить за реакцией обучаемого. Результатом может быть заключение о прохождении или не прохождении заданной тренировки и выданы рекомендации.

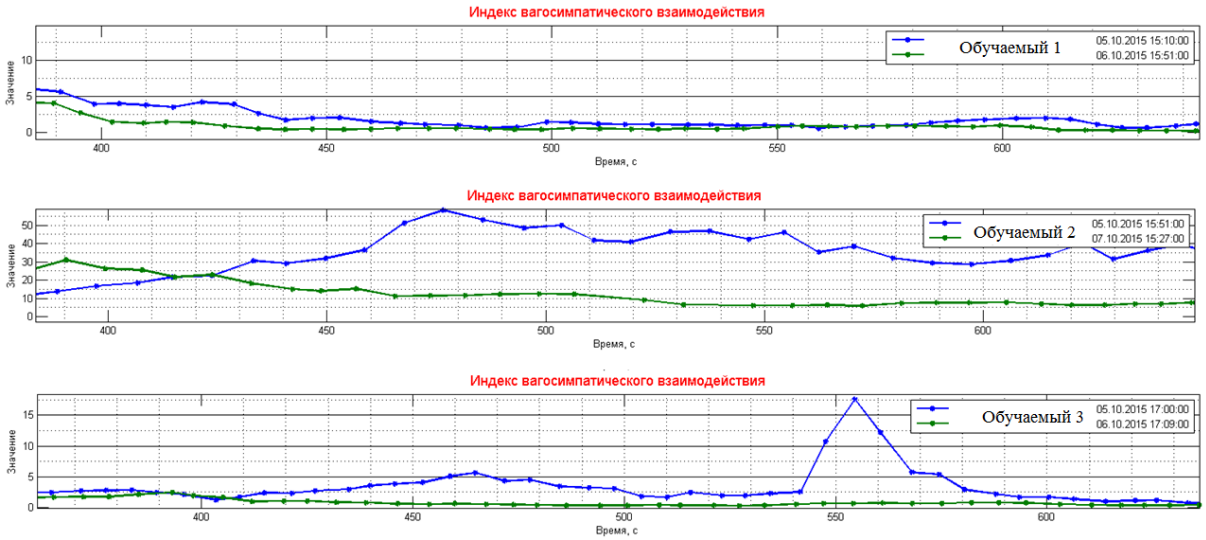


Рисунок. Результат эксперимента для трех обучаемых

К вариантам развития можно отнести выделение общего критерия или ряда критериев для определенных групп. Для этого требуются комплексные экспериментальные исследования на большой группе людей, не привязанные к возрасту и полу. Комплексирование с другими биосигналами организма, поиск зависимостей и общих критериев. Создание системы, объединяющей большое количество пользователей и передачей данных о сердечном ритме на удаленный сервер.

Список используемых источников

1. Зудбинов Ю. И. Азбука ЭКГ. Издание третье. Ростов-на-Дону : Феникс, 2003. 160 с. ISBN 5-222-02964-6.

2. Heart Rate. Variability Standards of measurement, physiological interpretation, and clinical use // European Heart Journal. 1996. V. 17. pp. 354–381.

3. Анализ вариабельности сердечного ритма при использовании различных электрокардиографических систем (методические рекомендации) / Под ред. Р. М. Баевского. М. : КНМТ МЗ РФ, 2000. 50 с.

4. Сайт корпорации «Токран». URL: www.tokranmed.ru

5. Jennifer A. Healey, Rosalind W. Picard. Detecting Stress During Real-World Driving Tasks Using Physiological Sensors // Cambridge Research Laboratory; HP Laboratories Cambridge; HPL-2004-229; December 17, 2004*.

6. Rajiv Ranjan Singha, Sailesh Conjetia, Rahul Banerjeeb. A comparative evaluation of neural network classifiers for stress level analysis of automotive drivers using physiological signals // Biomedical Signal Processing and Control, 2013.

Статья представлена научным руководителем, доктором технических наук, профессором М. А. Сиверсом.

УДК 623.624

РЕЗУЛЬТАТЫ МОДЕЛИРОВАНИЯ И ЭКСПЕРИМЕНТАЛЬНЫХ ИССЛЕДОВАНИЙ ЭЛЕКТРОФИЗИЧЕСКИХ СВОЙСТВ ВЫСОКОДОБРОТНЫХ КОМПОЗИТОВ

А. Д. Иванов, Т. Ю. Ковалева, Т. А. Рыжикова

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

В работе представлены результаты моделирования и экспериментальных исследований радио прозрачных свойств высокодобротных композитов, предназначенных для антенных обтекателей и укрытий, функционирующих в заданном частотном диапазоне.

полимерная матрица, аэродисперсный наполнитель, стеклоткань.

Высокодобротные композиты (ВДК) представляют класс материалов с малыми значениями электрофизических параметров – диэлектрической проницаемости и тангенса угла диэлектрических потерь. При заданных значениях электрофизических параметров композиты обладают радиопрозрачными свойствами для прохождения электромагнитной волны (ЭМВ) и находят широкое применение в конструкциях антенных укрытий и обтекателей антенн.

Защита РЛС от воздействия окружающей среды не должна существенным образом изменять диаграмму направленности антенных устройств. Агрессивное внешнее воздействие на диэлектрические материалы может существенно изменить важнейшие характеристики радиосистемы вплоть до вывода её из строя. Параметры диэлектрических материалов, из которых изготавливаются радиопрозрачные укрытия (РПУ) антенн СВЧ, в значительной мере определяют функциональные возможности укрываемых ими антенных систем.

При разработке нового высокодобротного композита задаются характеристики, необходимые для его функционального назначения, превосходящие характеристики традиционных материалов при выполнении данной цели в данном изделии, но уступающие им в каких-либо других аспектах.

Путем моделирования, подбора состава, свойств наполнителя, матрицы (связующего) и их соотношений, можно получить материалы с требуемым сочетанием эксплуатационных и технологических свойств.

Прозрачность ВДК обеспечивается малыми диэлектрическими потерями в заданном интервале рабочих температур ($tg\delta$ 10^{-2}–10^{-5}, $\varepsilon \leq 10$), и низким уровнем отражения радиоволн ($|\Gamma| \leq 1$ %) в заданном частотном диапазоне, подбором диэлектрической проницаемости отдельных слоев и соответствующим электродинамическим расчётом толщины слоев.

Технические полимерные композиты в большинстве случаев являются неоднородными (сложными) диэлектриками, состоящими из разнородных по электрическим свойствам частиц или слоев (наполненные композиции, миканиты, гетинакс, текстолит, лакоткань, пенопласты и т. д.).

При разработке полимерных ВДК с заданными электрофизическими свойствами учитывалось, что диэлектрическая проницаемость сложных диэлектриков, представляющих собой смесь компонентов с различными диэлектрическими проницаемостями, подлежит моделированию [1] и расчету.

На практике часто используются неоднородные композитные диэлектрики, представляющие собой смеси двух или более различных веществ – компонентов смеси. К таким материалам относятся многие пластические массы, состоящие из полимерной матрицы (связующего) и наполнителей, керамических, волокнистых, стеклянных, пропитанных и непропитанных пористых материалов и т. п.

Для расчета эффективной диэлектрической проницаемости смеси предполагается, что ее отдельные компоненты не вступают друг с другом в химические реакции, т. е. смесь является физической.

Для расчета диэлектрических потерь и диэлектрической проницаемости наполненного композита используют эквивалентные схемы замещения, как отдельных компонентов, так и всего неоднородного диэлектрика. Возможные варианты упорядоченного расположения компонентов могут быть представлены в виде их параллельного и последовательного включения.

Для расчета диэлектрической проницаемости мелкодисперсных хаотических смесей, которые находят практическое применение при синтезе композитов, широко используется формула Лихтенеккера. Она дает результаты расчета, достаточно хорошо совпадающие с измеренными величинами, если ε1 и ε2 не очень сильно отличаются друг от друга.

$$\ln \varepsilon = \Theta_1 \ln \varepsilon_1 + \Theta_2 \ln \varepsilon_2.$$

Для смесей типа пенопластов, поропластов, пенокерамики и других пористых материалов, состоящих из твердого и газообразного диэлектрика, удобнее пользоваться не объемными концентрациями компонентов, а их массовым содержанием в смеси. Плотность смеси можно рассчитать на основании закона смешения:

$$\rho = \Theta_1 \rho_1 + \Theta_2 \rho_2,$$

где ρ – плотность смеси (кг/м^3), ρ_1 и ρ_2 – плотности компонентов (кг/м^3).

Для радиопрозрачных изделий (РПИ) требуются композиты с малыми значениями диэлектрических проницаемостями от 1,5 до 1,8. В этом случае выражение для расчета эффективной диэлектрической проницаемости смеси принимает вид:

$$\varepsilon = \Theta_1 \times \varepsilon_1 + \Theta_2 \times \varepsilon_2,$$

где ε_1 и ε_2 – соответственно диэлектрические проницаемости отдельных компонентов смеси; Θ_1 и Θ_2 – объемные концентрации компонентов, удовлетворяющие соотношению $\Theta_1 + \Theta_2 = 1$, определяются формулой:

$$\Theta = m / \gamma,$$

где m – масса, г; γ – удельный вес, г/см^3.

Некоторые результаты расчета диэлектрической проницаемости смеси ВДК на основе аэрированного наполнителя при различных полимерных матрицах представлены в таблице 1.

ТАБЛИЦА 1. Результаты расчета диэлектрических параметров смесей

Тип наполнителя	Микросферы стекла, марки ВК 25						
Концентрация наполнителя	10	15	20	25	28	30	32
Тип полимерной матрицы	Хлорсульфированный полиэтилен ХСПЭ						
Вещественная ε′	2,241	2,251	2,26	2,269	2,275	2,28	2,29
Мнимая ε″	0,06	0,04	0,05	0,03	0,02	0,008	0,003
Тип полимерной матрицы	Эпоксидная смола						
Вещественная ε′	4,65	4,6	4,5	4,42	4,37	4,25	4,2
Мнимая ε″	0,08	0,07	0,06	0,03	0,02	0,009	0,005

Микросферы стекла являются микрообъемами с воздушным наполнением, часто используется в качестве высокочастотного наполнителя, обладают хорошей теплостойкостью и отличаются стабильностью радиофизических характеристик в различных условиях эксплуатации.

Моделирование радиофизических и конструктивных параметров, исходя из заданных требований по диапазону частот радиопрозрачности и обеспечению потерь эМЭ не более 0,3 Дб.

Ослабление амплитуды ЭМВ, прошедшей через плоский диэлектрический слой с потерями определяется соотношением:

$$F_1 = \exp\left[-2\pi\, d_1 / \lambda \cdot (\varepsilon_1\, 1/2\, \mathrm{tg}\delta_1) / (\sqrt{\varepsilon_1} - \sin^2\theta) - j\varphi_1\right], \qquad (1)$$

где $\varphi_1 = 2\pi\, d_1 (\sqrt{\varepsilon_1} - \sin^2\theta)\, 2$ – фазовый угол; λ – длина волны; φ – угол падения ЭМВ на слой диэлектрика; ε – диэлектрическая проницаемость материала; d – толщина слоя; tg δ – угол диэлектрических потерь в слое.

Коэффициент прохождения ЭМВ диэлектрического слоя определяется через коэффициент ослабление:

$$T_1 = F_1\,(1 - r_0)\,(1 - r_{12}) / (1 + F_1^2\, r_{01}\, r_{12}),$$

где r_{01}, r_{12} – коэффициенты Френеля.

При малой величине диэлектрических потерь, т. е. tgδ << 1, выражение (1) для ослабления амплитуды волны принимает вид:

$$F_1 = e^{-j\varphi}$$

и коэффициент прохождения ЭМВ через слой РПД будет следующим:

$$T_{02} = T_1\, e^{-\alpha 1},$$

где α_1 – коэффициент затухания, T_1 – коэффициент прохождения.

Коэффициент прохождения ЭМВ через слой диэлектрика без потерь определяется по круговой диаграмме. Результаты расчета коэффициента прохождения в заданном диапазоне представлены на рисунке.

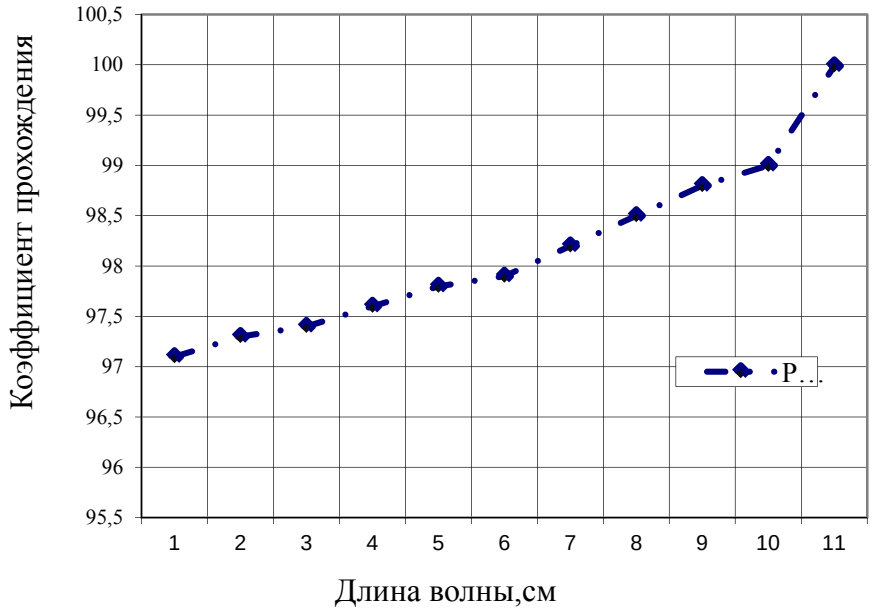


Рисунок. Зависимость коэффициента прохождения от длины волны

Результаты расчета коэффициента прохождения для трех вариантов толщин (стенок обтекателя) представлены в таблице 2.

ТАБЛИЦА 2. Расчетные частотные зависимости коэффициентов прохождения для трех вариантов стенки обтекателя различной толщины

Частота, ГГц	Длина волны, см	ε′	ε″	1*d*, мм	2*d*, мм	3*d*, мм	1–*T*, %	3–*T*, %
15,00	2	1,6	0,001	1,4	2,0	2,5	99,96	99,42
14,29	2,1	1,6	0,001	1,4	2,0	2,5	99,96	99,43
13,64	2,2	1,6	0,001	1,4	2,0	2,5	99,96	99,45

Частота, ГГц	Длина волны, см	ε′	ε″	1*d*, мм	2*d*, мм	3*d*, мм	1–*T*, %	3–*T*, %
12,50	2,4	1,6	0,001	1,4	2,0	2,5	99,97	99,49
12,00	2,5	1,6	0,001	1,4	2,0	2,5	99,97	99,50
11,54	2,6	1,62	0,0011	1,4	2,0	2,5	99,97	99,51
10,00	3	1,63	0,0011	1,4	2,0	2,5	99,97	99,55
7,50	4	1,65	0,0012	1,4	2,0	2,5	99,97	99,56
6,00	5	1,67	0,0013	1,4	2,0	2,5	99,98	99,57
5,00	6	1,7	0,0015	1,4	2,0	2,5	99,98	99,58
4,29	7	1,73	0,0016	1,4	2,0	2,5	99,98	99,60
3,00	10	1,79	0,0024	1,4	2,0	2,5	99,98	99,63
2,94	10,2	1,8	0,0027	1,4	2,0	2,5	99,99	99,65
2,86	10,5	1,8	0,0027	1,4	2,0	2,5	99,99	99,68
2,73	11	1,8	0,0028	1,4	2,0	2,5	99,99	99,72

Список используемых источников

1. Ковалева Т. Ю., Доценко С. М., Кирик Д. И. Композитный материал для антенных укрытий и обтекателей // Труды МКЭЭЭ-2014. Электромеханика, электротехнологии, электротехнические материалы и компоненты: материалы 15 межд. конф., Крым, Алушта, 21–27 сентября 2014 г. С 35–36.

УДК 654.172

МЕТОДЫ ПОИСКА ИЗОБРАЖЕНИЯ ПО ЗАПРОСУ ПОЛЬЗОВАТЕЛЯ

М. И. Иванова

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

Необходимость поиска участка видео в архивах или базах данных привело к развитию систем поиска изображений. Такие системы пользуются различными методами. Наибольший интерес представляют объектно-ориентированные методы поиска, так как они основаны на распознавании объектов изображения. Однако, основной проблемой остается «семантический разрыв». Существуют методы, значительно уменьшающие разрыв. Однако, на данный момент, нет метода, который бы полностью решал проблему «семантического разрыва».

метод поиска, семантический разрыв, признак низкого уровня, семантические признаки, объектно-ориентированный метод.

С развитием информационных технологий и увеличением числа видео устройств, значительно вырос объем видеоинформации, и появились видео базы данных и видео архивы. В связи с этим возникла потребность нахождения конкретного изображения или участка видео по запросу пользователя.

Данную процедуру реализуют системы поиска изображений. В общем случае процесс поиска сводится к нахождению изображений, наиболее удовлетворяющих запросу. Необходимым условием в поиске является совпадение запроса пользователя и описания изображения. Описание есть некий набор особенностей, характеризующий изображение.

Источником описания может служить текст или изображение. Поэтому различают два класса методов поиска: контекстные и контентные. Контекстные опираются на формирование описаний и присвоение их изображению. Запросом в этом случае является текст. Контентные методы основываются на анализе содержания изображения. Запросом в этом случае может быть изображение-образец.

Контекстный поиск изображений основан на анализе сопроводительной к изображению текстовой информации. Источником текстовой информации может быть текстовая часть документа, в котором находится изображение, либо текстовая аннотация, непосредственно введенная пользователем.

Контентные методы поиска изображений базируются на анализе содержательной стороны изображений. Поэтому ключевыми моментами являются: во-первых, извлечение и представление информации о содержании изображений, то есть формирование описания изображений; во-вторых, определение схожести между запросом и описаниями изображений из базы данных.

Множество контентных методов можно разделить на два подкласса: признаковые и объектно-ориентированные. Признаковые методы представляют изображения в виде вектора различных признаков (цвета, текстуры, формы, положения и др.). Поэтому описание изображений в данном случае формируется из числовых значений различных признаков. Объектно-ориентированные методы поиска изображений по содержанию отличаются от признаковых использованием методов распознавания для перевода содержания изображений на семантический уровень.

Таким образом, основное назначение признаковых методов – поиск похожих по внешним признакам изображений в коллекции данных, в то время как назначение объектно-ориентированных методов – поиск изображений, похожих по объектному составу (или семантическому содержанию).

Наибольший интерес представляют объектно-ориентированные методы, так как они основаны на распознавании объектов изображения. На данный момент, объектно-ориентированные методы используют многоуровневые модели обработки изображений [1].

В таких моделях процесс поиска разбивается на два основных этапа: определение объектов изображений и сопоставление выявленных объектов на изображении-образце с объектами изображений, хранящихся в базе данных. Первый этап начинается с извлечения смысловых областей на исходном изображении. Затем по выявленным областям происходит идентификация интересующих объектов.

Второй этап, сопоставление, характеризуется выделением основных свойств и атрибутов идентифицированных объектов изображения-образца. Затем осуществляется равнение объектов изображения-образца с объектами изображений, хранящихся в базе данных. После этого происходит извлечение изображений из базы данных, которые наилучшим образом соответствуют запросу пользователя. Кроме того, возможно использование обратной связи, которая выполняется за счет интерактивного взаимодействия человека и системы поиска с целью корректирования процесса поиска.

Однако существующие объектно-ориентированные методы работают на относительно небольшом объёме объектов и классов распознавания, т. е. способны решать задачу распознавания, но на множестве изображений, ограниченном по объектному содержанию.

В связи с этим все еще существует проблема «семантического разрыва». «Семантический разрыв» – разница между низкоуровневым описанием и семантическим содержанием. Основной проблемой остается перевод низкоуровнего представления признаков на семантический уровень, который оперирует объектами и сценами изображений.

Существуют методы, значительно уменьшающие разрыв. Например, метод, основанный на информационном взаимодействии.

Информационное взаимодействие в широком смысле – процесс взаимодействия информационных и неинформационных объектов друг на друга через информационную среду, информационные модели и информационные технологии [2]. Одной из особенностей информационного взаимодействия является возможность информационного копирования. Это означает, что при информационном взаимодействии возможна передача части свойств и признаков одного (передающего информацию) объекта в другой (принимающий информацию) путём их копирования или путём полного перемещения. При этом информационные свойства передающего объекта не изменяются.

Применительно к проблеме семантического разрыва, информационное представление следует понимать, как процесс взаимодействия, основным содержанием которого является достижение необходимой цели семантического соответствия между исходным и порожденным объектами на основе

использования информационных ресурсов (объемов, потенциалов, структур, качественных и количественных признаков).

Основная часть процессов информационного взаимодействия связана с двухсторонним или односторонним обменом информации. По существу, информационное взаимодействие структурно повторяет процесс управления с обратной связью. При формализации описания один объект является исходным (эталоном), второй – порожденным (копией). Это определяет качественное неравенство между ними. Исходный объект имеет большую полноту описания. При таком взаимодействии участвует субъект, поэтому в информационном поле необходимо рассматривать триаду «эталон – субъект – копия». При информационном взаимодействии субъект принимает информацию о текущем описании порожденного объекта. Если текущее описание не адекватно эталону, то формируется новое формальное описание в рамках того языка, на котором оно выполнено. Этот цикл повторяется, пока не будут исчерпаны возможности языка формального описания порожденного объекта.

Или же метод, который базируется на многоуровневой модели и использует в поиске семантические признаки. Целью использования данной модели является результат взаимодействия контекстного и контентного методов, позволяющий преобразовывать один тип описания объекта в другой для возможности использования различных типов пользовательских запросов [3].

Многоуровневая модель обработки и описания данных состоит из четырех базовых уровней: уровень элемента пространства признака (0), уровень элементарного элемента признака (1), уровень признака, образа, понятия (2), языковой уровень (3). Компоненты многоуровневой модели – элементы и представления уровня. Элементы – система постоянных единиц знаний, которые могут использоваться при обработке. Представления – описание данных. Семантический признак – особый компонент, который обеспечивает взаимосвязь уровней модели.

На каждом уровне изображение анализируется на наличие особенностей и определение их количественных характеристик. Первый уровень является уровнем взаимодействия с изображением. На этом уровне внешнее изображение переводится в вид, в котором каждому пикселю или области изображения соответствует элемент из пространства некоторого признака. На втором уровне выделяют различия признаков изображения, которые должны соотноситься с ощущениями человека. Следующий уровень предназначен для определения признаков, образов, понятий. Наконец, на языковом уровне выявленным признакам, образам, понятиям даётся некоторая языковая интерпретация.

Семантический признак позволяет обеспечить взаимосвязь между низкоуровневыми признаками и их языковыми интерпретациями, то есть изоб-

ражение можно описать посредством языковых единиц или языковые единицы можно представить в виде низкоуровневых признаков. В резуль-тате, помимо перевода содержания изображений на языковой уровень и дальнейшего текстового поиска, можно реализовать поиск по представле-ниям изображений на уровнях ниже языкового с использованием текстового запроса.

Это не единственные существующие методы, которые частично описывают пути решения проблемы. Однако, на данный момент, нет метода, который бы полностью решал проблему «семантического разрыва».

Список используемых источников

1. Zhang Y.-J. Toward high-level visual information retrieval // Semantic-based visual information retrieval. Hershey, PA: IRM Press, 2007. pp. 1–21. URL: http://oa.ee.tsinghua.edu.cn/~zhangyujin/Download-Paper/E135=SBVIR-07b.pdf.

2. Цветков В. Я. Информационное взаимодействие как механизм устранения семантического разрыва // European Researcher. 2013. Vol. (45). № 4-1.

3. Папулин С. Ю. Поиск электронных изображений по семантическим // Программные продукты и системы. 2011. № 1. С. 10–16.

Статья представлена научным руководителем, кандидатом технических наук, доцентом С. Л. Федоровым.

УДК 621.396

ПЕРСПЕКТИВЫ ИСПОЛЬЗОВАНИЯ КА-ДИАПАЗОНА ДЛЯ СПУТНИКОВОГО ШИРОКОПОДОСНОГО ДОСТУПА В РЕСПУБЛИКЕ КАЗАХСТАН

Ж. А. Каймолдинова[1], А. Н. Ликонцев[2]

[1]Евразийский национальный университет им. Л. Н. Гумилева (Астана)
[2]Санкт-Петербургский государственный университет телекоммуникаций им. проф. М. А. Бонч-Бруевича

Рассмотрена задача исследования Ка-диапазона для спутникового широкополосного доступа и создания спутника связи и вещания «KazSat-4». Приведены основные анализы, обоснование и пути решение.

Ка-диапазон, ШПД, спутниковые системы связи.

Основная проблема космической системы связи и вещания «KazSat» связана с тем, что в 2017 году заканчиваются долгосрочные контракты казахстанских операторов спутниковой связи по аренде спутниковых ем-костей у международных компаний спутниковой связи. Последнее означает,

что необходимо создать и запустить КА «KazSat-4» для удовлетворения потребностей казахстанских операторов спутниковой связи, которые появятся в результате отказа от аренды спутниковой емкости иностранных спутников.

Цель. Удовлетворение растущих потребностей экономики и общества в космических средствах и услугах:

– создание и развитие спутниковой системы связи;

– создание и развитие земной космической инфраструктуры;

– развитие международного сотрудничества в области космической деятельности.

Анализ отрасли. Информационно-коммуникационные технологии (ИКТ) занимают сегодня центральное место в инновационном развитии ключевых сфер жизнедеятельности общества: государственного управления, бизнеса, образования, здравоохранения, культуры, обеспечения безопасности, общественной жизни. Казахстан в настоящее время стоит перед вызовом активно включиться в глобальный процесс развития информационного общества и получить максимальную выгоду от вложений в ИКТ.

Одним из факторов, негативно влияющих на уровень распространения информационных технологий и развитие информационного общества в Казахстане, является недостаточно высокий уровень развития многих областей в этом отношении. Так, сохраняется высокий уровень различия в использовании информационных технологий населением в различных регионах. Остаются проблемы организации широкополосного доступа для конечных пользователей, так же в регионах ниже и доля предприятий, использующих широкополосный доступ в интернет (ШПД).

Согласно предоставленным данным агентства РК по статистике (табл.) в Казахстане наибольшее количество абонентов широкополосного доступа в Интернет.

ТАБЛИЦА. Число абонентов фиксированного Интернета в РК (тыс. единиц)

№ п/п	Регион	2013 г.	2012 г.	Изменения, %
1	Алматы	670,2	553,0	21,2
2	Карагандинская область	163,7	142,8	14,6
3	Астана	127,1	110,1	15,4
4	Восточно-Казахстанская область	111,3	101,8	9,3
5	Алматинская область	106,2	84,0	26,4
6	Костанайская область	105,9	106,8	0,8
7	Павлодарская область	94,5	85,0	11,2

№ п/п	Регион	2013 г.	2012 г.	Изменения, %
8	Южно-Казахстанская область	79,1	65,8	20,2
9	Акмолинская область	78,2	65,9	18,7
10	Актюбинская область	69,2	59,2	16,9
11	Северо-Казахстанская область	68,1	60,7	12,2
12	Атырауская область	65,8	56,5	16,5
13	Жамбылская область	57,3	44,5	28,8
14	Мангистауская область	49,4	39,4	25,4
15	Западно-Казахстанская область	44,0	41,2	6,8
16	Кызылодинская область	38,5	32,1	19,9

Так же является очевидным тот факт, что многими отраслями в Казахстане в ближайшее время потребуется и будет востребован высокоскоростной интернет. К 2020 году, по данным Ericsson, в мире будет насчитываться порядка 50 млрд различных подключенных устройств. Это означает, что в сфере доставки широкополосного интернета и передачи данных будут заняты компании из самых разных индустрий.

Однако нужно признать, что существуют проблемные вопросы по обеспечению высокоскоростного ШПД в сельской местности и на сегодняшний день становится, очевидно, что имеющийся частотный ресурс сетей CDMA недостаточен для удовлетворения возрастающих потребностей абонентов сельской местности в услугах высокоскоростной передачи данных. Одним из выходов из этого положения является развертывание собственной спутниковой системы предоставления высокоскоростного широкополосного интернета для регионов Казахстана с низкой плотностью населения. Конкурирующим преимуществом развертываемых сетей CDMA в сельской местности по сравнению с сетями 3G является большая зона покрытие до 35 км, но ограниченные скорости 512 Кбит/с могут устроить не всех потенциальных потребителей, т. е. отсутствует потенциал коммерческого успеха проекта развертываемых сетей CDMA в сельской местности и в некоторых случаях можно говорить о проблемах по снижению «цифрового неравенства» между городом и селом [1].

Проблему предоставления широкополосного доступа в интернет, возможно решить также развертыванием сетей мобильной связи 3G. Но в малонаселенной местности операторы сотовой связи не видят

коммерческого успеха, поэтому проникновение мобильного широкополосного доступа в интернет в сельской местности не равномерно.

Поэтому для большой территории как в Казахстане актуален вопрос использования транзитных спутниковых каналов для передачи данных используя спутники с высокой пропускной способностью. Что позволит операторам сотовых сетей разместить базовые станции в труднодоступных местах, без прокладки наземных линий связи.

В Казахстане цели в области повсеместного широкополосного доступа в интернет не могут быть достигнуты без использования сочетания технологий широкополосной связи, в том числе кабельных, волоконно-оптических, беспроводных и спутниковых. Исторически наземная инфраструктура сосредоточена в городских центрах, при этом в сельских и отдаленных районах имеется ограниченное покрытие, лишающее некоторые слои населения возможности воспользоваться преимуществами информационного общества.

Услуги спутникового доступа в интернет и широкополосного спутникового доступа обеспечивают возможность охвата соединениями даже наиболее отдаленных районов, где услуги наземного (проводного и беспроводного) доступа недоступны или их развертывание является дорогостоящим. По мере увеличения спроса и разработки стратегий универсального широкополосного доступа для сельских и отдаленных районов происходит увеличение спроса на решения для сельских и отдаленных районов на основе спутникового доступа, в том числе, посредством реализации государственных проектов или создания партнерств с участием государственного и частного секторов, целью которых является расширение возможности доступа.

Основанные на использовании спутниковой связи услуги предоставляют многочисленные преимущества, особенно для отдаленных и сельских районов, где слабо развита наземная инфраструктура, например:

– экономически эффективные и простые с точки зрения реализации решения даже для отдаленных и сельских районов;

– не требуются существенные инвестиции на развитие наземной инфраструктуры;

– обслуживается большое количество конечных пользователей;

– возможность развертывания большой сети;

– фиксированные и подвижные применения;

– предоставление надежных и резервируемых услуг в случае бедствий или чрезвычайных ситуаций.

В настоящее время является общепризнанный фактом перегрузка геостационарной орбиты системами спутниковой связи и вещания в полосах частот С (4/6 ГГц) и Ku (11–12/14 ГГц) и сегодня количество заявленных в МСЭ спутниковых сетей почти достигло 2000 сетей в С-диапазоне

и 2000 сетей в Ku-диапазоне. Поэтому вырос интерес к системам спутниковой связи, работающим в высокочастотном диапазоне 20/30 ГГц.

Таким образом, локомотивом развития телекоммуникационной отрасли Республики Казахстан станет создание современной телекоммуникационной спутниковой системы в Ка-диапазоне.

Обоснование и решение:

В современных условиях постоянно растущего потока информации полноценное использование Интернета невозможно без использования широкополосных линий связи.

С целью развития услуг широкополосного и высокоскоростного доступа (ШПД) к сети Интернет обеспечивается применение ряда новых технологий, которые позволяют пользователям отправлять и принимать информацию в больших объемах и с более высокой скоростью.

Для обеспечения широкополосного доступа к Интернету в Казахстане развиваются следующие направления:

1) модернизация и развитие информационно-коммуникационной инфраструктуры;

2) развитие цифрового телерадиовещания;

3) сокращение «цифрового неравенства» регионов Республики Казахстан (крупные города, моногорода, аулы), предупреждение изолированности отдельных граждан и социальных групп.

Надо признать, что существуют проблемные вопросы по обеспечению высокоскоростного широкополосного доступа к сети Интернет, такие как низкий темп развития ШПД, неполный охват домохозяйств страны услугами телефонной связи и ШПД к сети Интернет в сельской местности.

Несмотря на активное развитие наземных сетей передачи данных, необходимо развивать и наращивать спутниковую группировку, так как она позволяет покрывать большие территории при оптимальном соотношении цены, качества и скорости передачи данных, которое сопоставимо с наземными сетями, более того она позволит обеспечить резервирование наземных каналов связи.

Стоит отметить, что наращивание спутниковой группировки не включает в себя дополнение ее спутниками телевизионного вещания, так как на данный момент потребность в данном ресурсе с избытком покрыта возможностями спутников КазСат-2 и КазСат-3.

Крупные спутниковые операторы во всем мире уверены, что будущее спутниковой связи связано с Ка-диапазоном и ими уже запущены или ведутся работы по запуску спутников Ка-диапазона (по данным Comsys, в 2015 г. 90 % ёмкости всех спутников будет в Ка-частотах, и их суммарная емкость приблизится к 1 Тбит/с). Большинство этих спутников нацелено на массовое предоставление услуг широкополосного доступа к сети Интернет, так как пропускная способность существующих спутников С- и Ku-диапазонов не может обеспечить быстро растущие потребности

современного цифрового мира по цене, которая могла бы конкурировать с наземными сетями.

Появление спутников Ка-диапазона в сочетании с многолучевой технологией обеспечивает дополнительный частотный ресурс, использование которого обходится значительно дешевле, чем использование аналогичной емкости Ku или C диапазонов. Примером этого является европейский рынок, где использование Ка диапазона обеспечивает существенно более высокую скорость передачи данных, доступную для конечного абонента, – до 20 Мбит/с – по привлекательной цене, при этом спутниковой емкости вполне достаточно для обслуживания сотен тысяч абонентов в перспективе.

Ка-диапазон имеет широкие перспективы в Казахстане и обладает рядом основных преимуществ в решении задач предоставления информации и услуг гражданам и организациям по средствам таких проектов как Электронное правительство, e-learning, е-минфин, е-статистика, е-лицензирование, е-медицина, е-акимат, е-аул.

Для эксплуатации спутникового ШПД необходима наземная инфраструктура, следовательно, открываются широкие возможности взаимодействия с такими операторами как АО «Казахтелеком», АО «Kaztranscom», АО «Kazsatnet» и другие, что не может не оказать положительного влияния на развитие телекоммуникационной отрасли, а, следовательно, и благосостояния граждан Республики Казахстан.

Благодаря географическому положению и имеющимся орбитальным позициям существует возможность совместного использования полезной нагрузки спутника, более того уже имеются предложения иностранных государств и компаний о сотрудничестве.

Таким образом, есть все предпосылки тому, что спутниковый ШПД станет популярным среди широких масс и все перечисленные преимущества Ка-диапазона позволят операторам клиентскую базу, не опасаясь дефицита спутникового ресурса. В вопросе вхождения Казахстана в 30 наиболее развитых стран мира, развитие информационно-коммуникационных технологии (ИКТ) которое невозможно без спутникового ШПД поднимет Казахстан во многих рейтингах от рейтингов-показателей компьютерной грамотности, участия населения в политической жизни республики, до показателей использования интернета в бизнесе.

В результате создания национальной двухсторонней спутниковой системы ШПД в Ка-диапазоне, космическая отрасль Казахстана станет одной из немногих в мире, использующих подобный перспективный космический аппарат. Проведение работ с аппаратом в сборочно-испытательном комплексе г. Астана положительно повлияет на имидж космической отрасли РК, позволит получить огромный опыт в разработке, интеграции, проведении испытаний над геостационарным спутником. Всё это даст большой толчок к дальнейшему развитию космической отрасли РК.

Список используемых источников

1. Argyrios Kyrgiazos, Barry Evans, Paul Thompson, P. Takis Mathiopoulos and Stylianos Papaharalabos. A terabit/second satellite system for European broadband access: a feasibility study // International Journal of Satellite Communications and Networking. Int. J. Satell. Commun. Network. 2014; 32:63–92 Published online 27 January 2014 in Wiley Online Library (wileyonlinelibrary.com). doi: 10.1002/sat.1067.

УДК 681.3.06

СРАВНЕНИЕ LABVIEW И SIMULINK ПРИ МОДЕЛИРОВАНИИ СИСТЕМ ЦИФРОВОЙ ОБРАБОТКИ СИГНАЛОВ

Д. Б. Касабаева[1], А. Б. Степанов[2]

[1]Евразийский национальный университет им. Л. Н. Гумилева (Астана)
[2]Санкт-Петербургский государственный университет телекоммуникаций им. проф. М. А. Бонч-Бруевича

Статья посвящена сравнению LabVIEW и Simulink, как части системы MATLAB, при выполнении моделирования систем цифровой обработки сигналов. Рассматриваются особенности при работе с этими пакетами, описываются их достоинства и недостатки. В качестве примера при моделировании рассматривается цифровой фильтр. Приводится Simulink-модель системы цифровой фильтрации и ее блок-схема, построенная в LabVIEW.

MATLAB, LabVIEW, Simulink, Simulink-модель, цифровой фильтр.

В настоящее время, при моделировании систем цифровой обработки сигналов широкое распространение получили такие пакеты как MATLAB и LabVIEW [1].

MATLAB – это специализированный математический пакет, предназначенный для выполнения моделирования систем в самых различных областях науки и техники. MATLAB берет свое название от Matrix Laboratory. Возможность выполнения всех вычислений путем преобразования матриц позволяет считать язык MATLAB языком «сверхвысокого» уровня. MATLAB состоит из трех основных частей: ядро MATLAB, подсистема блочного моделирования Simulink и специализированные пакеты расширения Toolbox. Simulink позволяет выполнять динамическое моделирование систем цифровой обработки сигналов. Для этого необходимо выполнить: построение Simulink-модели, настройку параметров отдельных блоков, образующих модель, и ее тестирование. При необходимости к персональному компьютеру могут быть подключены различные устройства, служащие источником сигнала или позволяющие его визуализировать. Загрузка сигнала в персональный компьютер может осуществляться через порт USB или через звуковую

карту. В этом случае MATLAB воспринимает их как виртуальные COM-порты и сигнал загружается в Workspace. Далее сигнал может быть загружен в Simulink-модель и обработан. Достоинством Simulink является возможность обработки в реальном времени сигналов, полученных или путем генерирования встроенными блоками, или загруженными через упомянутые порты. Еще одним достоинством Simulink является открытость кода, что позволяет пользователю использовать не только уже готовые блоки, хранящиеся в библиотеке Simulink, но также создавать свои. На основе Simulink-модели может быть получен код для реализации моделируемой системы на цифровых сигнальных процессорах [2, 3] или на программируемых логических интегральных схемах (ПЛИС).

На рисунке 1 показан пример построения Simulink-модели. Данная модель реализует систему цифровой фильтрации и содержит:

- два источника сигнала (Sine Wave);
- сумматор (Add);
- цифровой фильтр ФНЧ (Lowpass Filter);
- средства анализа последовательностей (Scope).

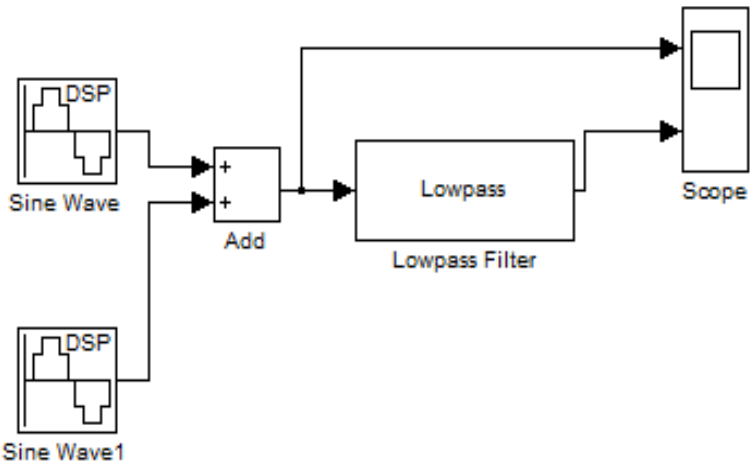


Рис. 1. Simulink-модель системы цифровой фильтрации

На рисунке 2 показаны результаты визуализации сигналов на входе и выходе цифрового фильтра.

LabVIEW (Laboratory Virtual Instrument Engineering Workbench) – это среда разработки лабораторных виртуальных приборов. LabVIEW является средой графического программирования [4, 5]. Программирование в LabVIEW выполняется на уровне построения блок-схем проектируемых систем. К достоинствам LabVIEW можно отнести простоту построения моделируемой системы за счет использования графического языка G, возможность подключения специализированных устройств для ввода и вывода сигналов, их обработки и отображения. К недостаткам относится закрытость кода, ограничивающая возможность создания пользовательских блоков.

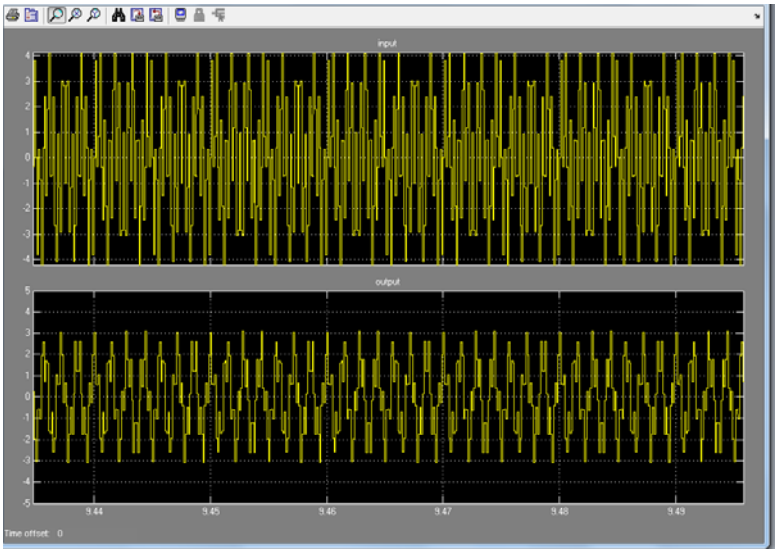


Рис. 2. Визуализация сигналов на входе и выходе цифрового фильтра

На рисунке 3 представлена блок-схема системы цифровой фильтрации, построенная в LabVIEW. Она содержит следующие блоки:

– два источника сигнала (Simulate Signal);
– сумматор (Add);
– цифровой фильтр (Filter);
– блок визуализации на входе и выходе цифрового фильтра (Waveform Graph).

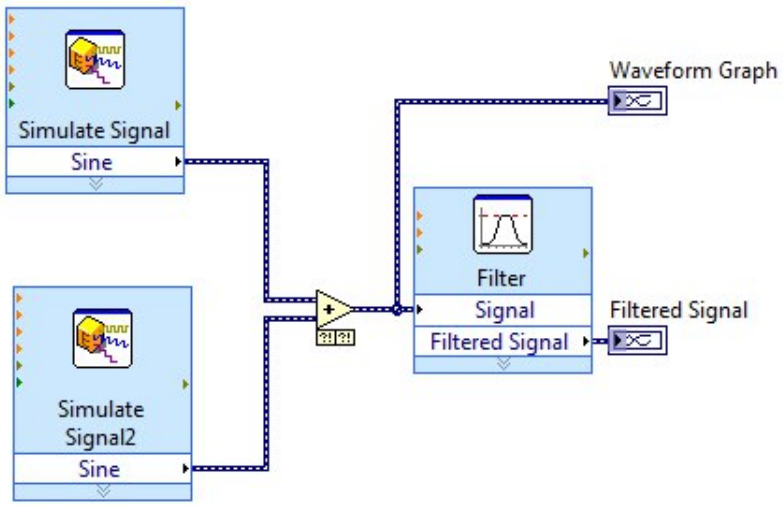


Рис. 3. Блок-схема системы цифровой фильтрации, построенная в LabVIEW

На рисунке 4 показана лицевая панель системы цифровой фильтрации.

Как следует из рисунков 1–4 подсистема блочного моделирования Simulink и LabVIEW имеют схожие принципы построения моделей (блок-схем)

систем цифровой обработки сигналов, а также аналогичные средства визуализации обработанных сигналов.

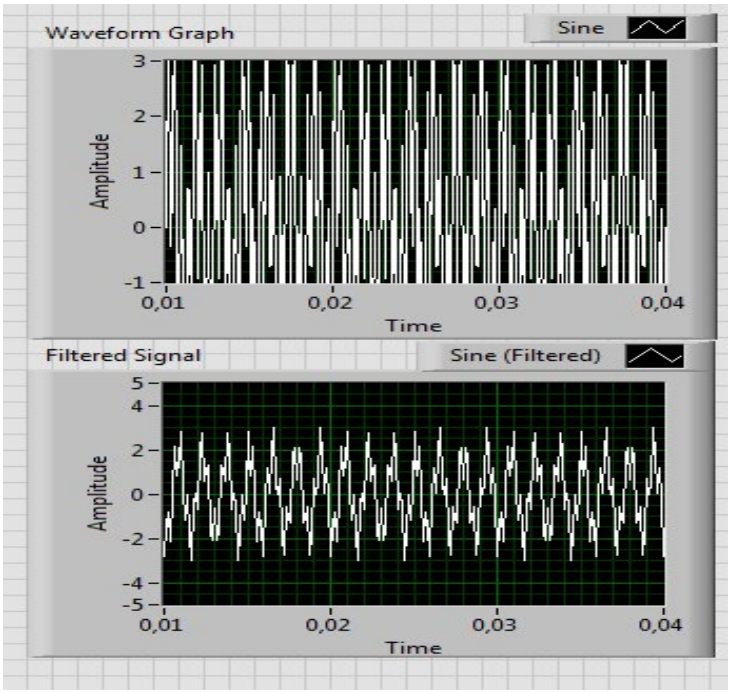


Рис. 4. Лицевая панель системы цифровой фильтрации

К достоинствам системы MATLAB и подсистемы Simulink можно отнести: возможность использования в качестве источников реальных сигналов оборудования, подключенного через порты компьютера; открытость кода, что позволяет использовать не только имеющиеся блоки, но и создаваемые пользователем.

Достоинствами LabVIEW является возможность подключения разнообразного профессионального оборудования, удобство работы с виртуальными приборами. В качестве недостатков можно отметить закрытость кода, что затрудняет расширение имеющего функционала.

В заключении отметим, что и система MATLAB, и LabVIEW являются признанными мировыми стандартами в моделировании систем цифровой обработки сигналов, имеют большие возможности. Эти пакеты имеют свою специфику и ориентацию, что делает их удобным инструментом при проектировании систем цифровой обработки сигналов.

Список используемых источников

1. Солонина А. И. Цифровая обработка сигналов. Моделирование в Simulink. СПб. : БХВ-Петербург, 2012. 432 с. ISBN 978-5-9775-0686-1.

2. Журавов Д. В., Степанов А. Б. Реализация процедуры вейвлет-сжатия на цифровом сигнальном процессоре // Юбилейная 70-я Всероссийская научно-техническая конференция, посвященная Дню радио : статья в сборнике трудов конференции, Санкт-Петербург, 21–29 апр. 2015 г. СПб. : СПбГЭТУ «ЛЭТИ», 2015. С. 86–87.

3. Журавов Д. В., Степанов А . Реализация алгоритмов цифровой обработки сигналов на основе непрерывного вейвлет-преобразования средствами MATLAB [Электронный ресурс] // Актуальные проблемы инфотелекоммуникаций в науке и образовании : материалы IV международной науч.-технической и науч.-методической конф., Санкт-Петербург, 03–04 марта 2015 г. СПб. : СПбГУТ, 2015. С. 99–103. URL: http://www.sut.ru/doci/nauka/4.apino.2015.sut.pdf (дата обращения 15.04.2016).

4. Трэвис Д., Кринг Д. LabVIEW для всех. М. : ДМК Пресс, 2011. 904 с. ISBN 978-5-94074-674-4.

5. Батоврин В. К., Бессонов А. С., Мошкин В. В., Папуловский В. Ф. LabVlEW : практикум по основам измерительных технологий : учеб. пособие для вузов. М. : ДМК Пресс, 2005. 208 с.

УДК 621.396.94

РАЗРАБОТКА МОБИЛЬНОЙ СИСТЕМЫ ИНФОРМАЦИОННОГО ОБЕСПЕЧЕНИЯ С ИСПОЛЬЗОВАНИЕМ КАНАЛОВ МЕТЕОРНОЙ СВЯЗИ

А. И. Качнов, А. В. Пенкин, А. В. Рыбаков

Научно-производственное предприятие «Авиационная и Морская Электроника»

Представлено решение задачи по созданию мобильной системы информационного обеспечения с использованием каналов метеорной связи, входящей в состав комплексной системы информационного обеспечения безопасности судоходства Северного морского пути. Рассмотрен вариант реализации мобильной (носимой) системы. Приведены результаты апробации технических решений.

метеорная радиосвязь, коротковолновая радиосвязь, телекоммуникации, система передачи данных.

Актуальность работы заключается во внедрении результатов в районах с условиями постоянно действующих ионосферных возмущений, характерных для приполярных широт, метеорная радиосвязь (МС) может стать хорошей альтернативой коротковолновой радиосвязи (КВ), а в районах со слаборазвитой телекоммуникационной инфраструктурой МС может стать основным средством связи. МС имеет следующие преимущества по сравнению с КВ радиосвязью:

– повышенная устойчивость радиосвязи при ионосферных возмущениях естественного и искусственного происхождения;

– повышенная помехозащищенность канала связи;

– отсутствие «зоны молчания» в пределах всей зоны обеспечения;

– простота построения системы передачи данных от удаленных необслуживаемых объектов;

– существенно более низкое энергопотребление;

– более высокий показатель эффективности функционирования системы по критерию эффективность/стоимость для труднодоступных районов и районов со слабо развитой инфраструктурой [1].

Система метеорной связи (макет) прошла заводские натурные испытания на трассе Санкт-Петербург – Киржач (рис. 1). Показала свою работоспособность.

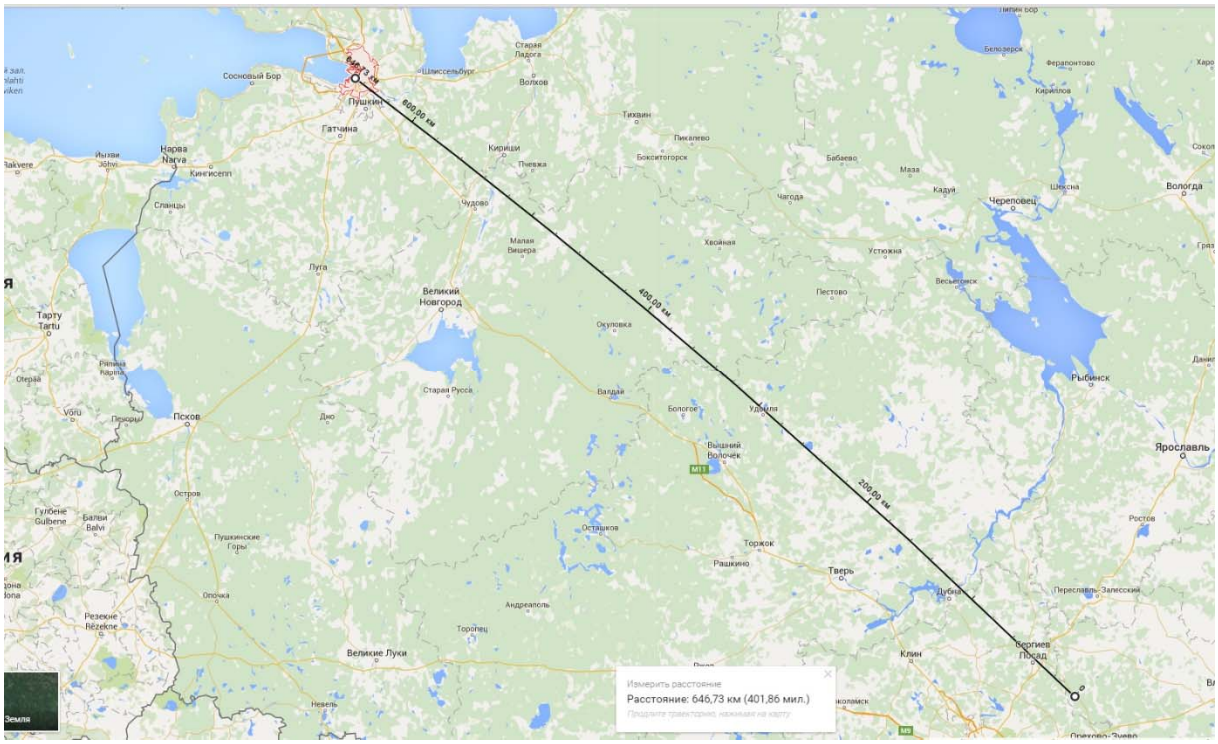


Рис. 1. Трасса испытаний Метеорной связи

Координаты: 30.27 *E*/59.89 *N*;

Координаты: 38.56 *E*/56.13 *N*.

Изначальной задачей для натурных испытаний было определение возможности передачи данных через случайные метеорные отражения без учёта метеорных потоков. Возможность эта подтвердилась. Вероятность образования 2–3 каналов передачи данных с размером окна 0,1–1 с в течение суток на максимально хорошо оборудованный комплект МС подтверждена. При наличии метеорных дождей, вероятность образования канала, а значит и количества передаваемых данных, существенно увеличивается. Так как испытания проходили в южных широтах, то 2–3 метеорита в сутки это очень хороший показатель, но, как известно, для приполярных широт показатель существенно больше [1].

Если необходимо увеличить количество окон передачи данных от базовой станции к мобильной станции, при создании базовой станции следует

рассчитывать на использовании более сложных антенн с большим усилением (например, применять параллельное включение нескольких антенн – т. н. «стекирование» и увеличение количества элементов в антенне), а также, увеличивать мощность в 5–10 раз [2].

На рисунке показан макет блока мобильной (носимой) станции мощностью 200 Вт (рис. 2). Планируемая мощность базовой станции 800 Вт.

Рис. 2. Макет блока мобильной станции

При создании мобильной станции необходимо учитывать, что сложные и громоздкие антенны неприменимы. Предлагается применять:

– для приёма и передачи «стекирование» нескольких антенн с небольшим количеством элементов;

– только для приёма в экстремально-простых вариантах можно применять вертикальные антенны, с пониманием, что вероятность образования канала есть, но она ничтожно мала [3].

В процессе натурных испытаний проекта использовалась модуляция с мгновенной скоростью в канале 1000 бит/с, обусловленная допустимой шириной канала 2,5 кГц. При использовании более широкой полосы можно достичь существенного увеличения мгновенной скорости передачи данных.

ТАБЛИЦА. Результаты натурных испытаний

День	1	2	3	4
Количество пакетов по дням	23	8	9	1
Количество бит по дням	1035	360	405	45

В таблице приведены результаты измерений по исследуемой трассе. Выбор оптимального варианта антенн для мобильной станции может быть определен только после проведения обширных дополнительных натурных испытаний. Пример декодирования сигнала на мощности 0,1 Вт изображен на рисунке (рис. 3).

Рис. 3. Пример декодирования сигнала на мощности 0,1 Вт

При создании базовой станции необходимо учитывать узость диаграмм направленности антенн, (особенно это касается антенн с большим усилением) и, при необходимости покрытия базовой станции нескольких зон покрытия, использовать несколько комплектов оборудования МС и антенн, направленных в нужную сторону [4, 5].

Результаты испытаний позволяют сделать заключение о правильности принятых технических решений и послужили основанием для выбора дальнейшего пути развития системы информационного обеспечения безопасности судоходства Северного морского пути с использованием каналов метеорной связи. Аналогов разработанной системе в отечественной продукции нет. Необходимо отметить тот факт, что применение разработки возможно и на судах гражданского флота РФ, что автоматически выводит разработку в коммерческую область с достаточно широким потенциалом применения [6].

Список используемых источников

1. Вишневский В. М., Ляхов А. И., Портной С. Л., Шахнович И. В. Широкополосные беспроводные сети передачи информации. М. : Техносфера, 2005. 597 с. ISBN 5-94836-049-0.

2. Подосенов С. А., Потапов А. А., Соколов А. А. Импульсная электродинамика широкополосных радиосистем и поля связанных структур. М. : Радиотехника, 2003. 720 с. ISBN 5-93108-058-9.

3. Бабков В. Ю., Фокин Г. А. Оценка вероятности успешного радиоприема в самоорганизующихся пакетных радиосетях на основе радиостанций с направленными антеннами // Научно-технические ведомости Санкт-Петербургского государственного

политехнического университета. Информатика. Телекоммуникации. Управление. 2009. Т. 4. № 82. С. 77–84.

4. Воробьев О. В., Рыбаков А. И. Архитектура радиопередающей системы в составе автоматизированного корабельного комплекса связи // В сборнике: Неделя науки СПбПУ материалы научного форума с международным участием. Институт физики, нанотехнологий и телекоммуникаций; отв. ред. В. Э. Гасумянц, Д. Д. Карпов. СПб. : СПбПУ, 2015. С. 40–42.

5. Фокин Г. А. Управление самоорганизующимися пакетными радиосетями на основе радиостанций с направленными антенными решетками : автореф. дис. … канд. техн. наук : 05.13.13 / Фокин Григорий Алексеевич. СПб., 2009. 17 с.

6. Воробьев О. В., Рыбаков А. И. Универсальный блок беспроводного взаимодействия с корабельной системой управления // В сборнике: Неделя науки СПбПУ материалы научного форума с международным участием. Институт физики, нанотехнологий и телекоммуникаций; отв. ред. В. Э. Гасумянц, Д. Д. Карпов. СПб. : СПбПУ, 2015. С. 43–45.

УДК 621.398

МОДЕЛЬ КАНАЛА ПЕРЕДАЧИ ДАННЫХ В СИСТЕМАХ МОБИЛЬНОЙ МЕДИЦИНЫ

Д. И. Кирик, А. Г. Малышев

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

Рассматриваются проблемы стандартизации в системах мобильной медицины. Приводятся наиболее значимые и используемые стандарты.

ZigBee, протокол, мобильная медицина, телемедицина.

Проблема стандартизации процессов в системах мобильной медицины становится одной из самых актуальных при построении телемедицинских сетей. В настоящее время ей уделяется все больше внимания развитием телемедицинских технологий.

Информационные стандарты, которые применяются в телемедицине можно разделить на несколько видов:

− классификаторы и справочники;

− стандарты передачи медицинских записей и изображений;

− стандарты формирования электронных медицинских записей и документов.

В телемедицинских системах каждый из этих видов стандартов имеет особое значение на этапах оказания телемедицинских услуг. В нашей работе мы рассмотрим только стандарты передачи медицинских данных.

При реализации телемедицинских услуг необходимо передавать консультанту и обратно пользователю различные медицинские данные по каналам связи. Понятно, что такая передача должна осуществляться по определенным правилам и форматам, чтобы они воспринимались любым участником телемедицинской консультации. Согласно требованиям, к перечню документов, которые используются в телемедицинских консультациях, к ним относятся медицинские записи, медицинские изображения и графический материал. Таким образом, передаются учетные медицинские формы в виде запроса на телемедицинскую консультацию, карты амбулаторного больного, эпикризы и выписки из историй болезни и др. Медицинские изображения включают различные виды изображений от ЭКГ и ЭЭГ до рентгеновских изображений, КТ-изображений, УЗ-изображений, МРТ-изображений и др. Современные информационные технологии позволяют в настоящее время оперировать с четырьмя основными типами изображений – двухмерными (планарными), послойными, трехмерными (3D-рендеринг) и четырехмерными (4D-рендеринг). Получают распространение и новейшие подходы к визуализации – виртуальная эндоскопия, мультипланарная реконструкция органов, 3D-виртуальная энеретическая эхоангиография, рентгеноостеоденситометрия, радиотермография, электроимпедансная томография, цифровая апостериорная алгоритмическая обработка рентгенограмм и некоторые другие. Ниже приводится список различных типов медицинских изображений, применяемых в диагностических системах:

– планарные изображения (рентгенография, сцинтиграфия и др.);

– послойные изображения (линейная и компьютерная томография, МРТ, эмиссионная томография, ПЭТ и др.);

– трехмерные изображения (3D-rendering): на основе спиральной КТ, УЗИ и др.;

– четырехмерные изображения (4D-rendering)

– трехмерные изображения в реальном времени;

– энергетические изображения (энергетический допплер, спиральная КТ с выделением изомерных по напряжениям потоков крови, сосудистых стенок и др.);

– параметрические эквиваленты диагностических изображений (МР-спектрометрия, остеоденситометрия и др.) [1].

Рассмотрим некоторые системы, стандарты и протоколы беспроводных сетей.

В настоящее время широко используются системы PACS (*Picture Archiving and Communication Systems*), установленные в настоящее время в больницах и позволяющие решить некоторые задачи, связанные с управлением медицинскими данными [2]. Однако у них есть много ограничений:

– часто они не связаны с радиологической информационной системой

(RIS – *Radiological Information System*), которая ведет медицинскую документацию;

– часто они являются собственными разработками компаний по обработке медицинских изображений, и не существует открытых стандартов для взаимодействия с другими PACS;

– обычно они имеют дело с медицинскими данными только внутри одного лечебного учреждения (одна больница или, в лучшем случае, объединение больниц) и не используются в национальном или международном масштабе.

Чтобы сделать более удобным хранение и передачу данных, несколькими международными организациями и промышленными компаниями был принят стандарт DICOM (*Digital Image and Communication in Medicine*) [2]. Стандарт DICOM реализован в современном оборудовании для получения изображений и медицинском оборудовании, что облегчает обмен данными между устройствами для визуализации изображений, пультами постобработки и системами архивирования. Однако этот стандарт не охватывает все свойства RIS (*Radiological Information System*), касающиеся управления данными и доступа к данным, и не описывает стратегию архивирования, чем занимается PACS. В то же время часть диагностической техники снабжена различными модификациями DICOM, что часто затрудняет ее интеграцию в медицинские информационные системы. Стандарт DICOM позволяет решить задачи интеграции на основе открытой архитектуры. DICOM позволяет организовать не только пересылку данных по сети, но и автоматическую обработку данных. Он значительно уменьшает время подготовки и проведения исследований, управления изображениями и сопутствующей информацией. Для достижения наивысшей эффективности, он поддерживает все стадии диагностики, снижая себестоимость за счет:

− сокращения времени обслуживания;

− отказа от пленок и затрат на их хранение;

− резкого сокращения потерь изображений и результатов.

На основе стандарта DICOM и типовых сетевых решений, как один из вариантов, рекомендуется 3-х уровневое интеграционное решение.

Для предоставления возможности обмена информацией между различными системами чрезвычайно важным было создание стандартного протокола обмена для компьютеризации электрокардиограммы (ЭКГ). Инициативная группа начала его разработку в 1978 г. Основной целью создания этого стандарта является спецификация формата данных и средств передачи ЭКГ и заключений по прямой линии соединения от какого-либо источника записи компьютерной ЭКГ центральной системе управления ЭКГ. Этот протокол также должен поддерживать стандартизованный обмен цифровыми

ЭКС и результатами измерений между различными компьютерными системами. В результате под эгидой технического комитета ТС 251 Европейского Комитета по Стандартизации (CEN) был разработан документ ENV1064 [2].

ENV1064 устанавливает единый протокол SCP передачи ЭКГ данных как между цифровым электрокардиографом и компьютеризированной системой управления, так и между компьютерными системами различных производителей [2]. Стандарт SCP-ECG не накладывает ограничений на физический уровень протокола, а лишь определяет минимально необходимые требования. Он же регламентирует некоторые соглашения по передаче других данных: сведений о пациенте, результатов анализа ЭКГ, условиях проведения измерений и т. д.

В рамках протокола SCP содержание и формат ЭКГ-сигнала и результатов измерений, полученных от электрокардиографов различных марок не обязательно должны быть идентичны. В результате определение удобства использования той или иной системы регистрации электрокардиостимулятора (ЭКС) для какого-либо приложения остается за пользователем. Следующие возможные варианты использования записей ЭКС требуют особого внимания:

− сравнение серий ЭКС и их интерпретаций;

− форматы диаграмм ЭКС;

− двунаправленная передача.

Данный стандарт поддерживает традиционную запись электрокардиограммы, т. е. так называемые стандартные 12 отведений и вектор-кардиографию. Компьютерная обработка ЭКС может быть разделена на 3 стадии:

1. Получение, кодирование, передача и хранение данных.

2. Распознавание образцов и выявление особенностей, т. е. измерение ЭКС.

3. Диагностическая классификация.

На каждой из этих стадий существуют наиболее важные моменты для стандартизации и проверки соответствия качества данных. Рамки стандарта ограничены первой из этих трех стадий.

ZigBee – беспроводная спецификация с низким потреблением на базе стандарта IEEE 802.15.4-2003. Она обеспечивает ячеистую беспроводную сеть с малым потреблением и предназначена для таких приложений как интеллектуальные счетчики, системы домашней автоматики и дистанционного управления [3]. К сожалению, сложность и высокая потребляемая мощность ZigBee не позволяют использовать эту технологию в необслуживаемых устройствах, которые должны работать в течение длительного времени от батарейного питания. Каналы ZigBee разделены 5-МГц промежутком, что несколько ограничивает спектр. В ZigBee не используется технология перескока частоты, поэтому требуется тщательное планирование сети в процессе развертывания, чтобы гарантировать отсутствие поблизости сигналов помех.

Технология Radio Frequency for Consumer Electronics (RF4CE) основана на ZigBee и стандартизирована в 2009 г. четырьмя компаниями-производителями потребительской электроники: Sony, Philips, Panasonic и Samsung. RF4CE поддерживают также два поставщика полупроводников: Texas Instruments и Freescale Semiconductor [4]. Технология RF4CE предназначена для дистанционного управления потребительскими устройствами, например, телеприставками. Целью разработки RF4CE являлась попытка преодоления общих проблем ИК-управления: функциональная совместимость устройств, необходимость работы в прямой видимости и ограниченные функции управления.

Вопросы энергоэффективности актуальны для построения систем мобильной медицины, обеспечивающих сбор, хранение и обработку низкоскоростных данных в условиях ограничения энергии аккумуляторных батарей. Поэтому целесообразно решение задачи оптимизации параметров передачи сигналов в беспроводных системах для снижения энергопотребления.

Список используемых источников

1. Блажис А. К., Дюк В. А. Телемедицина : учебн. пособие. СПб. : СпецЛит, 2001. 143 с. ISBN 5-299-00084-7.

2. Кобринский Б. А. Автоматизированные регистры медицинского назначения: теория и практика применения. М. : Менеджер здравоохранения, 2011. 148 с. ISBN 978-5-903834-19-8.

3. Балонин Н. А., Сергеев М. Б. Беспроводные персональные сети на основе ZigBee: учеб. пособие. СПбГУАП. СПб., 2012. 68 с.

4. Симанков В. С., Халафян А. А., Системный анализ и современные информационные технологии в медицинских системах поддержки принятия решений. М. : Бином-Пресс, 2009. 362 с.

УДК 654.191

РАЗРАБОТКА ПЕРСПЕКТИВНОГО РАДИОПЕРЕДАЮЩЕГО УСТРОЙСТВА КВ ДИАПАЗОНА ВОЕННОГО НАЗНАЧЕНИЯ

Н. В. Кудряшов, О. А. Михалев, М. И. Петренко

Военная академия связи им. Маршала Советского Союза С. М. Буденного

В настоящее время в России большая часть радиопередающих устройств коротковолновой связи имеет ряд недостатков: низкий коэффициент полезного действия, построены на элементной базе старого парка, не способны вещать в цифровых форматах. Построение радиопередающего устройства по методу Канна способного вещать как в аналоговых видах модуляции, так и в цифровом стандарте радиовещания DRM с использованием усилителя класса D и современной отечественной элементной базы

позволит повысить энергоэффективность передатчика, качество принимаемых программ, расширить зону уверенного приема.

усилитель, Digital Radio Mondiale, коэффициент полезного действия, модуляция.

В начале 90-х годов общегосударственная сеть коротковолновой (КВ) связи в России снизила темпы развития и к настоящему периоду почти полностью прекратила своё существование. Создание сети КВ связи даст возможность:

– устойчивой связи для государственных нужд со всеми субъектами Российской Федерации;

– предоставит широкий спектр телекоммуникационных услуг: открытая и закрытая цифровая телефония, факсимильная связь, передача данных;

– организует резервные каналы доставки программ государственного радиовещания, потоков документальной связи, особенно в условиях чрезвычайных ситуаций.

Кроме того, важно понимать, что для Крайнего Севера России и его арктического побережья, коротковолновая радиосвязь часто представляет собой единственный способ связи с остальными субъектами Российской Федерации.

В настоящее время в России большая часть радиопередающих устройств (РПдУ) КВ связи имеет ряд недостатков:

1 Низкий коэффициент полезного действия (КПД)

КПД РПдУ на прямую зависит от используемого в нем класса усилителя мощности. Наиболее распространенные применяемые усилители мощности классов – *A*, *AB*, *B*, *C*. Теоретический КПД таких усилителей порядка 50–75 %, но на практике он существенно ниже и не превышает 40 %. Усилители класса *A* дают очень «чистый» сигнал, но обладают низкой эффективностью. Эффективность усилителя класса *B* почти в два раза выше эффективности усилителя класса *A*. Однако, искажения в выходном сигнале очень высоки. Усилители класса *C* также, как и *B*, имеют высокую эффективность, но с увеличением КПД резко увеличиваются искажения. Этих недостатков лишены усилители класса *D*. В целом, принцип работы усилителя класса *D* очень напоминает принцип работы импульсного блока питания, но в отличие от него, на выходе, за счет широтно-импульсной модуляции, формируется не постоянное напряжение, а переменное, по форме соответствующее входному сигналу. Теоретически, КПД подобных усилителей должен достигать 100 %, но сопротивление канала транзистора присутствует в небольшой величине. В зависимости от сопротивления нагрузки, КПД усилителей этого типа может достигать 90–95 %. Разумеется, при такой эффективности нагрев выходных транзисторов практически отсут-

ствует, что позволяет создавать небольшие и экономичные усилители. Коэффициент гармонических искажений при грамотном построении выходного фильтра можно довести до 0,01 %, что является прекрасным результатом [1].

Существует множество различных инженерных решений усилителей классов *A*, *AB* и *B*, *C*. Во всех, даже в самых эффективных, линейных выходных каскадах рассеивание мощности больше, чем в усилителях класса *D* (рис. 1). Это свойство усилителей класса *D* обеспечивает им преимущество в различных системах, так как малое рассеивание мощности означает меньший нагрев схемы, снижает стоимость и уменьшает массогабаритные показатели оборудования.

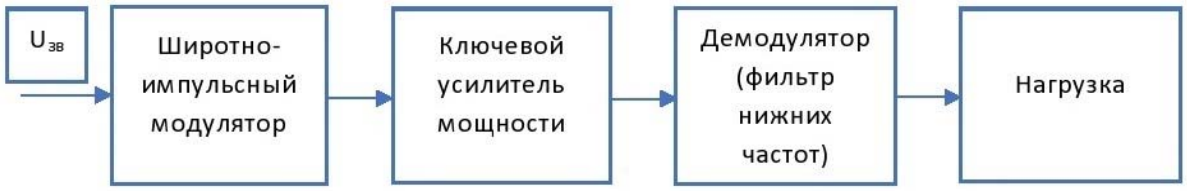


Рис. 1. Структурная схема однотактного усилителя класса *D*

2 Построены на элементной базе старого парка

Большинство эксплуатируемых в настоящее время РПдУ работают с усилителями мощности, построенных на электронных лампах. Почти во всех устройствах, в которых применяются вакуумные лампы, могут работать транзисторы.

По сравнению с электронными лампами у полупроводниковых приборов имеются существенные достоинства:

– малый вес и малые размеры;

– отсутствие затраты энергии на накал;

– большой срок службы (до десятков тысяч часов);

– большая механическая прочность (стойкость к тряске, ударам и другим видам механических перегрузок);

– различные устройства (выпрямители, усилители, генераторы) с полупроводниковыми приборами имеют высокий КПД, так как потери энергии в самих приборах незначительны;

– маломощные устройства с транзисторами могут работать при очень низких питающих напряжениях.

В настоящее время разработаны генераторные транзисторы мощностью – до 250…1000 Вт на частотах до 150…1000 МГц.

3 Не способны вещать в цифровых форматах

Особый интерес представляет использование цифровых радиосигналов, позволяющих улучшить помехоустойчивость систем радиосвязи. Однако возможности применения цифровых методов передачи в КВ диапазоне ограничены из-за многолучевости распространения радиоволн и существенного ослабления сигналов на трассах радиосвязи в частотном диапазоне 1,5–30 МГц.

Digital Radio Mondiale (DRM) – это многофункциональная система цифрового радиовещания, разработанная для работы в диапазонах, используемых в настоящее время для вещания с амплитудной модуляцией, в частности на коротких волнах. По сравнению с амплитудной модуляцией DRM позволяет передавать больше каналов с высоким качеством, используя различные кодеки MPEG-4. Система передачи данных в формате DRM работает по принципу передачи данных на многих несущих. В то время, как в аналоговой технологии используется только одна несущая с передачей одинаковой информации в обеих боковых полосах, то в «цифре» закодированный сигнал распределяется почти по 200 несущих с различными видами цифровой модуляции. Информация, прежде чем дойти до радиослушателя, проходит сложный путь, сохраняя качество звука путём цифрового кодирования [2].

В результате возникающих трудностей при построении и эксплуатации систем передачи цифровой информации в КВ диапазоне, связанных со сложной помеховой обстановкой, большой загруженностью КВ диапазона, недоступностью абонента для сеанса связи в определенное время, в существующих системах КВ радиосвязи удается поддерживать среднесуточную скорость передачи данных не более 3200 бит/с с вероятностью ошибки $p_б = 10^{-2}$. В основном же скорость передачи данных составляет 200–2400 бит/, а зачастую связь вообще пропадает. Анализ современных требований, предъявляемых к КВ радиосистемам, показал, что вероятность ошибки на бит должна составлять $p_{тр} = 10^{-4}$.

Для обеспечения требуемой вероятности ошибки необходимо использовать модуляции, наиболее подходящие для коротковолновой связи. Анализ международных стандартов и исследований показал, что таковыми для КВ радиосвязи считаются сигналы с фазовой модуляцией (КИМа-ФМ), квадратурной фазовой модуляцией (КИМа-КФМ), квадратурной амплитудной модуляцией (КИМа-КАМ) с основанием кода а = 2, 4, 8, 16, 32 и 64, а также перспективный комбинированный метод модуляции КИМа-КАМ4/ЧМа/4 [3].

Использование перспективного комбинированного метода модуляции КИМа-КАМ4/ЧМа/4 в цифровом стандарте радиовещания DRM позволит

повысить устойчивость сигнала к эффектам затухания, интерференции сигнала, а также их эффективность в условиях сильных помех, которым подвержено обычное вещание.

Так как большинство эксплуатируемых РПдУ работают в аналоговых режимах вещания необходимо обеспечить возможность работы перспективных РПдУ не только в цифровых форматах вещания, но и аналоговых.

Необходимо выбрать схему построения РПдУ, позволяющую осуществлять работу в аналоговых и цифровых режимах вещания без изменения схемотехнической структуры построения, основных режимов работы и без перестройки каскадов передатчика (рис. 2).

Для построения передатчика, работающего в аналоговых и цифровых режимах вещания выбрана система модуляции по методу Верзунова (Канна), в котором реализуется раздельное усиление высокочастотной составляющей сигнала и сигнала звуковой частоты [4].

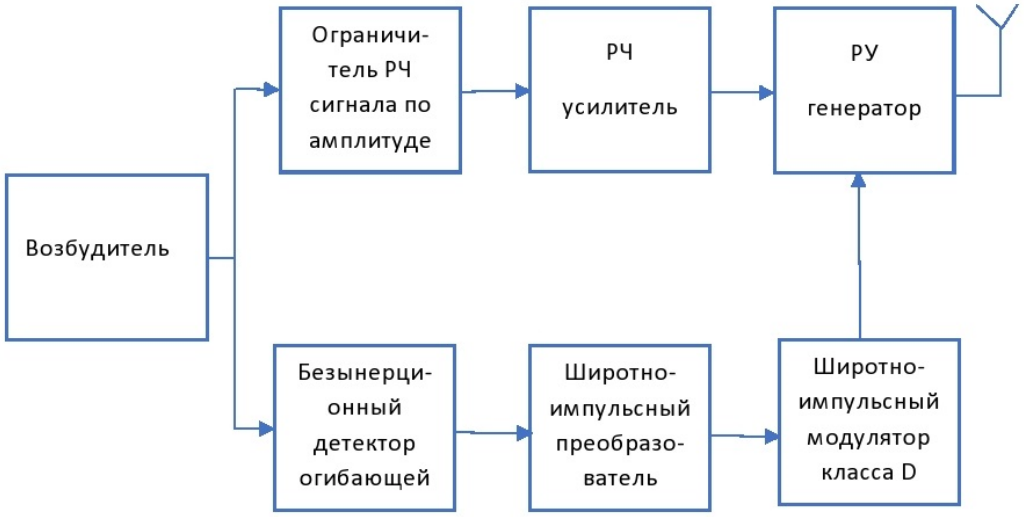


Рис. 2. Упрощенная структурная схема РПдУ,
позволяющего осуществлять вещание в аналоговых и цифровых режимах

Построение РПдУ по методу Канна способного вещать как в аналоговых видах модуляции, так и в цифровом стандарте радиовещания DRM с использованием усилителя класса *D* и современной отечественной элементной базы позволит повысить энергоэффективность передатчика, качество принимаемых программ, расширить зону уверенного приема.

Список используемых источников

1. Артым А. Д. Усилители класса D и ключевые генераторы в радиосвязи и вещании. М. : Связь, 1980. 232 с.

2. Оптимизация параметров и характеристик дополнительного оборудования и аппаратуры преобразования сигналов передатчика с целью обеспечения требуемого качества передаваемого цифрового сигнала, предусмотренного стандартом DRM. Создание обобщенной методики перевода передатчиков ДВ, СВ, КВ диапазона, построенных

по современным технологиям, в совместный режим передачи аналоговых и цифровых сигналов: отчет по НИР / Николаев В. В. СПб. : ФГУП НПЦРРТ «ДАЙМОНД», 2007. 37 с.

3. Котенко О. О. Повышение достоверности передачи информации в радиолиниях коротковолновой радиосвязи на основе применения эффективных сигнально-кодовых конструкций: автореф. дис. … канд. техн. наук : 05.12.13 / Котенко Олег Олегович. СПб., 2013. 16 с.

4. Разработка концепции внедрения DRM радиовещания в Российской Федерации: отчет по НИР / Николаев В. В. СПб. : ФГУП НПЦРРТ «ДАЙМОНД», 2006. 82 с.

УДК 004.732

ИССЛЕДОВАНИЕ СТАНДАРТНЫХ МЕХАНИЗМОВ ПРОВЕДЕНИЯ ИЗМЕРЕНИЙ WI-FI-СТАНЦИЯМИ С ЦЕЛЬЮ ВЫБОРА ТОЧКИ ДОСТУПА ДЛЯ ПОДКЛЮЧЕНИЯ

В. А. Лаврухин, А. С. Лежепёков

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

В сетях Wi-Fi выбор абонентской станцией сети для подключения или точки доступа внутри такой сети не регламентирован стандартом IEEE 802.11. Поэтому решение о том, к какой сети подключиться, ложится на плечи конечного пользователя Wi-Fi-устройства, то есть абонента. И хотя каждый производитель устройств со встроенным Wi-Fi вправе помочь пользователю выбрать сеть, основываясь на любых доступных абонентской станции измерениях, большинство компаний предлагают пользователям скромный набор критериев выбора сети. Во-первых, это уровень сигнала, оцениваемый графически по числу «черточек» на значке Wi-Fi. Во-вторых, это название сети. И, в-третьих, это флаг, показывающий защищена сеть или нет. Все указанные параметры не позволяют пользователю эффективно выбрать сеть в современных условиях.

В данной работе экспериментально доказана неэффективность существующих методов автоматического.

Wi-Fi, станция, точка доступа, фрейм, измерения.

Wi-Fi (*Wireless-Fidelity*) – широко распространенный в мире стандарт на оборудование Wireless LAN, разработанный консорциумом Wi-Fi Alliance в 1991 г.

Простейшая сеть беспроводного доступа Wi-Fi состоит из ведущего устройства, вещающего общедоступную информацию для подключения (*Beacon-frame*), и ведомого устройства, которое сравнивает полученные общедоступные Beacon-frame и, на основе сконфигурированных производителем критериев, сортирует для пользователя список доступных сетей по степени релевантности заданным критериям (рис. 1).

Качество связи и ёмкость беспроводной сети обусловлена физическими свойствами среды, в которой она развёрнута. Таким образом, нелицензируемый диапазон вещания 2,4 ГГц, используемый технологией Wi-Fi, разделен на 12 пересекающихся каналов. Радиовещание на пересекающихся частотных каналах является таким же частным случаем электромагнитной помехи, как и замирания, джиттер, многолучёвость, негативно влияющие на качественные параметры сети (мощность сигнала, скорость обмена данными, пропускная способность, количество битовых ошибок – параметры качества предоставляемых услуг) беспроводной передачи данных [1, 2, 3].

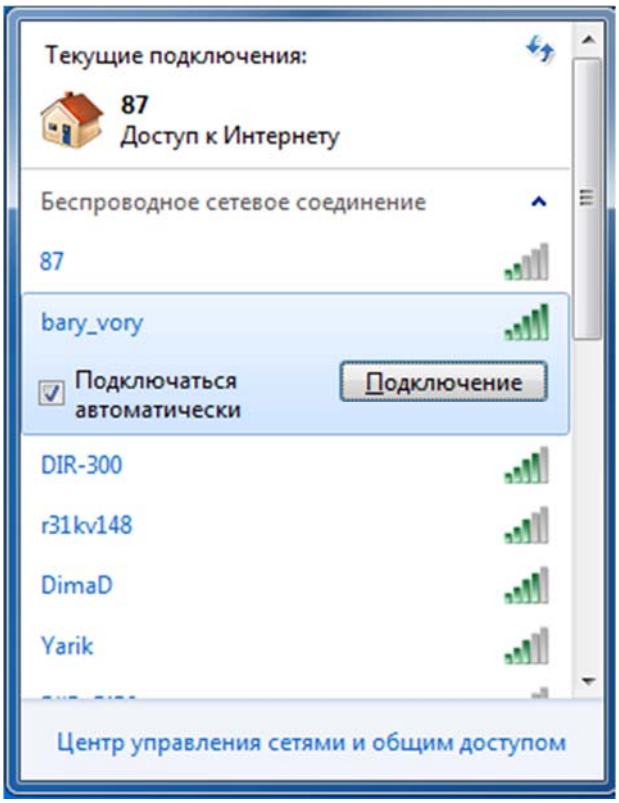


Рис. 1. Пример списка доступных Wi-Fi сетей

В рамках данной статьи разделим требования к оптимальной точке доступа (ТД) на «практические» и «теоретические». Теоретические требования устойчивой Wi-Fi сети четко не регламентированы стандартом, следовательно, каждый производитель клиентского программного обеспечения определяет оптимальную точку доступа самостоятельно. В общем случае, опираясь исключительно на значения RSSI (*Received Signal Strength Indicator*). Практически же точка доступа является оптимальной, если радиоканал от ведущего до ведомого устройства имеет минимальную электромагнитную помеху, достаточный уровень принимаемого сигнала RSSI и обеспечивает скорость передачи данных, удовлетворяющую потребностям клиента. Таким образом, теоретически оптимальная точка доступа, имеющая прием-

лемый уровень сигнала RSSI, зачастую не удовлетворяет требованиям клиента как по физическим критериям, влияющим на параметры качества предоставляемых услуг, так и аппаратным, имеющим ограничение по максимальному количеству абонентов сети.

Как итог, RSSI – исключительный параметр, используемый производителями программных продуктов для сортировки имеющихся Wi-Fi точек доступа в релевантном порядке, начиная с наибольшего и заканчивая наименьшим значением RSSI (дБ). Проблема заключается в недостатке этих данных для оценки качества сети, в том числе физических свойств радиоканала, и отсутствии исчерпывающей спецификации для четкого определения этого параметра. На сегодняшний день каждый производитель чипов калибрует его величину, исходя из собственных интересов. На рисунке 2 изображен пример инспектирования уровня RSSI двух точек доступа на одной мощности и разных частотных каналах. Пунктирной линией отмечен момент аутентификации UE (*User Equipment*) miPad. Целью данной работы являлось установление критериев, являющихся основой для автоматического выбора сети, и подтверждение исключительного влияния RSSI на выбор оптимальной ТД.

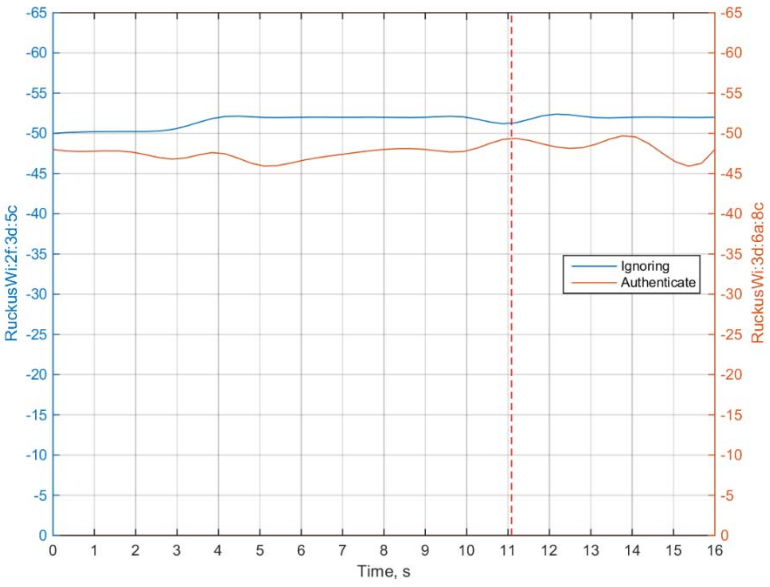


Рис. 2. Аутентификация

В данной работе на исследуемую тему было воспроизведено 940 экспериментов. Методика проведения испытаний включала в себя: запуск параллельного сканирования прохождения фреймов Wi-Fi ТД на двух частотных каналах (включая отслеживание RSSI), вещающих единым SSID (*Service Set Identifier*). UE очищался от сохраненных в памяти Wi-Fi сетей, перезагружался, и подключался к ТД в режиме автоматического выбора.

Испытательный стенд состоял из двух точек доступа Ruckus и одного UE, равноудалённых друг от друга на одинаковое расстояние (рис. 3).

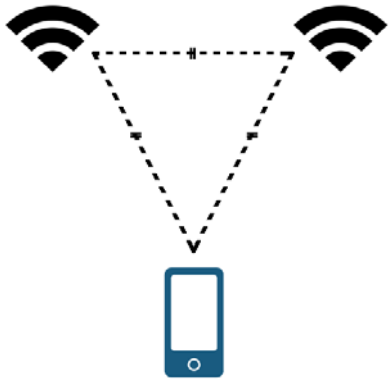


Рис. 3. Испытательный стенд

Измерения инспектировались ПО CommView for Wi-Fi с использованием Wi-Fi адаптера Tp-Link TL-WDN3200. Цикл экспериментов был разделен на 13 этапов:

1. RuckusWi:2f:3d:5c и RuckusWi:3d:6a:8c вещают на 36 и 52 частотном канале соответственно, нагрузка отсутствует, максимальный уровень мощности. UE – iPhone 5C.

2. RuckusWi:2f:3d:5c и RuckusWi:3d:6a:8c вещают на 36 и 48 частотном канале соответственно, нагрузка отсутствует, максимальный уровень мощности. UE – miPad.

3. RuckusWi:2f:3d:5c и RuckusWi:3d:6a:8c вещают на 48 и 36 частотном канале соответственно, нагрузка отсутствует, максимальный уровень мощности. UE – miPad.

4. RuckusWi:2f:3d:5c и RuckusWi:3d:6a:8c вещают на 48 и 36 частотном канале соответственно, нагрузка отсутствует, минимальный уровень мощности. UE – miPad.

5. RuckusWi:2f:3d:5c и RuckusWi:3d:6a:8c вещают на 36 и 48 частотном канале соответственно, нагрузка отсутствует, минимальный уровень мощности. UE – miPad.

6. RuckusWi:2f:3d:5c и RuckusWi:3d:6a:8c вещают на 48 и 36 частотном канале соответственно, нагрузка отсутствует, 1 дБ и 10 дБ уровень мощности соответственно. UE – iPhone 5C.

7. RuckusWi:2f:3d:5c и RuckusWi:3d:6a:8c вещают на 36 и 48 частотном канале соответственно, нагрузка отсутствует, 1 дБ и 10 дБ уровень мощности соответственно. UE – iPhone 5C.

8. RuckusWi:2f:3d:5c и RuckusWi:3d:6a:8c вещают на 36 и 48 частотном канале соответственно, нагрузка отсутствует, 1 дБ и 10 дБ уровень мощности соответственно. UE – miPad.

9. RuckusWi:2f:3d:5c и RuckusWi:3d:6a:8c вещают на 48 и 36 частотном канале соответственно, нагрузка отсутствует, 1 дБ и 10 дБ уровень мощности соответственно. UE – miPad.

10. RuckusWi:2f:3d:5c и RuckusWi:3d:6a:8c вещают на 48 и 36 частотном канале соответственно, у первой ТД реализована нагрузка, минимальный уровень мощности. UE – miPad.

11. RuckusWi:2f:3d:5c и RuckusWi:3d:6a:8c вещают на 48 и 36 частотном канале соответственно, у второй ТД реализована нагрузка, минимальный уровень мощности. UE – miPad.

12. RuckusWi:2f:3d:5c и RuckusWi:3d:6a:8c вещают на 36 и 48 частотном канале соответственно, у второй ТД реализована нагрузка, минимальный уровень мощности. UE – miPad.

13. RuckusWi:2f:3d:5c и RuckusWi:3d:6a:8c вещают на 36 и 48 частотном канале соответственно, у первой ТД реализована нагрузка, минимальный уровень мощности. UE – miPad.

Результаты экспериментов отражают исключительную зависимость выбора точки доступа от уровня RSSI, определяемым UE. С учётом изложенной ранее информации, существующий автоматический выбор точки доступа, предлагаемый производителями ПО, не обеспечивает нахождение оптимальной ТД. Дальнейшая работа будет направлена в сторону изучения влияния современных параметров стандарта 802.11k на выбор оптимальной ТД, оптимизацию имеющегося алгоритма и, как следствие, предложения по актуализации этой области.

Список используемых источников

1. Лежепёков А. С. Проектирование высоконагруженной беспроводной локальной сети Wi-Fi [Электронный ресурс] // 68-я региональная научно-техническая конференция студентов, аспирантов и молодых ученых «Студенческая весна – 2014» : материалы конференции. СПб. : СПбГУТ, 2014. С. 17–21. URL: https://sut.ru/doci/nauka/ 68sntksut.pdf (дата обращения 28.04.2016).

2. Lavrukhin V., Simonina O., Volodin E. An experemental study of the key QoS parameters in public Wi-Fi networks // 6th international congress on ultra modern telecommunications and control systems and workshops (ICUMT), 2015, pp 198–203.

3. Лаврухин В. А. Оценка времени установления соединения в сетях Wi-Fi // Научно-технические ведомости Санкт-Петербургского государственного политехнического университета, 2007. № 52-2. С. 45–48.

Статья представлена доктором технических наук, профессором М. А. Сиверсом.

УДК 621.396.949

О РЕЗУЛЬТАТАХ ЧИСЛЕННОГО МОДЕЛИРОВАНИЯ АНТЕННЫ-РАДИОУДЛИНИТЕЛЯ

А. Н. Ликонцев[1], Д. Н. Ликонцев[2], А. Ш. Шахобиддинов[2]

[1]Санкт-Петербургский государственный университет телекоммуникаций им. проф. М. А. Бонч-Бруевича
[2]Ташкентского университета информационных технологий

В статье приводятся результаты численного моделирования характеристик направленности и согласования четырехэлементной антенны «волновой канал». Также

приведены результаты моделирования антенны в виде антенной решетки из двух антенн «волновой канал», соединенных поочередно в плоскостях E и H. Такая антенна может быть использована в качестве радиоудлинителя мобильной радиосвязи и установлена в местах неуверенного приема.

радиоудлинитель, антенна, мобильная радиосвязь, неуверенный прием.

Известно, что в городской и сильно пересеченной местности наблюдаются деполяризация и многолучевое распространение волн.

Экспериментально установлено, что в городе за счет интерференции переотраженных волн, минимумы напряженности поля располагаются на расстоянии $r = (0{,}5\ldots1{,}0)\lambda$ (λ – длина волны) в зависимости от характера городской застройки [1, 2].

Препятствия на трассе распространения радиоволн приводят к образованиям радиотеневых зон.

При решении задач организации мобильной связи в радиотеневых зонах можно прибегнуть к использованию антенн-радиоудлинителей. В качестве радиоудлинителя мобильной связи можно использовать антенну типа «волновой канал».

Расчет оптимальных размеров антенны с точки зрения получения входного сопротивления $R_{вх} = 50$ Ом и максимального значения коэффициента направленного действия затруднителен, поскольку даже небольшое изменение в одном из размеров антенны приводит к значительным изменениям входного сопротивления антенны за счет наведенных сопротивлений в ее вибраторах [3].

Результаты расчета характеристик направленности радиоудлинителя из одной четырехэлементной антенны «волновой канал» при разных углах поворота полотна антенны χ вокруг его оси представлены в виде значений коэффициента усиления G, коэффициента стоячей волны (КСВ), ширины главного лепестка антенны по половинной мощности в вертикальной плоскости $2\theta_{0,5верт}$, в горизонтальной плоскости $2\theta_{0,5гориз}$, коэффициента защитного действия (КЗД) при разных углах χ и приведены в таблицах 1–3.

Так, в таблице 1 приведены значения характеристик направленности и степени согласования с фидером радиоудлинителя из одной антенны «волновой канал» при разных углах поворота полотна антенны χ.

В таблице 2 приведены значения характеристик направленности и степени согласования с фидером радиоудлинителя из двух антенн «волновой канал», соединенных в плоскости E в антенную решетку, при разных углах поворота полотен антенн χ, а в таблице 3 – значения характеристик направленности и степени согласования с фидером радиоудлинителя из двух антенн «волновой канал», соединенных в плоскости H в антенную решетку, при разных углах поворота полотен антенн χ.

ТАБЛИЦА 1. Значения характеристик направленности и степени согласования с фидером радиоудлинителя из одной антенны «волновой канал» при разных углах поворота полотна антенны

χ	*G*	КСВ	$2\theta_{0,5верт}$	$2\theta_{0,5гориз}$	КЗД
град	дБ	–	град	град	дБ
0	9,07	1,07	58	82	13,46
15	9,07	1,07	60	80	13,46
30	9,07	1,07	63	77	13,46
45	9,07	1,07	64	76	13,46

ТАБЛИЦА 2. Значения характеристик направленности и степени согласования с фидером радиоудлинителя из двух антенн «волновой канал» плоскости *E* при разных углах поворота полотна антенны

χ	*G*	КСВ	$2\theta_{0,5верт}$	$2\theta_{0,5гориз}$	КЗД
град	дБ	–	град	град	дБ
0	11,95	1,07	27,0	83	13,87
15	11.98	1,06	27,3	82	13,80
30	12,06	1,04	27,6	79	13,61
45	12,15	1,02	28,0	69	13,38

Так, в случае одной антенны при повороте полотна антенны менялась только ширина главного лепестка диаграммы направленности. Все остальные параметры не менялись. В случае радиоудлинителя из двух антенн «волновой канал», соединенных в антенную решетку в плоскости *E*, практически все характеристики направленности менялись при изменении угла поворота полотен антенн χ, за исключением ширины главного лепестка в вертикальной плоскости. Согласование антенны с питающим фидером улучшилось, а коэффициент усиления антенны вырос на 3 дБ. В случае радиоудлинителя из двух антенн «волновой канал», соединенных в плоскости *H* в антенную решетку, практически все характеристики направленности менялись при изменении угла поворота полотен антенн χ, за исключением ширины главного лепестка в горизонтальной плоскости. Согласование антенны с питающим фидером несколько ухудшилось (но осталось в пределах нормы), а коэффициент усиления антенны вырос в среднем на 3.

Антенну «волновой канал» для ее работы в качестве радиоудлинителя можно также доработать путем введения в ее конструкцию элемента механической фиксации положения полотна антенны с увеличением длины горизонтальной траверсы антенны на (0,5–0,75)λ (λ – длина волны) для установки полотна антенны в местах с максимальной напряженностью поля мобильной радиосвязи (рис.).

ТАБЛИЦА 3. Значения характеристик направленности и степени согласования с фидером радиоудлинителя из двух антенн «волновой канал» в плоскости *H* при разных углах поворота полотна антенны

χ	*G*	КСВ	$2\theta_{0,5верт}$	$2\theta_{0,5гориз}$	КЗД
град	дБ	–	град	град	дБ
0	11,70	1,19	58	42	15,00
15	11,67	1,19	59	42	15,26
30	11,57	1,20	61	41	15,71
45	11,42	1,22	66	40	15,70

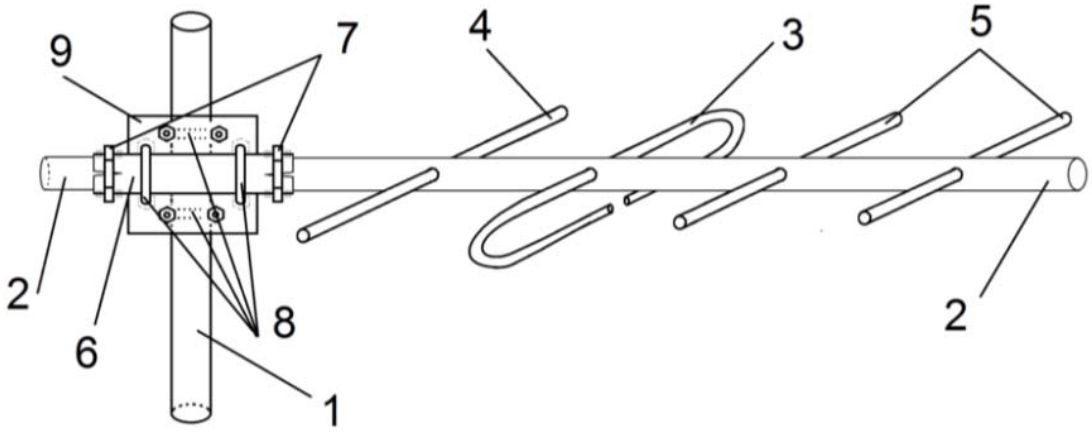


Рисунок. Чертеж радиоудлинителя сотовой связи для мест неуверенного приема (1 – вертикальная стойка, 2 – горизонтальная траверса антенного полотна, 3 – петлевой вибратор, 4 – рефлектор, 5 – директоры, 6 – металлическая трубка с резьбой и горизонтальными прорезями на концах, 7 – металлические гайки с конической резьбой, 8 – крепители (в частности хомуты или струбцины), 9 – крепежная пластинка)

Список используемых источников

1. Абарыков В. Н., Алексеев В. К. Ослабление и пространственные флуктуации поля УКВ в городе, пригороде и поселках сельского типа // Распространение электромагнитных волн: материалы всерос. науч. конф. Улан-Удэ, 12–15 мая 1993 г. Улан-Удэ : Наука, 2013. С. 43–53.

2. Шахобиддинов А. Ш. Особенности и характеристики распространения радиоволн диапазона сотовой связи 900 МГц // Проблемы развития информационого общества: материалы респ. науч. конф. Ташкент, 15–17 марта 2007 г. Ташкент : Изд. Гафура Гуляма, 2007. С. 37–39.

3. Ерохин Г. А. и др. Антенно-фидерные устройства и распространение радиоволн. М. : Радио и связь, 2004. 495 с.

УДК 591.71

ИТЕРАЦИОННАЯ МОДЕЛЬ ДЕЙСТВИЯ БИОФИЗИЧЕСКИХ ФАКТОРОВ

Л. М. Макаров, С. В. Протасеня

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

Рассмотрены вопросы системного моделирования событий в живом организме с учетом циркадных ритмов, клеточного митоза, нейронной активности сенсорных систем и биохимических факторов, обеспечивающих формирование прогноза развития процессов жизнедеятельности.

компьютерное моделирование, диссипативные системы.

Жизнедеятельность любого организма проявляется в среде обитания. Для человека такой средой является социум. Среда обитания может оказывать благотворное или неблагоприятное влияние на состояние здоровья человека, его самочувствие и работоспособность. Параметры окружающей среды, при которых создаются наилучшие для организма человека условия жизнедеятельности, называются комфортными. Естественно, понятие комфорта для каждого человека формируется индивидуально. Здесь большое значение приобретают как генетические параметры, так и физические параметры среды.

К наиболее значимым, аппаратно регистрируемым физическим факторам относятся все виды электромагнитных излучений.

Самым мощным естественным источником электромагнитного излучения в природе является Солнце. Именно благодаря солнечной энергии происходят все биологические процессы на Земле. Вся биосфера и сама жизнь существуют только за счет солнечной энергии. Диапазон длин волн солнечных излучений простирается от нескольких долей нм (гамма-излучение) до метровых радиоволн.

Живые организмы являются открытыми термодинамическими системами. В живом организме постоянно «включено» множество функциональных процессов, которые сопровождаются притоком из окружающей среды вещества и энергии. Существует и обратный процесс – сброса вещества и энергии. Часть процессов поддерживается постоянно, например, сердечная деятельность. Другая часть процессов реализуется по некоторому правилу, где в качестве переменного параметра рассматривается текущее время суток и интенсивность выраженность электромагнитного излучения.

Последние исследования указывают на то, что внутренние ритмы в организме организованы по законам иерархии: имеются основные

и подчиненные генераторы ритма. Главным центром циркадианных часов является супрахиазматическое ядро в головном мозге – это плотное скопление из примерно 20 тысяч нейронов. Другие генераторы ритма распределены по разным клеточным ансамблям. Это, как правило, специализированные клетки печени, почек, мышечной ткани. Принимая во внимание наличие различий в структуре одноименных функциональных тканей (клеточных структур) для каждого организма проявляется свой уникальный механизм генерации ритма. В среднем, клетки печени обновляются по истечении примерно одинакового промежутка времени у разных индивидуумов, хотя в реальности могут наблюдаться свои хронобиологические особенности.

Наиболее ярко такие индивидуальные отклонения от типовых показателей наблюдаются у людей, называемых «жаворонками» и «совами». Действительно внутренняя предрасположенность организма к раннему пробуждению и позднему сну, реализуется на основе сложного «генетического алгоритма», формируемого в момент рождения. Используя эти представления, в прогрессивных клинических рекомендациях по образу жизни, устанавливаются диетологические рационы питания, продолжительность периодов работы и отдыха. Эти рекомендации создаются на известных представлениях о динамике жизненных процессов в организме и с учетом действия циркадных ритмов, которые определяют ритмы смены неравновесных состояний.

Постоянный приток вещества, энергии и информации является необходимым условием существования неравновесных состояний в живом организме. Открытые системы называют необратимыми. В живых организмах, как необратимых системах, большое значение имеет фактор времени. Развивая это представление можно говорить о временном развитии организма, об особенностях развития термодинамической системы в разные периоды жизни. С целью детального изучения этих процессов создаются модели развития сложных систем [1]. Естественно многие современные суждения в этой области формируются на представлениях о естественных природных особенностях развития, формируемых сложными механизмами генетики.

Отдельно взятый ритм смены клеточных популяций является запрограммированным генетическим показателем, как, например, цвет глаз или цвет волос. С хронотипом связаны определенные черты характера, показатели здоровья и адаптационных возможностей.

Интересны клинические наблюдения в которых декларируется, что «совы» в большей степени, чем «жаворонки», подвержены риску возникновения сердечно-сосудистой патологии, однако их биоритмы более пластичны, и они лучше приспосабливаются к новым режимам жизнедеятельности. У «жаворонков» многие показатели здоровья лучше,

чем у «сов», но они более консервативны и с трудом переносят изменения привычного режима жизни.

В естественных условиях ритм физиологической активности человека синхронизирован с его социальной активностью, обычно высокой днем и низкой ночью. При перемещениях человека через временные пояса (особенно быстро на самолете через несколько временных поясов) наблюдается десинхронизация функций. Это проявляется в усталости, раздражительности, расстройстве сна, умственной и физической угнетенности; иногда наблюдаются расстройства пищеварения, изменения артериального давления.

Эти ощущения и функциональных нарушений возникают в результате десинхронизации циркадианных закрепленных ритмов физиологических процессов с измененным временем световых суток (астрономических) и социальной активности в новом месте пребывания человека.

Через некоторое время эти ритмы согласуются, но для разных направлений перемещения человека и разных функций это время будет неодинаковым. При перелетах в западном направлении биологические часы отстают по отношению к 24-часовому солнечному циклу, и для приспособления к распорядку дня в новом месте должна произойти фазовая задержка биологических часов.

По распространенному мнению, многие перестройки ритмов в организме происходят с участием зрительного анализатора, формирующего некоторые параметры запуска «клеточных хронометров». В этом отношении большое внимание уделяется диагностической дисциплине – иридодиагностике.

Визуальное и специализированное исследование зрачка, радужной оболочки создает предпосылки для раннего обнаружения нарушения внутренних ритмов организма. Иногда относительно небольшие изменения «картины» радужной оболочки оказывается достаточным чтобы наметить эффективные мероприятия по нормализации работы внутренних подсистем организма.

Фазы внутренних хронометров могут сдвигаться под воздействием определенных стимулов, которые способны навязывать свой ритм. Такие стимулы называются *цайтгеберами* (от нем. Zeit – «время» и geben – «давать») или задатчиками ритма. Индивидуальные часы различных клеточных популяций, связанных с потреблением энергии, способны реагировать на уникальные задатчики ритма, проявляющиеся в форме биохимических факторов или нейронных стимулов. Например, свет задает ритм центральным часам в супрахиазматическом ядре, опосредовано – через зрительный анализатор.

Благодаря своим связям со светочувствительными клетками сетчатки глаза, нейроны супрахиазматического ядра способны получать информацию о световом периоде снаружи и подстроить к внешним

условиям внутренние ритмы организма. Синхронизация периферических часовых систем осуществляется посредством вегетативной нервной системы специальными гормонами.

Цайтгеберами могут быть не только внешние воздействия, но и особенности поведения: режим физической активности, цикл смены сна и бодрствования и даже режим питания. Так, например, хорошо известно, что внутренние часы печени больше настроены на ритмичность приема пищи, чем на ритмы смены светлого и темного периодов суток [2].

В современной медицинской практике часто используют фармакологические препараты. Биохимические свойства таких препаратов часто декларируются на представлениях о среднем статическом терапевтическом эффекте. Известные теоретические методики оценки действия биохимического фактора только в последнее время стали учитывать физические факторы среды, скорость смены клеточных популяций в индивидуально исследуемом организме. Такие информационные модели расчета терапевтического эффекта значительно улучшили финальные результаты, позволили выявить специфические механизмы, влияющие на развитие ряда нарушений организма. Так, например, используя информационные представления о клеточном митозе, факторах среды, стало возможным устанавливать ореолы распространения мало изученных вирусов.

Вирусы представляют собой мельчайшие формы жизни, которые по размерам в несколько раз меньше бактерий. Они попадают в организм из воздуха, с пищей, водой и т. д. В отличие от бактерий, вирусы обладают генетическим материалом – РНК или ДНК, за счет чего могут воспроизводиться при включении в геном человека. Другими словами, они могут размножаться только в клетках живых существ. К тому же, вирусы действуют целенаправленно и избирательно, то есть проникают лишь в конкретные места и поражают только определенные структуры. Скорость размножения вирусов различается в зависимости от типа клеток, в которых они паразитируют. И чем выше скорость воспроизводства вирусов, тем короче инкубационный период.

Рассмотрим модель распространения биофактора на территории. Для определенности полагаем, что развертка событий – проявления интенсивности биофактора, описывается выражением:

$$E(a,b,c,t) = \sum_{i=1}^{12} a_i \sin(b_i t + c_i),$$

где период наблюдения выбран t = 18–20 мес.

Параметры $\{a, b, c\}$ характеризуют начальные значения вероятностей обнаружения биофактора. Эскизный расчет по данным модели позволяет

создать образ событий на интервале наблюдения, который представлен на рисунке.

Рисунок. Интенсивность проявления биофактора

Полученный результат демонстрирует присутствие как положительных, так и отрицательных значений биологического фактора. Возможность обнаружения моментов времени активации негативных факторов среды, даже на уровне модели, открывает широкие перспективы в планировании защитных мероприятий.

Для практической медицины такой метод обнаружения моментов активации позитивных или негативных факторов, в реальных физических условиях среды обитания человека, позволяет намечать терапевтические процедуры с использованием фармакологических средств. Фармакология – как научное направление постоянно предлагает новые виды лекарственных препаратов, способствующих формированию комфортной среды обитания человека. Математическое целенаправленное моделирование и прогнозирование конечного результата во многом способствует решению поставленной задачи.

Список используемых источников

1. Макаров Л. М. Структурированный лингвистический анализ // Информационные технологии и телекоммуникации. 2013. вып. 2. С. 61–74.

2. Комаров О. М., Рапопорт С. И. Хронобиология и хрономедицина. М. : Триада-Х, 2000. 488 с.

УДК 681.3.06

ГРАФИЧЕСКИЙ ИНТЕРФЕЙС ВЕЙВЛЕТ-ОБРАБОТКИ ИЗОБРАЖЕНИЙ ДЛЯ ПОЛЬЗОВАТЕЛЕЙ КАЗАХСТАНА

Ж. Б. Маликова[1], А. Б. Степанов[2]

[1]Евразийский национальный университет им. Л. Н. Гумилева (Астана)
[2]Санкт-Петербургский государственный университет телекоммуникаций им. проф. М. А. Бонч-Бруевича

Статья посвящена описанию предложенного графического интерфейса вейвлет-обработки изображений, разработанного для пользователей Казахстана. Приводятся этапы разработки данного интерфейса, подробное описание его элементов, преимущества по сравнению со встроенным в систему MATLAB пакетом Wavelet Toolbox. В завершении приводятся результаты работы графического интерфейса при обработке одного из тестовых изображений.

вейвлет, изображение, графический интерфейс, MATLAB.

Вейвлеты – это класс особых функций с нулевым интегральным значением [1, 2]. Вейвлеты находят широкое применение при анализе различных одномерных сигналов [3, 4] и изображений [1].

В состав системы MATLAB входит специализированный пакет для выполнения вейвлет-анализа сигналов – Wavelet Toolbox. Данный пакет обладает широким набором инструментов для обработки одномер-ных сигналов и изображений. Достойнствами данного пакета является большой выбор настроек, а также средств визуализации полученных результатов. Основным недостатком является ограничения в выборе языка его интерфейса. Данный пакет, как и вся система MATLAB, поддерживает английский язык. При проведении большого числа однотипных исследо-ваний чрезмерный набор настроек может снижать скорость выполнение работы. Кроме того, отсутсвие родного языка в настройках интерфейса может затруднять проведение занятий по обработке изображений с обучающимися, не владеющими английским языком.

В данной работе предлагается альтернатива данному пакету: графический интерфейс пользователя, позволяющий выполнять вейвлет-разложение изображений с заданным числом уровней и возможностью выбра вейвлета. Преимущество предлагаемого графического интерфейса пользователя заключется в его простоте, что особенно важно при обработке большого числа изображений при проведении исследований. Все пояснения выполнены на казахском языке, что облегчает работу с ним для пользователей Казахстана. Данный графический интерфейс может быть использован при проведений научных исследований и выполнении лабораторных работ студентами высших учебных заведений Казахстана.

При разработке данного интерфейса использовался встроенный инструмент MATLAB – GUIDE QUICK Start. Основное окно интерфейса имеет (рис. 1):

– поле для вывода исходного изображения и результатов вейвлет-разложения (*Суреттің вейвлет-өңдеуі*);

– кнопку загрузки изображения (*Суретті жүктеу*);

– поле для ввода названия вейвлета (*Вейвлетті таңдау*);

– поле для ввода числа уровней разложения (*Бөлу деңгейлерінің саны*);

– кнопка выход (*Шығу*).

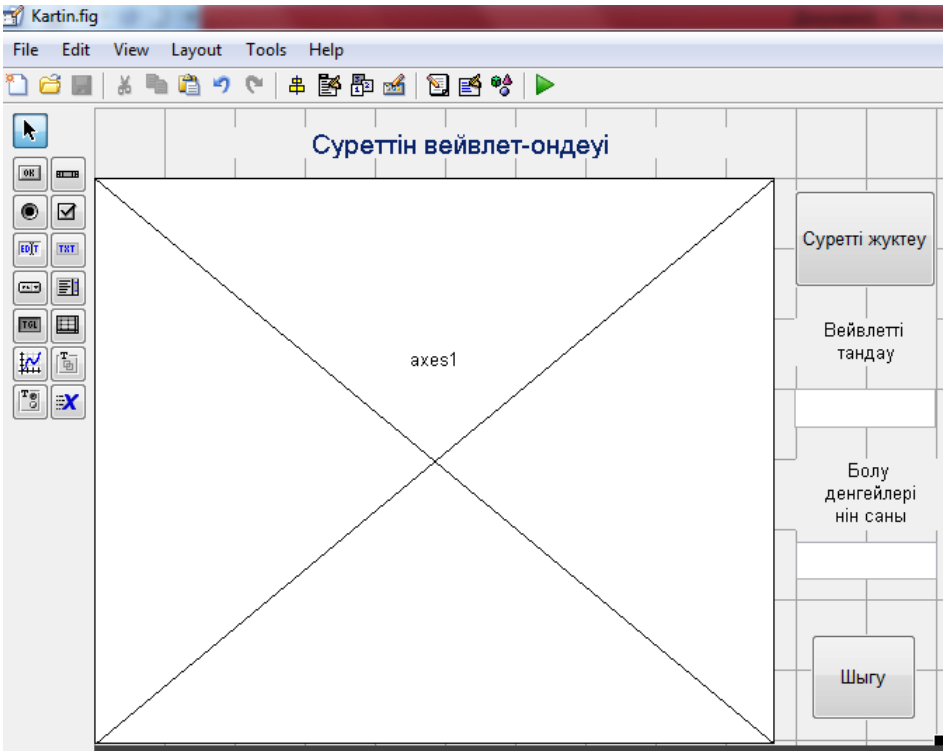


Рис. 1. Окно интерфейса, созданное с помощью GUIDE QUICK Start

Данный интерфейс выполняет вейвлет-разложение согласно схеме показанной на рисунке 2 [1].

– Изображение $s(x, y)$ подвергается разложению на аппроксимирующие коэффициенты $cA1$, горизонтальные $cH1$, вертикальные $cV1$ и диагональные $cD1$ детализирующие коэффициенты.

– Аппроксимирующие коэффициенты $cA1$ являются результатом разложения изображения $s(x, y)$ по базису $\varphi(x)\varphi(y)$ [1].

Детализирующие коэффициенты могут быть получены [1]:

– горизонтальные $cH1$ – при разложении изображения по базису $\varphi(x)\psi(y)$;

– вертикальные $cV1$ – при разложении изображения $s(x, y)$ по базису $\psi(x)\varphi(y)$;

– диагональные $cD1$ – при разложении изображения $s(x, y)$ по базису $\psi(x)\psi(y)$.

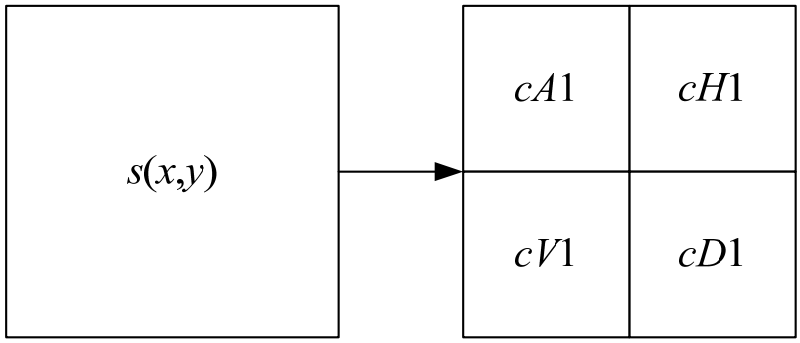


Рис. 2. Схема вейвлет-разложения изображения

На рисунке 3 показана работа графического интерфейса при вейвлет-разложении изображения. При этом используется вейвлет Добеши 5 и один уровень разложения. В верхней левой части окна выводится исходное изображение, далее детализирующие коэффициенты.

Благодаря отсутствию избыточного числа настроек, применение предложенного графического интерфейса позволяет значительно упростить выполнение вейвлет-разложения изображений, а поддержка казахского языка значительно облегчает работу с интерфейсом для жителей Казахстана.

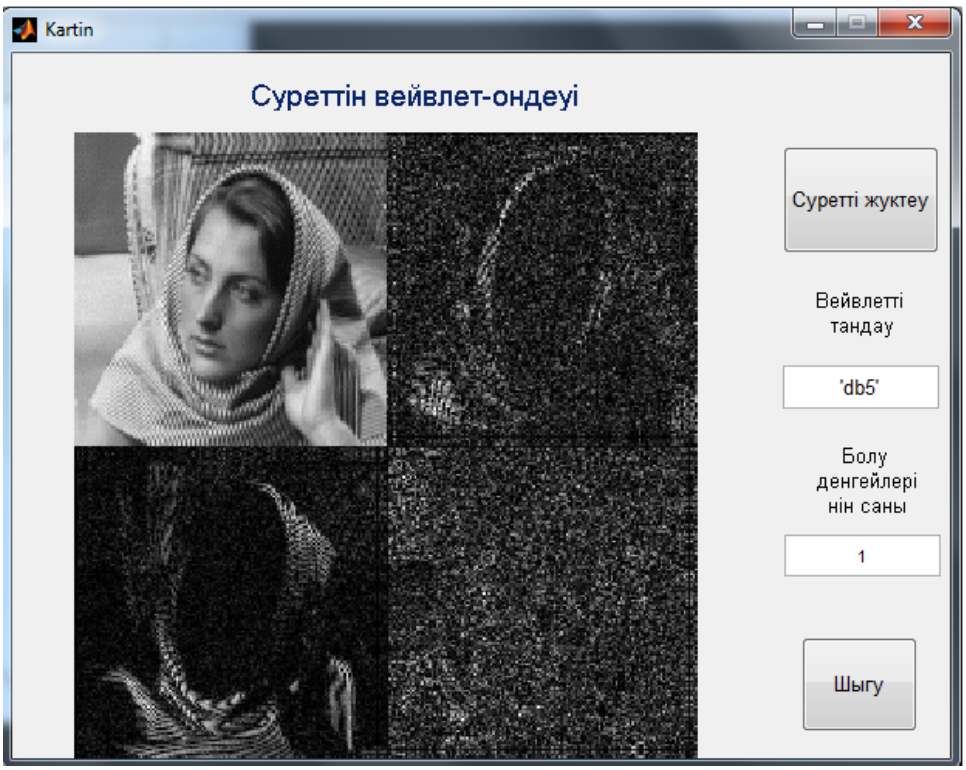


Рис. 3. Графический интерфейс вейвлет-обработки изображений для пользователей Казахстана

Список используемых источников

1. Смоленцев Н. К. Основы теории вейвлетов. Вейвлеты в MATLAB. М. : ДМК Пресс. 2005. 304 с. ISBN 5-94074-122-3.

2. Добеши И. Десять лекций по вейвлетам. Ижевск : НИЦ @ Регулярная и хаотическая динамика@. 2001. 464 с.

3. Stepanov A. B. One the use of splines for wavelet construction for solving the problem of biomedical signal analysis process automation // Conference of Open Innovation Association, FRUCT. 2015. pp. 216–221.

4. Stepanov A. B. Neural network model of wavelets for the continuous wavelet transform // IEEE Catalog number CFP14BDA-USB. 2014. pp. 177–178.

УДК 621.396.96

АКТУАЛЬНЫЕ ЗАДАЧИ ОБРАБОТКИ И ПЕРЕДАЧИ РАДИОЛОКАЦИОННОЙ ИНФОРМАЦИИ

С. М. Одоевский, В. И. Покровская

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

Статья посвящена проблемам обработки радиолокационной информации. Приведено описание основного алгоритма обнаружения траектории (фильтр Калмана). Рассмотрены основные задачи при обработке информации, полученной от радиолокационной станции. Для дальнейшего рассмотрения предложен метод предсказания траектории объекта на основе метода физической регуляризации и функции Грина.

обработка радиолокационной информации, третичная обработка информации, фильтр Калман, метод физической регуляризации, функция Грина.

Радиолокационные станции (далее РЛС) являются основными средствами получения радиолокационной информации в любых системах наблюдения за воздушной, надводной и подводной обстановкой.

Основная задача радиолокации заключается в сборе и обработке радиолокационной информации (далее траекторная обработка) относительно зондируемых объектов, а также своевременной и достоверной передаче данных в центр управления.

Целью траекторной обработки является оценка параметров движения объекта, находящегося в зоне наблюдения РЛС, на основе измерений его мгновенного положения для определения траектории на интервале измерений и прогнозирования его последующего движения.

В радиолокации приходится иметь дело с очень малыми сигналами, интенсивность которых соизмерима с интенсивностью собственных шумов ра-

диоприемного устройства РЛС. Так же следует учитывать пропускную способность канала связи, ввиду чего требуется фильтрация ложных сигналов. Это ведет к проблеме выбора порога обнаружения цели. Если он завышен, то есть вероятность пропустить цель. Если же наоборот, занизить его, то получим огромное количество ложных отметок. Из этого вытекает проблема повышения надежности и непрерывности автосопровождения в условиях воздействия активных и пассивных помех. Кроме того, в современной радиолокации существует необходимость обработки объединенной информации от разных РЛС.

Одной из важнейших проблем современной радиолокации является задача точного построения траектории цели и её надежное сопровождение.

На данный момент актуальным является создание нового или улучшение существующего алгоритма обработки информации, поступающей от РЛС, с целью точного определения траектории и фильтрации ложных сигналов.

На основе исследованного материала [1, 2, 3, 4, 5], можно сделать вывод, что в основном все разработчики, для предсказания траектории объекта используют фильтр Калмана.

Фильтр Калмана предназначен для рекурсивного дооценивания вектора состояния априорно известной динамической системы, то есть для расчёта текущего состояния системы необходимо знать текущее измерение, а также предыдущее состояние самого фильтра. Таким образом, фильтр Калмана, подобно другим рекурсивным фильтрам, реализован во временном, а не в частотном представлении. Алгоритм работает в два этапа. На этапе прогнозирования фильтр Калмана экстраполирует значения переменных состояния, а также их неопределенности. На втором этапе, по данным измерения (полученного с некоторой погрешностью), результат экстраполяции уточняется. Благодаря пошаговой природе алгоритма, он может в реальном времени отслеживать состояние объекта (без заглядывания вперед, используя только текущие замеры и информацию о предыдущем состоянии и его неопределенности) [6].

При одновременной работе нескольких РЛС, основной сложностью пространственного совмещения наблюдений, является возможное смещение локальных оценок положения цели. Наличие смещения может быть вызвано систематическими погрешностями измерений пространственных координат цели, неточностью измерения местоположения РЛС, рассогласованием временных шкал или нестабильностью датчиков. Всё это приводит к снижению точности совместного оценивания положения цели, уменьшается вероятность правильного отождествления, может появиться эффект дублирования траектории [7]. При обработке информации от нескольких РЛС фильтром Калмана, алгоритм будет чувствителен к резким изменениям входного сигнала, что приводит к неточной оценке координат цели (рис. 1).

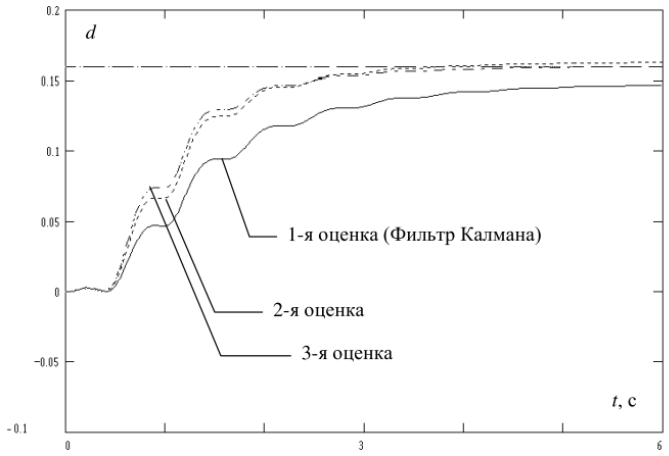


Рис. 1. Переходный процесс фильтра Калмана

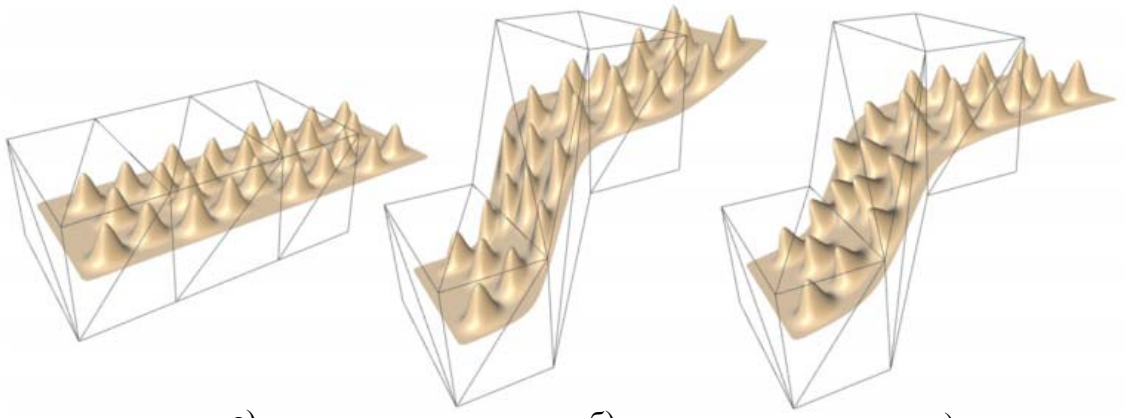
В такой ситуации основой решения задачи синтеза систем, функционирующих в условиях неопределенности относительно параметров входных воздействий, с успехом могут служить методы регуляризации [8].

Для решения некорректных задач советским математиком А. Н. Тихоновым был предложен простой, но чрезвычайно эффективный метод, называемый регуляризацией и основанный на привлечении дополнительной априорной информации о решении, которая может быть, как качественной, так и количественной. Например, можно искать решение, обладающее определенной гладкостью, или максимально близкое к некоторому вектору, что позволяет решить проблему адаптации фильтра к изменяющимся внешним воздействиям.

Вторым вариантом реализации алгоритма определения траектории объекта может послужить работа сотрудников Тель-Авивского университета [9]. Ими было предложено использовать функцию Грина, как функцию изменения координат. Их метод основан на книге о конформных преобразованиях, советского математика Л. В. Канторовича [10]. Идея заключается в расчёте области входных данных в виде координатной сетки, представленной функцией Грина. Разработанный метод был использован авторами для обработки изображений и 3D моделей, позволив им переносить в пространстве точки изображений с учетом и сохранением исходных пропорций (рис. 2).

Благодаря возможности перерасчёта функции Грина для последующих положений точек в пространстве предлагается использовать данный метод в качестве алгоритма определения будущей траектории объекта, за счёт перерасчёта координат.

Используя предложенные подходы или их комбинацию, кажется возможным получение алгоритма способного адаптироваться к резким изменениям входного сигнала и точно вычислять траекторию наблюдаемых объектов.



а) б) в)

Рис. 2. Деформация 3D объекта:
а – исходный объект; б – деформация стандартными методами;
в – деформация с помощью функции Грина

Список используемых источников

1. Коновалов А. А. Основы траекторной обработки радиолокационной информации. Часть 2. СПб. : СПбГЭТУ «ЛЭТИ», 2014. Ч. 2. 180 с. ISBN 978-5-7629-1544-1.

2. Машаров К. В. Применение фильтра Калмана для оценки координат цели в РЛС // Вестник СибГУТИ. 2011. № 3. С. 59–66.

3. Зайцев Д. В. Многопозиционные радиолокационные системы. Методы и алгоритмы обработки информации в условиях помех. М. : Радиотехника, 2007. 96 с. ISBN 5-88070-138-7.

4. Кузьмин С. З. Цифровая обработка радиолокационной информации. М. : Советское радио, 1967. 398 с.

5. Сейдж Э. Теория оценивания и её применение в связи и управлении. М. : Связь, 1976. 496 с.

6. Браммер К., Зиффлинг Г. Фильтр Калмана-Бьюси: пер. с нем. М. : Наука. Главная редакция физико-математической литературы. 1982. 200 с.

7. Коновалов А. А. Основы траекторной обработки радиолокационной информации. Часть 1. СПб. : СПбГЭТУ «ЛЭТИ», 2013. 164 с. ISBN 978-5-7629-1449-9.

8. Костоглотов А. А. Метод синтеза алгоритмов адаптивной фильтрации на базе принципа регуляризации А. Н. Тихонова // Ростовский военный институт, «Журнал Радиоэлектроники. 2002. № 5. URL: http://jre.cplire.ru/alt/may02/2/text.html (Дата обращения 17.04.2016).

9. Yaron Lipman, David Levin, Daniel Cohen-Or. Green coordinates // Tel-Aviv University, SIGGRAPH '08 ACM SIGGRAPH, Article No. 78, 2008. ISBN 978-1-4503-0112-1.

10. Канторович Л. В., Крылов В. И. Приближенные методы высшего анализа. Л. : Физматгиз, 1962. 708с.

УДК 621.391.825

ФОРМИРОВАНИЕ ШИРОКОПОЛОСНЫХ ПОМЕХ

Э. Н. Сунгатуллин, В. М. Устименко

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

Широкополосные заградительные помехи в нисходящем канале (от базовой станции к мобильной) используются для обеспечения защиты от утечек информации по всем каналам сетей беспроводной мобильной радиосвязи. В статьее рассмотрен вариант цифрового формирования таких помех, более оптимальный по сравнению с аналоговым. При этом дальность блокирования связи зависит от расстояния до ближайшей базовой станции.

постановщик помех, мобильная радиосвязь, частотно-манипулированная шумовая помеха, 3G, цифро-аналоговый преобразователь, псевдослучайная последовательность, управляемый напряжением генератор.

При нынешнем широком распространении систем радиосвязи применение радиопомех чрезвычайно актуально в задачах радиоэлектронной борьбы (РЭБ). В коммерческих системах связи возможна несанкционированная утечка информации. Блокирование радиоканалов этих систем позволяет предотвратить эту утечку или нежелательное использование систем связи в конкретных помещениях, зданиях или зонах местности.

Во многих случаях априорных данных о радиоканалах, частотах и сигналах, подлежащих блокированию, недостаточно, поэтому обычно подавлению подвергается весь диапазон радиочастот, в котором возможна работа радиолинии передачи информации или системы связи, т. е. используются *заградительные* по частоте помехи [1]. В противоположных случаях применяют *прицельные* (узкополосные) по частоте помехи.

Непрерывные шумовые помехи являются наиболее универсальными, так как обеспечивают принципиальную возможность маскировки полезных сигналов любой структуры и формы на временной и частотной оси, а также по направлению [2]. В зависимости от способа формирования непрерывные шумовые помехи подразделяются на *прямошумовые* (немодулированные), которые образуются в результате усиления собственных шумов, возникающих в электронных приборах (электровакуумных лампах, полупроводниковых диодах и транзисторах), и *модулированные*. *Прямошумовые* помехи не получили широкого применения из-за сравнительно низкой мощности источников первичного шума, необходимости его последующего многоступенчатого усиления и трудности сохранения высоких энтропийных свойств.

Модулированные формируются путём модуляции высокочастотных гармонических колебаний низкочастотным шумом по амплитуде (АМШ), частоте (ЧМШ), фазе (ФМШ) или одновременно по нескольким параметрам.

Для подавления связи необходимо выполнение условия (1) превышения отношения помеха/сигнал над коэффициентом подавления K_n на входе приемника мобильной станции (МС):

$$\frac{Pn}{Pc} > Kn,$$

где Pn и Pn – мощности помехи и сигнала на входе приемника блокируемой системы соответственно [3].

Постановка такой помехи приводит к срыву управления мобильного телефона базовой станцией мобильной связи (происходит потеря сети мобильным телефоном) и, следовательно, к невозможности передачи информации. При этом на экране телефона значок уровня сигнала пропадает и появляется сообщение «Поиск сети».

Ранее [4] был рассмотрен способ формирования широкополосной заградительной помехи (рис. 1).

Здесь с целью повышения эффективности помехового сигнала используется модуляция полосовым белым гауссовским шумом (БГШ) по частоте высокочастотного сигнала.

Генератор помех включает: высокочастотный генератор (ГВЧ) на базе генератора, управляемого напряжением, (ГУН); генератор линейно изменяющегося (пилообразного) напряжения (ГЛИН); источник низкочастотного шума (ИНШ); полосовой фильтр; усилитель мощности; согласующее устройство и антенну.

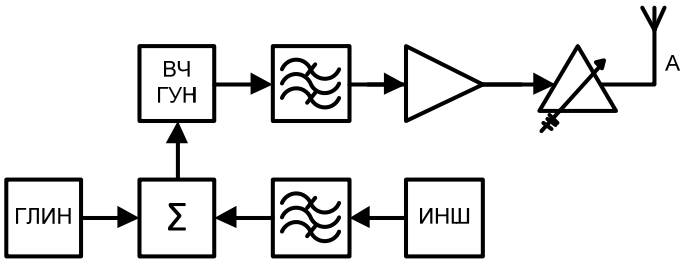


Рис. 1. Схема блокиратора стандарта связи UMTS2100
с широкополосной помехой с шумовой частотной модуляцией (ЧМШ)

Для обеспечения требуемой эффективности работы блокиратора скорость изменения управляющего пилообразного напряжения должна быть довольно высокой. Например, у блокиратора связи в стандарте 3G UMTS2100 подобранный экспериментально оптимальный по энергетике период следования пилообразных импульсов составляет около 4 мкс [4].

Рассмотрим подробнее ИНШ. Наиболее простым способом формирования низкочастотного шума является аналоговый. В данном случае можно использовать тепловой шум в резисторе или лавинный шум обратно смещенного p-n-перехода (диода Шоттки или стабилитрона) с последующим его усилением и фильтрацией до необходимой полосы частот.

Существует также менее дорогой цифровой способ формирования полосового низкочастотного шума из псевдослучайной последовательности, полученной, например, в микроконтроллере и дальнейшим цифро-аналоговым преобразованием и фильтрацией.

Рассмотрим пример формирования широкополосной заградительной помехи системе связи UMTS2100.

На рисунке 2 приведена схема модели цифрового формирователя широкополосной помехи в системе автоматизированного проектирования Microwave Office.

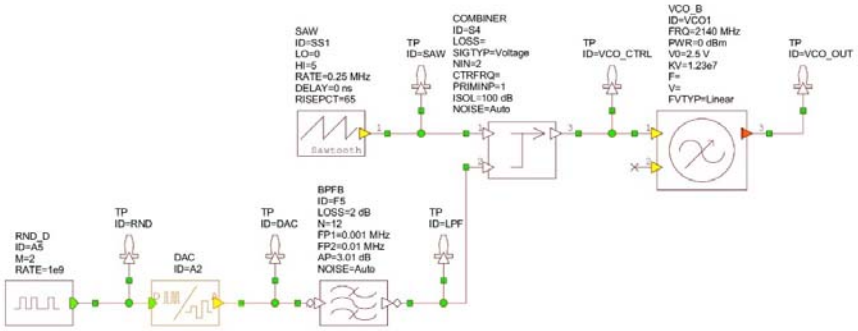


Рис. 2. Схема формирователя широкополосной заградительной помехи

Ниже (рис. 3) приведен спектр помехи, модулированной сгенерированным цифровым способом шумом полосой 9 кГц.

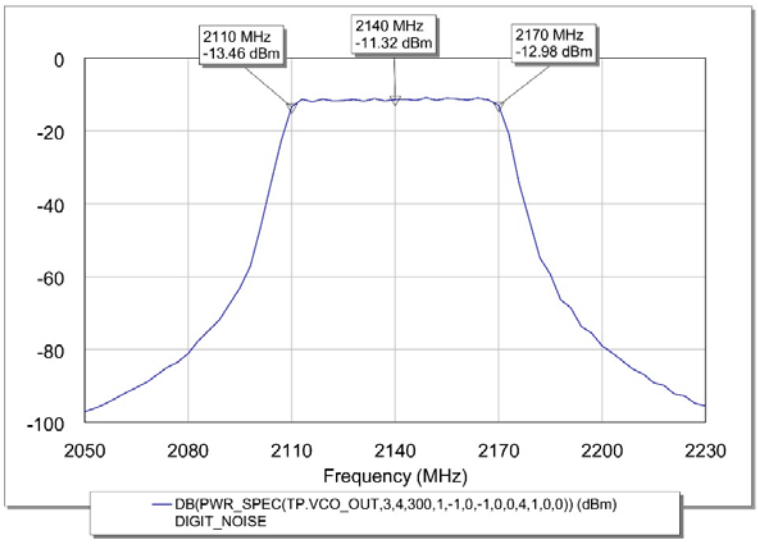


Рис. 3. Спектр моделированной помехи UMTS2100

Еще ниже (рис. 4) приведены спектры экспериментальной помехи, модулированной шумом полосой 5, 10 и 15 кГц соответственно.

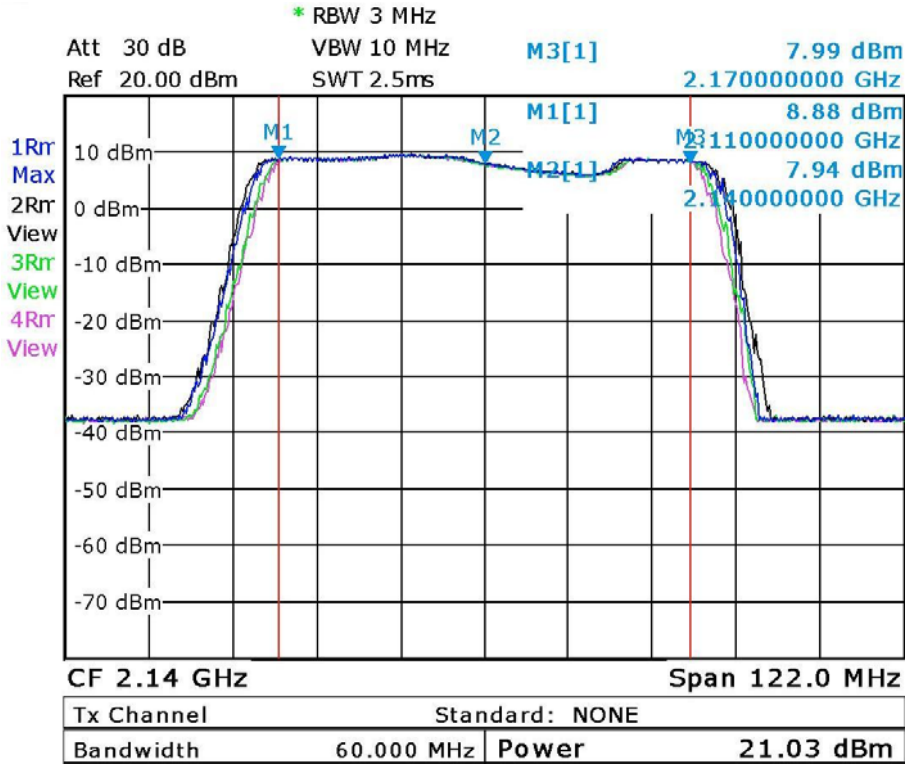


Рис. 4. Спектры экспериментальной помехи UMTS2100

При подавлении систем связи наиболее широко используют широкополосные помехи, модулированные шумом, поскольку у них наилучшие маскирующие свойства; кроме того, обычно не требуется большой точности совмещения несущей частоты передатчика помех с несущими частотами базовых станций.

Список используемых источников

1. Палий А. И. Радиоэлектронная борьба, изд. 2-е, перераб. и доп. М. : Воениздат, 1989. 350 с.

2. Давыдова Н. С. Информационное подавление радиоэлектронных систем. Активные помехи, передатчики и станции активных помех : учебное пособие. М. : МАИ, 2002. 80 с.

3. Современная радиоэлектронная борьба. Вопросы методологии / под ред. В. Г. Радзиевского. М. : Радиотехника, 2006. 424 с. ISBN 5-88070-082-8.

4. Сунгатуллин Э. Н., Устименко В. М. Выбор помеховых сигналов блокираторов систем мобильной связи // Актуальные проблемы инфотелекоммуникаций в науке и образовании. IV Международная научно-техническая и научно-методическая конференция: сб. науч. ст. в 2 т., т. 1 / под ред. С. В. Бачевского. СПб. : Санкт-Петербургский государственный университет телекоммуникаций им. проф. М.А. Бонч-Бруевича, 2015. С. 164–170. URL: http://sut.ru/doci/nauka/4.apino.2015.sut.pdf (Дата обращения 4.04.2016).

УДК 621.397

DVB-S2X – РАСШИРЕНИЕ СТАНДАРТА DVB-S2

С. Л. Федоров

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

Стандарт DVB-S2x (ETSI EN 302307 часть 2) является расширением стандарта DVB-S2 (ETSI EN 302307 часть 1) и предоставляет дополнительные технологии и функции, обеспечивающие повышение эффективности для применения в непосредственном телевизионном вещании (Direct to Home – DTH), при распространении цифровых телевизионных программ через магистральные линии связи, в приложениях VSAT и DSNG. Стандарт затрагивает также и рынок мобильных приложений.

DVB-S2, DVB-S2x, пропускная способность, спутниковые линии связи, цифровое телевидение.

С каждым годом растет количество передаваемой информации (данные, программы телевизионного и звукового вещания) через спутниковые линии связи. Пользователи ожидают получить необходимый сервис в любом месте земного шара. Самые востребованные приложения, заставляющие функционально расширить стандарт DVB-S2 это цифровое телевизионное и звуковое вещание, а также высокоскоростные IP сервисы. Учитывая развитие телевидения ультравысокой четкости (ТУВЧ), в долгосрочной перспективе потребуется большая пропускная способность спутниковых линий связи. Предоставляемые стандартом DVB-S2x новые технологии позволяют повысить пропускную способность на 20 % для DTH-приложения и на 51 % для профессиональных приложений, к которым относится распространение программ цифрового телевидения через магистральные линии связи [1], что позволяет увеличить количество передаваемых программ. Для VSAT приложений это приведет к увеличению количества абонентов и, как следствие, повышение доходов провайдеров. Также появляется возможность добавления дополнительных услуг (мультисервисные спутниковые сети).

Первая инновация в новом стандарте касается использования малых коэффициентов скругления (5 %, 10 % и 15 %) по сравнению с теми, которые используются в настоящее время в стандарте DVB-S2. Уменьшение коэффициентов скругления приводит к увеличению крутизны АЧХ фильтра (рис. 1). Пропускная способность может повысится до 15 % [1]. Необходимо отметить, что не всегда коэффициент 5 % может дать хорошие результаты. В некоторых случаях предпочтительным оказывается коэффициент 10 %.

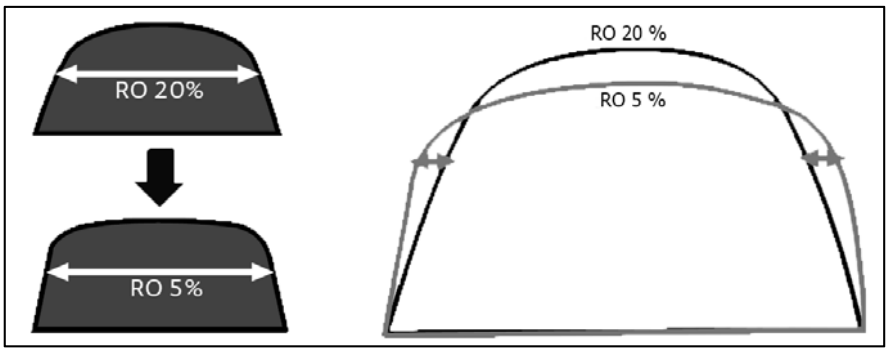


Рис. 1. Вид АЧХ спектрообразующего фильтра
при коэффициенте скругления (RO) 5 % и 20 %

В стандарте DVB-S2x применена улучшенная технология фильтрация, которая позволяет уменьшить боковые лепестки спектра и, тем самым, уменьшить расстояние между несущими (рис. 2).

Следующим шагом стало расширение режимов помехоустойчивого кодирования и видов модуляции (добавлены 64, 128, 256-APSK). Количество режимов выросло с 28 (DVB-S2) до 112 (DVB-S2x). Варьируя предложенными режимами, удельная пропускная способность может быть повышена до 51 % (по сравнению с DVB-S2).

Для обеспечения приема сигналов с низким отношением Es/No (до минус 10 дБ. В стандарте DVB-S2 минимальное отношение Es/No до минус 2,5 дБ) были добавлены 9 режимов помехоустойчивого кодирования (модуляции QPSK и BPSK). Это позволило обеспечить устойчивость спутниковых сетей к атмосферным замираниям и возможность использования небольших антенн для приложений «на ходу» (земля, воздух, вода).

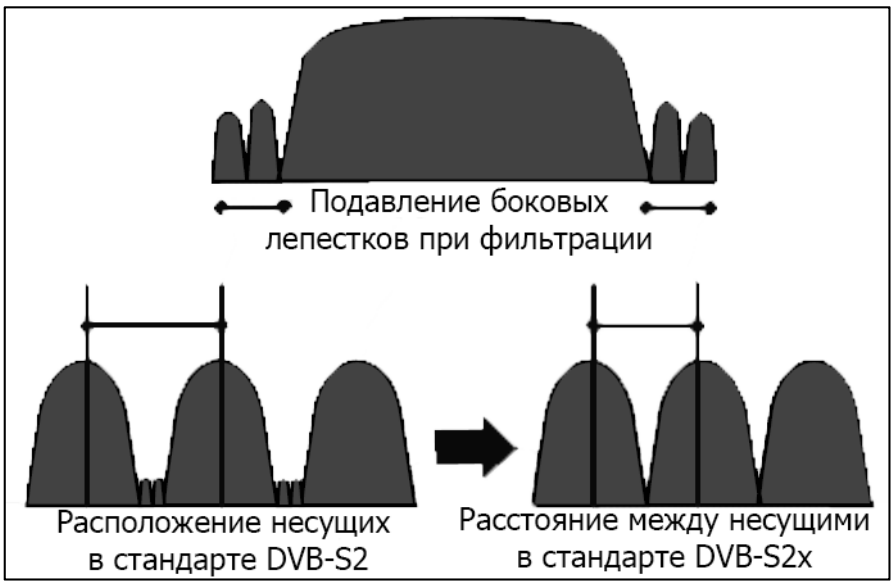


Рис. 2. Оптимальное расположение несущих

Введение стандарта DVB-S2 уже привело к значительному улучшению показателей спектральной эффективности для работы DTH-приложений, поэтому DVB-S2X не смог принести каких-либо значимых новых преимуществ на физическом уровне в этом плане, которые были бы подобны переходу от DVB-S к DVB-S2 (где-то на уровне 30 %). Тем не менее, стандарт DVB-S2X обеспечивает для DTH более точную настройку физического и верхнего протоколов DVB-S2, предлагая довольно привлекательный пакет (для проектов нового поколения, которые, в любом случае, потребуют обновления ресиверов).

Стандарт DVB-S2x поддерживает широкополосные транспондеры: от 72 МГц (как правило, в С-диапазоне) до нескольких сотен МГц (Ка-диапазон). В принципе, можно было бы выбрать несколько узкополосных каналов внутри широкополосных транспондеров, но это потребует работы спутникового ретранслятора на пониженной мощности в нисходящей линии связи. Такой режим не является оптимальным.

Технология параллельной передачи через несколько транспондеров транспортного потока предназначена, в основном, для приложения непосредственного телевизионного вещания и связана с внедрением в ближайшее время ТУВЧ. Пропускная способность для передачи такого сигнала требуется в четыре раза больше, чем при передаче сигнала телевидения высокой четкости (ТВЧ). При использовании нового стандарта видеокодирования H.265/HEVC коэффициент сжатия увеличивается примерно в 2 раза по сравнению со стандартом H.264/AVC (табл.).

ТАБЛИЦА. Значения информационной скорости при передаче одной ТВ программы

Формат разложения изображения	Стандарт видеокодирования	Скорость, Мбит/с
ТВЧ	H.264/AVC	10
ТУВЧ	H.264/AVC	40
ТУВЧ	H.265/HEVC	20

При использовании транспондера с полосой частот 36 МГц можно было бы передать 6 программ ТВЧ с суммарной скоростью 60 Мбит/с. Количество программ может быть увеличено до 7 при использовании технологии статистического мультиплексирования. Для ТУВЧ только 3 программы можно передать в полосе транспондера 36 МГц. Стандарт DVB-S2x предоставляет возможность передать транспортный поток с программами ТУВЧ одновременно через несколько транспондеров. Используя статистическое мультиплексирование, можно будет передать в этом потоке, например, дополнительную программу ТУВЧ.

С увеличением типа и количества передаваемых сервисов в одном частотном спутниковом канале вопрос о помехах в совмещенном канале связи не обойден в стандарте DVB-S2x. Новый стандарт имеет механизм для «смягчения» помехи, обеспечивая лучшее разграничение между соседними услугами.

Список используемых источников

1. Willems K. DVB-S2X Demystified. Newtec White paper [Электронный ресурс]. URL:http://www.newtec.eu/frontend/files/userfiles/files/DIALOG/Whitepaper DVB_S2X.pdf (дата обращения 15.04.2016).

2. DVB Fact Sheet. DVB-S2X – 2nd Generation Satellite Extensions [Электронный ресурс]. URL: https://www.dvb.org/resources/public/factsheets/dvb-s2x_factsheet.pdf (дата обращения 15.04.2016).

УДК 534.31

ИНТЕГРАЛЬНАЯ ОЦЕНКА АКУСТИЧЕСКОГО КАЧЕСТВА ЗВУКОВЫХ СИГНАЛОВ

Д. В. Шувалов

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

В настоящее время исследователями предложены различные субъективные критерии оценки вклада акустики помещений в качество звучания аудиосигналов, предложены соответствующие им объективные параметры, на основе которых рассчитывается оценка. В данной работе рассмотрены основные критерии и параметры, проведена их систематизация.

время реверберации, критерий оценки, звуковое давление, разборчивость речи.

Сигнал по пути от источника к слушателю претерпевает различные изменения: в электрических трактах идёт ограничение полосы, добавляются шумы и искажения, в современных системах используется сжатие на основе психоакустики, и т. д. При воспроизведении сигнала в помещении, происходит его изменение за счёт суммирования прямого сигнала с его отражениями, и слушатель оценивает совокупность сигнала и вклада в его звучание, определяемое помещением.

Качество звучания определяется видом сигнала. Для речи наиболее важно правильно распознать как можно больше слов, т. е. чем выше её разборчивость, тем выше оценка, для музыкальных сигналов оно описывается множеством критериев, среди которых нельзя выделить один наиболее важный.

На основе измерений различных параметров отраженных сигналов определён ряд обособленных объективных параметров оценки акустического качества помещений. Далее будут рассмотрены некоторые из них и соответствующие им субъективные критерии оценки качества акустики помещений.

Одним из субъективных критериев оценки является жизненность, она связана с величиной времени реверберации, особенно на высоких и средних частотах. Стандартное время реверберации – такой интервал времени, за который уровень звуковой энергии снижается на 60 дБ.

Рассчитать величину времени реверберации T можно по формуле [1]:

$$T = \frac{0{,}163\,V}{4mV - S\ln(1-\alpha_{ср})},$$

где V – объём помещения, м^3, m – показатель затухания как функция частоты и поглощения звука в воздухе, S – площадь отражающих поверхностей, м^2, $\alpha_{ср}$ – средний коэффициент поглощения поверхности зависящий от частоты.

В [1] указано, что оптимальное значение времени реверберации составляет 0,4–1 с для речи, 1–1,5 с для камерной музыки, 1,6–2,2 с для симфонической музыки.

В то время как T является важным объективным параметром, субъективному восприятию отзвука больше соответствует величина времени ранних затуханий EDT (*Early Decay Time*), которая соответствует снижению уровня звука на 10 дБ на начальном этапе реверберации [2, 3].

В [4] даны такие параметры как мера гулкости H и мера четкости звука C_{50}, определяемые энергией ранних и поздних отражений. Субъективно они соответствуют громкости реверберации и возможности слушателя воспринимать звуки отдельно друг от друга. Другой параметр, соответствующий балансу между ранними и поздними отражениями – центральное время t_s [5]:

$$t_s = \frac{\int_0^\infty t p^2(t)dt}{\int_0^\infty p^2(t)dt}.$$

Небольшая величина t_s соответствует чистому звуку с высокой разборчивостью, большие значения возникают при преобладании энергии поздних отражений [5].

Пространственное впечатление соответствует ощущению расширения размеров источника звука, погружению в звук, когда присутствует большое количество боковых отражений. Можно измерить индекс пространственного впечатления R при помощи микрофонов с разной направленностью [6]:

$$R = 10\lg\frac{\int_{25мс}^{\infty} p_K^2(t)dt - \int_{25мс}^{80} p_R^2(t)dt}{\int_0^{25мс} p_K^2(t)dt + \int_{25мс}^{80} p_R^2(t)dt},$$

где p_K^2 – квадрат звукового давления, измеренного микрофоном с круговой диаграммой направленности, p_R^2 – квадрат звукового давления, измеренного однонаправленным микрофоном, ориентированным на источник звука.

Оптимальное значение индекса пространственного впечатления составляет 2–6 дБ [6].

Теплота субъективно воспринимается как «звучность» низких частот по сравнению со средними. Данная характеристика тембра оценивается через КНТ (коэффициент низкого тона), для определения которого необходимо измерить время реверберации на нескольких частотах [1]:

$$\text{КНТ} = \frac{T_{125}+T_{250}}{T_{500}+T_{1000}},$$

где T_X – время реверберации на частоте X Гц

В лучших концертных залах величина КНТ составляет 1,08..1.10, т. е. время реверберации возрастает на более низких частотах [1].

По аналогии с КНТ в [5] предложен КВТ (коэффициент высокого тона) как ещё один показатель оценки влияния помещения на тембр звука:

$$\text{КВТ} = \frac{T_{2000}+T_{4000}}{T_{500}+T_{1000}}.$$

Существенную роль для оценки акустического качества помещений играет такой субъективный критерий как разборчивость речи – т. е. степень, в которой речь может быть понята слушателями.

Метод оценки потери артикуляции позволяет оценить разборчивость речи. При увеличении времени реверберации и расстояния от источника звука до слушателя будет снижаться доля правильно принятых согласных Al_{cons}, что будет соответствовать снижению разборчивости речи [4]:

$$Al_{cons} \approx 0{,}652 \left(\frac{r_{LH}}{r_R}\right)^2 T\ \%,$$

где r_R – радиус гулкости – критическое расстояние, на котором энергия прямого звука равна энергии отражений, r_{LH} – расстояние от источника до слушателя, T – время стандартной реверберации.

Величина Al_{cons} менее 12 % соответствует хорошей разборчивости речи [4].

Группа методов расчёта индекса передачи речи STI (*Speech Transmission Index*) основана на измерении модуляционной передаточной функции MTF (*Modulation Transfer Function*) и рассматривает речевой сигнал как широкополосный, модулированный низкочастотным сигналом. При этом скорость модуляции соответствует произнесению человеком формант, т. е. артикуляции. При наложении шумов и отражений снижается глубина модуляции, что субъективно воспринимается как ухудшение разборчивости речи.

Измерения проводятся на наборе полос широкополосного сигнала, и наборе частот узкополосного. Коэффициент *m* характеризует глубину модуляции [7]:

$$m(F) = \frac{1}{\sqrt{\left[1+\left(\frac{2\pi FT}{13{,}8}\right)^2\right]}} \cdot \frac{1}{1+10^{-\left(\frac{(S/N)}{10\text{дБ}}\right)}},$$

где *F* – частота модуляции, *T* – время реверберации, *S/N* – отношение сигнал-шум, дБ.

STI рассчитывается путем усреднения и взвешивания полученных значений *m(F)* в соответствии с вкладом каждой частотной полосы, его значения от 0,6 до 1 соответствуют хорошей разборчивости речи [7].

Различные объективно измеряемые параметры оценки акустического качества помещений поставлены в соответствие с субъективными критериями, которые дополняют друг друга, а иногда и противопоставляются. В таблице приведены субъективные критерии оценки акустического качества помещений, объективные параметры и измеряемые величины (отмечены знаком «+»), важно отметить что объем данной статьи позволяет рассмотреть лишь часть существующих методов оценки.

ТАБЛИЦА. Субъективные критерии оценки акустического качества помещений, соответствующие им объективные параметры и измеряемые величины

Субъективный критерий	Объективный параметр	Время реверберации	Энергия отзвука	Уровень боковых отражений
Жизненность	Время реверберации	+		
	Мера гулкости		+	
Различимость	Центральное время		+	
	Мера четкости		+	
Пространственность	Индекс пространственного впечатления			+
Тембр	Коэффициент низкого тона	+		
	Коэффициент высокого тона	+		
Разборчивость речи	Потери артикуляции согласных	+		
	Индекс передачи речи	+		

Как видно, оценка акустических свойств помещения определяется различными характеристиками отражений звука. Величина времени

реверберации непосредственно влияет на многие критерии, в том числе на разборчивость речи. Однако, другие параметры, основанные на измерении свойств прямого и отраженных звуков, позволяют составить более детальное представление о качестве звучания.

Исследователями определены оптимальные величины объективно измеряемых параметров, но не проведено работы по их объединению, по определению величины вклада каждого из них в оценку качества. Т. е. при оценке вклада акустического качества помещения в качество звучания сигнала можно провести ряд измерений по предложенным методам объективной оценки, но определение того, какой из параметров будет играть первоочередную роль до настоящего времени остаётся за исследователем.

Целесообразно дальнейшее выявление влияния каждого объективно измеряемого параметра акустики помещений для вынесения единой интегральной объективной оценки акустического качества звуковых сигналов, соответствующей результатам субъективных экспертиз.

Список используемых источников

1. Приттс Р., Алдошина И. А. Музыкальная акустика : учебник для высших учебных заведений. СПб. : Композитор–Санкт-Петербург, 2014. 720 с. ISBN 978-5-7379-0298-8.

2. ГОСТ Р ИСО 3382-1-2013. Акустика. Измерение акустических параметров помещений. Часть 1. Зрительные залы. М. : Стандартинформ, 2014.

3. ISO. 2009. ISO 3382-1:2009(E). Acoustics – Measurement of room acoustic parameters. Part 1: Perfomance spaces. Geneva : 2009.

4. Анерт В. и Стеффен Ф. Техника звукоусиления. М. : ЭРА, Леруша, 2003. 416 с. ISBN 5-901-138-06-6.

5. Handbook of Acoustics. [ред.] Thomas D. Rossing. New York : Springer, 2007. e-ISBN 0-387-30425-0.

6. Анерт В. и Райхардт В. Основы техники звукоусиления. М. : Радио и связь, 1984. 320 с.

7. Ковалгин Ю. А., Свиньина О. А., Фадеев А. А. Расчет аппаратно-студийных комплексов телерадиовещания и аудиотехники. Ч.2. Расчёт систем озвучения и звукоусиления: методические указания по курсовому и дипломному проектированию. 2016.

Статья представлена научным руководителем, кандидатом технических наук, доцентом А. А. Фадеевым.

ИНФОКОММУНИКАЦИОННЫЕ СЕТИ И СИСТЕМЫ

УДК 621.398

M2M РЕШЕНИЕ ДЛЯ ЭКОЛОГИЧЕСКОГО МОНИТОРИНГА ОКРУЖАЮЩЕЙ СРЕДЫ

М. В. Авраменко, В. Ю. Гойхман

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

Технологии IoT (Internet of Things, Интернет Вещей), такие как межмашинное взаимодействие (M2M, Machine-to-Machine), уже используются с целью улучшения состояния окружающей среды, например, для переработки нефти, сокращения выбросов CO2, контроля шумового загрязнения, очистки сточных вод. Поэтому – разработка M2M решения для экологического мониторинга окружающей среды является актуальной задачей.

m2m, интернет вещей, mqtt, http, трафик.

Введение

Благодаря своевременной конвергенции различных технологий в настоящее время существует возможность подключиться и взаимодействовать с любыми устройствами имеющими доступ в сеть интернет, в любое время и в любом месте. Согласно обзору исследовательской компанией Garthner (*Gartner's 2015 Hype Cycle for Emerging Technologies*) [1] среди 2 тыс. технологий как одна из наиболее востребованных, позволяющих получить хорошую обратную связь от современного потребителя, значительно улучшить качество существующих продуктов и сервисов.

В ряде работ профессоров М. А. Шнепс-Шнеппе, Б. С. Гольдштейна, А. Е. Кучерявого и некоторых других авторов исследованы вопросы спецификации и структуры технологий интернета вещей и межмашинного взаимодействия, где авторы подчеркивают большую значимость и развитие этих технологий в будущем [2, 3, 4, 5].

Разрабатываемый проект нацелен решить задачи мониторинга окружающей среды, а также иметь минимальную сложность интеграции устройств и отображать данные от датчиков с любых устройств в режиме реального времени. Для исследования трафика, порождаемого сенсорными узлами необходимо создать макет устройства, реализовав M2M сеть.

Метод решения

Разрабатываемая в рамках проекта сеть M2M представлена на рисунке 1. Устройство организует пакетную передачу данных о качестве воздуха и атмосферных показателях через ССОП (*Public Internet*) и отправляет информацию на веб-сервере, где собирается и отражается информация, собранная со всех датчиков. Пользователь через устройство, имеющее возможность выхода в сеть Интернет, получает доступ к сервису и производит мониторинг необходимой информации.

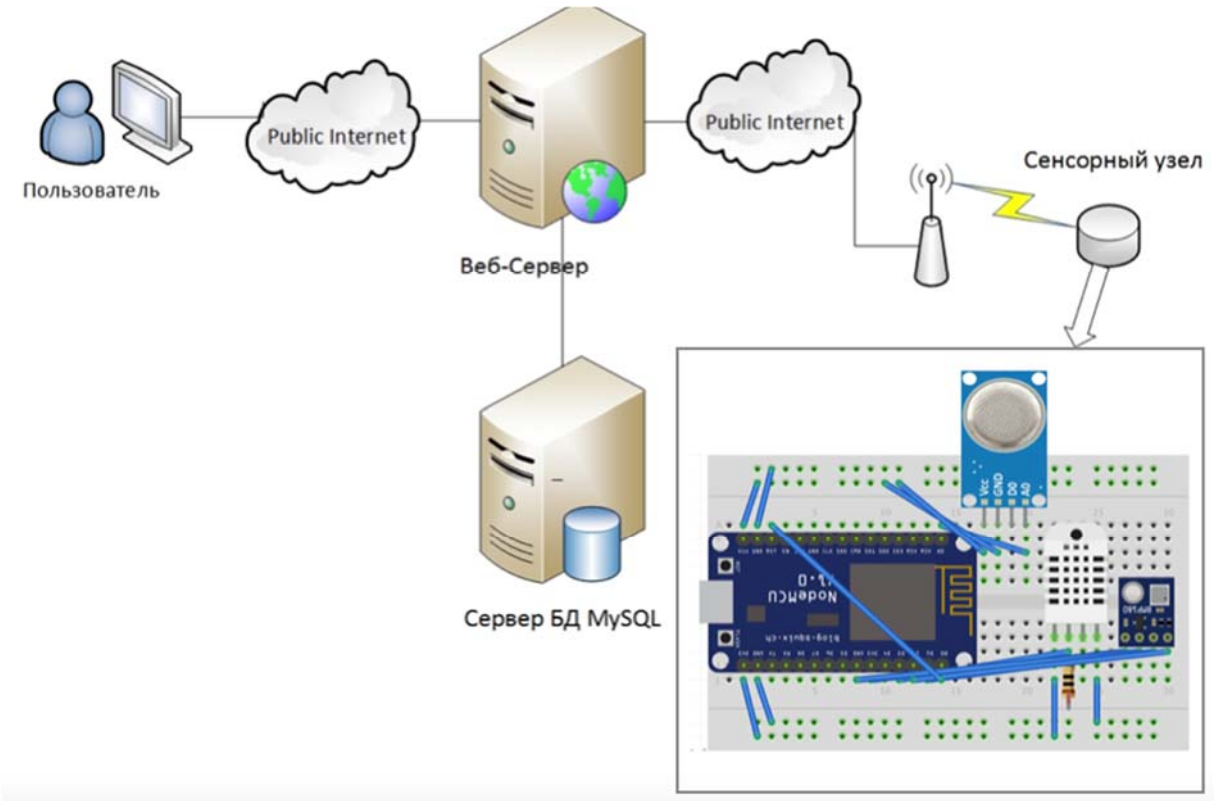


Рис. 1. Схема разработанной M2M-сети

Были разработаны поэтапно следующие блоки:

– *сервер* под управлением операционной системы Debian 7, который обеспечивает соединение с передающим устройством, обрабатывает полученные данные и сохраняет необходимую информацию в БД, для реализации веб-сервера был выбран Apache 2;

– *база данных* для хранения информации о пользователях, устройствах и информации, переданной с зарегистрированных в системе объектах. За основу для хранения всех сведений и информации была выбрана реляционная система управления базами данных – MySQL;

– *web-приложение*, которое визуализирует необходимую информацию для пользователя. Для реализации приложения использовались технологии PHP, HTML, CSS (CSS3), API Яндекс Карты;

– *макетная плата* для анализа и подбора элементов для будущего устройства, состоящая из:

1. Датчика температуры и влажности DHT22.
2. Датчика давления BMP180.
3. Датчика качества воздуха MQ-135.
4. Wi-FI модуля ESP8266 ESP-12.
5. Аккумуляторный блок для автономной работы устройства на 9V с DC-DC преобразователем на 3.3V.

Анализ результатов и исследование трафика

В ходе опытного тестирования будет осуществлён подбор подходящих датчиков разных модификаций. Wi-Fi модуль ESP8266, модификации ESP-12 помимо PCB антенны имеет микроконтроллер с flash памятью 512 кб для загрузки программы. Модуль может работать при температуре от –40 до +125 градусов, что является несомненным плюсом для реализации в будущем устройстве. В модуле реализован TCP/IP стек, позволяющий использовать для передачи данных на удаленный сервер любой протокол, работающий поверх транспортного уровня. Для тестирования были выбраны протоколы: HTTP и MQTT.

HTTP – символьно-ориентированный клиент-серверный протокол. Каждое HTTP-сообщение состоит из трёх частей рис.4, которые передаются в указанном порядке. При передаче информации от датчиков ESP8266 формирует HTTP:POST запрос, в теле которого содержаться переменные с присвоенными параметрами: температуры, влажности, давления и качества воздуха.

После получения данных от устройства сервер при помощи скрипта на языке PHP обрабатывает и отправляет запрос SQL:INSERT INTO{} о внесении значений от датчиков в базу данных MySQL в соответствующую таблицу. После записи значений в БД, сервер отправляет сообщение на устройство HTTP:200 OK, обозначающее успешную отправку данных. Приняв сообщение 200 OK, через некоторое время устройство повторяет процедуру.

MQTT (*Message Queue Telemetry Transport*) [6] представляет протокол обмена сообщениями publish/subscribe (издатель-подписчик), как следует из названия этого протокола, основное его назначение – телеметрия, или дистанционный мониторинг. Клиенты (устройства), подключаются к брокеру, посылая и отправляя данные только ему. Брокер – это приложение, выполняющее функции TCP сервера с динамической базой данных. Каждый клиент MQTT обязан иметь уникальный идентификатор ClientId, представленный UTF-8 строкой.

«Издатель» (*Pub, Publisher*) «публикует» данные и метаинформацию (формирует описанные метаинформацией «каналы»), «подписчик» (*Sub,*

Subscriber) «подписывается» на «каналы», определённые метаинформацией. Транспортируемые данные и метаинформация, формирующая «каналы» транспорта, создаются из фрагментов, имеющих название топиков (*topic*), создающиеся при помощи специальной иерархии. Иерархия формируется соединением топиков с помощью символа «/», например строка:

city1/room_1/temperature.

Сценарий обмена сообщениями по протоколу MQTT показан на рисунке 2.

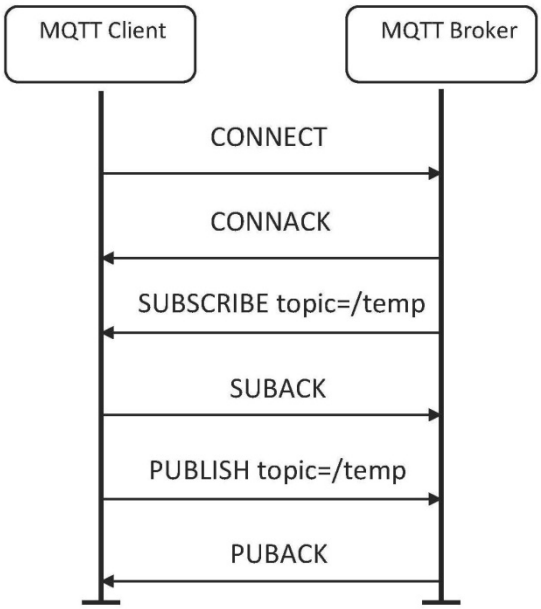


Рис. 2. Сценарий обмена сообщениями по протоколу MQTT

Так как устройства в сети обмениваются с сервером малой по объёму информацией, около 90 байт, и между устройством и точкой доступа предполагаются кратковременные разрывы, то для построения сети был выбран протокол MQTT.

Для исследования трафика, порождаемого сенсорным узлом, был снят дамп анализатором сетевого трафика Wireshark. Трафик межмашинных коммуникаций представляет собой поток данных, пакетов в сети передачи данных. Основное отличие данного трафика от трафика H2M (Человек-Машина) или H2H (Человек-Человек) в том, что инициаторам передачи данных является некоторое устройство, поэтому свойства трафика межмашинных коммуникаций зависят от алгоритмов их работы [7]. На рисунке 3 представлен график, построенный по результатам захвата пакетов, переданных по протоколу MQTT от макета сенсорного узла. На графике видно, что трафик является неравномерным. Неравномерность трафика характеризуется методом работы устройства и предполагает, что сенсорный узел отправляет пакеты после выхода из спящего режима и подключения к точке доступа.

Со случайным трафиком работать гораздо сложнее, чем с постоянным, так как он непредсказуем и оказывает влияние на качество обслуживания трафика других услуг связи.

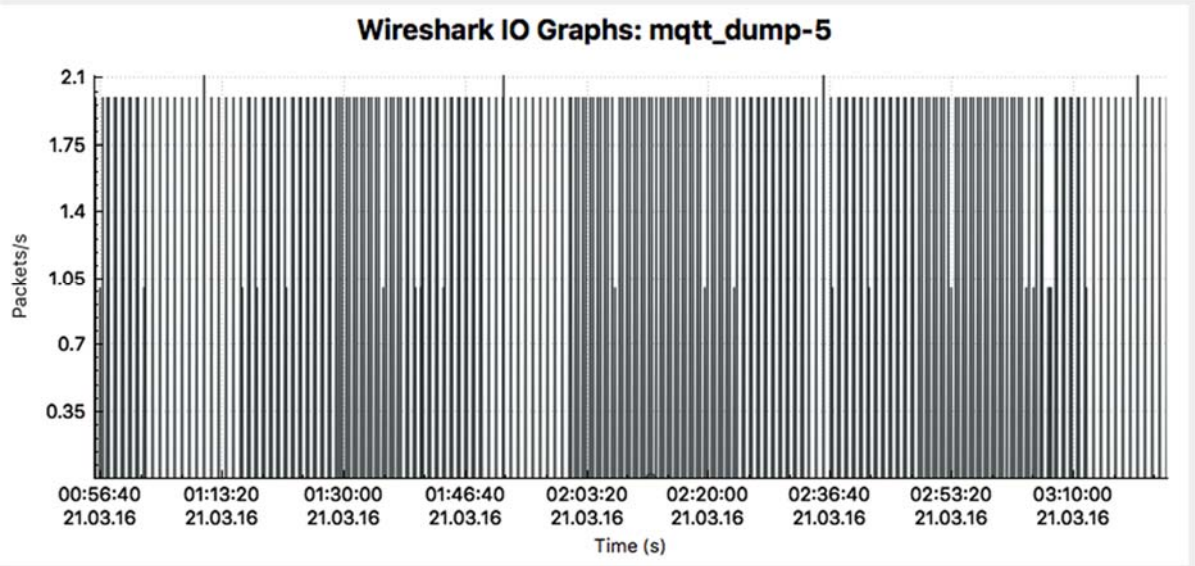


Рис. 3. Трафик от сенсорного узла по протоколу MQTT

Выводном данной работы является то что, цель исследования достигнута. Проведен предварительный анализ для будущего проекта: подбор элементов для устройства и протокола межмашинных коммуникаций. Анализ полученного трафика от сенсорных узлов - это тема для будущей работы.

Список используемых источников

1. Gartner's 2015 Hype Cycle for Emerging Technologies Identifies the Computing Innovations That Organizations Should Monitor. URL: http://www.gartner.com/newsroom/id/3114217 (дата обращения 22.03.2016).

2. Бондарик В. Н., Кучерявый А. Е. Прогнозирование развития Интернета Вещей на горизонте планирования до 2030 года // Труды МФТИ. 2013. Том 5. No 3, С. 92–96.

3. Гольдштейн Б. С., Кучерявый А. Е. Сети связи пост-NGN. СПб. : БХВ-Петербург, 2013. 160 с. ISBN 978-5-9775-0900-8.

4. Намиот Д. Е, Шнепс-Шнеппе М. А. О международной стандартизации M2M коммуникаций // T-Comm - Телекоммуникации и Транспорт. 2014. Т. 8. № 12. С. 62–67.

5. Stryjak J., Sharma A. Analysis Agricultural machine-to-machine (Agri M2M): a platform for expansion // GSMA. 2015. PP. 10–47.

6. MQ Telemetry Transport (MQTT) V3.1 Protocol. OASIS Specification, 2015. URL: http://mqtt.org/documentation (дата обращения 22.03.2016).

7. Shafig M. Z. and all. A First Look at Cellular Machine-to-Machine Traffic: Large Scale Measurement and Characterization // 12th ACM Sigmetrics / Performance International Conference. June 11–15, London, England, UK, 2012. pp. 65–76.

УДК 004.056.53

ИССЛЕДОВАНИЕ АЛГОРИТМА ЗАЩИТЫ ОБЩЕДОСТУПНЫХ ПЕРСОНАЛЬНЫХ ДАННЫХ В ИНФОРМАЦИОННЫХ СИСТЕМАХ

В. И. Андрианов, Л. А. Виткова, Д. В. Сахаров

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

В статье исследуется алгоритм защиты общедоступных персональных данных, основанный на внедрении самомодифицирующегося кода в графические изображения и внедрении ЦВЗ. Анализируются существующие решения и методы, которые применяются в рамках мониторинга, поиска и защиты графических изображений и файлов в информационных системах. Использование общедоступных персональных данных приводит к новым постановкам задач в области проектирования комплексных систем защиты общедоступных персональных данных в информационных системах.

общедоступные персональные данные, информационные системы, графические изображения, фотография, самомодифицирующийся код, мониторинг, стеганография.

Введение

Новая среда обитания массовых коммуникаций активно формирует потребность в новых способах программной защиты граждан. Требует реализации новых алгоритмов, направленных на решение вопросов информационной безопасности, возникающих в информационной сфере жизни общества, государства и личности.

Согласно терминам и определениям, расшифрованным в Федеральном законе от 27.07.2006 N 152-ФЗ «О персональных данных» [1], персональные данные – это любая информация, относящаяся к прямо или косвенно определенному, или определяемому физическому лицу (субъекту персональных данных). При этом под обработкой персональных данных понимается любое действие (операция) или совокупность действий (операций), совершаемых с использованием средств автоматизации или без использования таких средств с персональными данными, включая сбор, запись, систематизацию, накопление, хранение, уточнение (обновление, изменение), извлечение, использование, передачу (распространение, предоставление, доступ), обезличивание, блокирование, удаление, уничтожение персональных данных.

Также под информационной системой персональных данных законодатель понимает совокупность содержащихся в базах данных персональных данных и обеспечивающих их обработку информационных технологий и технических средств, а под понятием оператор – государственный орган, муниципальный орган, юридическое или физическое лицо, самостоятельно или совместно с другими лицами организующие и (или) осуществляющие

обработку персональных данных, а также определяющие цели обработки персональных данных, состав персональных данных, подлежащих обработке, действия (операции), совершаемые с персональными данным.

При этом анализ судебной практики по общедоступным персональным данным показывает, что защищать собственные интересы гражданам Российской Федерации чаще всего приходится уже в суде, а проактивных мер защиты на сегодня не существует.

Анализ

Рассмотрим данные по делу № 1-96/2015, приговор № 1-96/2015 от 6 мая 2015 г. [2]. Гражданин Асакаев Р. А. в январе 2015 года, зарегистрированный под именем «Фаир-Авердун», на сайте под названием «В Контакте» в группе под названием «Курицы Махачкалы» (htpp://vk.com/kury05), выложил фотографии для всеобщего обозрения с целью хищения чужого имущества путем вымогательства под угрозой дальнейшего распространения вышеуказанной информации, 29.01.2015 г. потребовал от ФИО1, представившейся под именем «Barbie», перевода денежных средств в сумме 10 000 рублей за удаление фотографий на счет электронного кошелька «Вебмани» №, которые были переведены последней на указанный адрес. Всего в деле фигурирует более 10 пострадавших, и в деле указаны только те, кто заявил о противоправном деянии.

Другой пример – решение № М-5453/2013 2-7287/2013 2-7287/2013~М-5453/2013 от 18 ноября 2013 г. [3]. Гражданка Одинцова М. Н. обратилась с иском к НП «Общество защиты бездомных животных» и Уваркиной С. В. о взыскании компенсации морального вреда с каждого из ответчиков, указав в обоснование требований на то, что в сети Интернет на сайте социальной сети ответчиками размещены сообщения, содержащие высказывания о ней в оскорбительной форме с использованием, без согласия, её фотографии.

Однако если внимательно познакомится с пользовательским соглашением социальных сетей, которое по Гражданскому Кодексу РФ имеет силу присоединения, мы видим следующее: Сайт ВКонтакте – это интернет-ресурс, состоящий из совокупности: а) программ для ЭВМ (программных кодов, исполняющихся на ЭВМ); и б) информации (Контента), размещенной в них Администрацией и/или Пользователями. Сайт ВКонтакте содержится в информационной системе, обеспечивающей доступность такой информации в сети Интернет. В п.п. 7.1.3. сказано, что пользователь, размещая на Сайте принадлежащий ему на законных основаниях Контент, предоставляет другим пользователям неисключительное право на его использование путем просмотра, воспроизведения (в том числе копирования) и иные права исключительно с целью личного некоммерческого использования, кроме случаев, когда такое использование причиняет или может причинить вред охраняемым законом интересам правообладателя [4]. Социальная сеть ВК

взята для анализа, как наиболее популярная социальная сеть в РФ по данным TNS [5].

Обратим внимание на п.п. 7.1.3., можем ли мы трактовать пункт пользовательского соглашения следующим образом?: «Пользователь, загружая свои фотографии, предоставляет другим пользователям неисключительное право на его использование». Фотография, как и иное графическое изображение, есть ни что иное, как контент, графическое изображение. Следовательно, ответ скорее – да можем.

Дальнейший анализ пользовательского соглашения показывает, что пользователь может защитить свои изображения. Так, например, в п.п. 7.1.4. сказано, что использование Пользователем Контента, доступ к которому получен исключительно для личного некоммерческого использования, допускается при условии сохранения всех знаков авторства (копирайтов) или других уведомлений об авторстве, сохранения имени автора в неизменном виде, сохранении произведения в неизменном виде.

Знак охраны авторского права представляет собой латинскую литеру «*C*» (первая буква слова «*copyright*»), помещённую в центре окружности.

Наличие или отсутствие знака охраны авторского права наличие знака является определяющим для предоставления защиты авторских прав, в соответствии с п. 1 ст. III указанной конвенции в редакции 24.07.1971 г. [6].

При этом знак охраны авторского права технически возможно обрезать, удалить с графического изображения, и он не позволяет отслеживать пути копирования и распространения файла. Более высокой степенью защиты может являться цифровой водяной знак. Но ни первый способ защиты, ни второй не позволяют нам реализовать мониторинг – отслеживание факта копирования и публикации фотографии.

Синтез

Рассмотрим два варианта мониторинга графических изображений (фотографий) в социальных сетях.

Первый, т. н. активный. Прежде всего, потребуется внедрение самомодифицируещегося кода, что позволит своевременно отслеживать факт копирования и незаконных публикаций фотографий. В этом случае мы сталкиваемся с несколькими проблемами:

Во-первых, ни один оператор распространения информации (информационная система) согласно требованиям, указанным в договоре оферте не позволяет использовать сторонний код, внедряемый в контент пользователя, без ведома и без участия оператора. Таким образом, прежде чем реализовать данный проект, нам потребуется не только и не столько программный продукт, сколько официальное декларирование его допуска для контроля операторов информационных систем. При этом если копия фотографии будет размещена в пределах зарегистрированной информационной

системы, код сможет получить обратную связь, а если фотография будет размещена на обычном сайте? По данным регистратора домена только в RU зоне по состоянию на февраль 2016 г. зарегистрировано более 5 000 000 доменов [7].

Во-вторых, сама фотография, согласно договору оферты с социальной сетью ВК – это графическое изображение. Для защиты согласно требованиям того же положения автор может использовать знак авторского права. Гражданский кодекс Российской Федерации гарантирует судебную защиту. Решение об удовлетворении иска выносится судом. При этом заявитель обязан доказывать факт распространения графического изображения лицом, к которому предъявлен иск, и факт нарушения ответчиком. Отсутствие знака охраны авторского права на графическом изображении позволяет ответчикам избегать ответственности. Фактически единственным способом защиты графических изображений в информационных системах становится ЦВЗ, как наиболее устойчивый к модификации способ защиты графического изображения.

И второй вариант мониторинга – пассивный. Существует несколько вариантов реализации совместного алгоритма поиска и мониторинга через информационно-поисковые системы yandex.ru и vk.com. При этом существуют реализованные успешные программы мониторинга графических файлов и текста, анализаторы связей в социальных сетях, например, Social Network Analysis in Sentinel Visualizer.

Все многообразие моделей традиционного информационного поиска (IR) принято делить на три вида:

1) теоретико-множественные (булевская, нечетких множеств, расширенная булевская);

2) алгебраические (векторная, обобщенная векторная, латентно-семантическая, нейросетевая);

3) вероятностные.

Булевское семейство моделей, по сути, – первое, приходящее на ум программисту, реализующему полнотекстовый поиск. Есть метка – документ считается найденным, нет – не найденным. Собственно, классическая булевская модель – это мостик, связывающий теорию информационного поиска с теорией поиска и манипулирования данными.

Исследование поиска похожих изображений, показывает, что он реализуется несколькими путями

1) Алгоритм индексирования: Каждому изображению ставится в соответствие некоторый вектор фиксированной длины. Эти вектора задают пространство индексов.

2) Сравнение форм: предлагаемый алгоритм выделения характеристик формы представлен следующим образом:

для каждого изображения выполняется:

а) вейвлет-декомпозиция;

б) вычисление нормализованных центральных моментов на всех масштабах и сохранение их в виде характеристик формы в базе данных.

3) Сравнение текстур: при выделении характеристик текстуры, для каждого изображения выполняется следующее:

а) вейвлет-декомпозиция;

б) вычисление обобщенных Гауссовых плотностей параметров и сохранение их как текстурных характеристик в базе данных.

4) Совместный анализ формы и текстуры.

Выводы

Таким образом, для защиты общедоступных персональных данным, а именно графических изображений, требуется реализовать алгоритм защиты графических изображений.

Вероятно, для реализации потребуются:

1) Цифровой водяной знак (ЦВЗ) – это специальная метка, незаметно внедряемая в контейнер (которым может выступать как изображение, видео или аудио, так и приложение) с целью тем или иным образом контролировать его использование.

2) Программа мониторинга сети Интернет на предмет появления копий (пассивная защита)

3) Программа слежения за контейнером, с возможностью защиты от копирования и модификации.

Список использованных источников

1. О персональных данных: федер. закон Рос. Федерации от 27.07.2006 № 152-ФЗ (ред. от 21.07.2014): принят Гос. Думой Федер. Собр. Рос. Федерации 8 июля 2006 г.: одобр. Советом Федерации Федер. Собр. Рос. Федерации 14 июля 2006 г. // Российская Федерация. Собрание законодательства РФ. 31.07.2006. N 31 (1 ч.). Ст. 3451.

2. Приговор № 1-96/2015 от 6 мая 2015 г. по делу № 1-96/2015 / Хасавюртовский городской суд (Республика Дагестан). URL: http://sudact.ru/regular/doc/KWaHTTfQfcLw/ (дата обращения 16.04.2016).

3. Решение № М-5453/2013 2-7287/2013 2-7287/2013~М-5453/2013 от 18 ноября 2013 г. / Сыктывкарский городской суд (Республика Коми). URL: http://sudact.ru/regular/doc/1x1pORtGPRm5/ (дата обращения 16.04.2016).

4. Правила пользования Сайтом ВКонтакте. URL: http://vk.com/terms (дата обращения 16.04.2016).

5. Топ-20 интернет-проектов Февраль 2016, Россия 0+, 12-64 лет URL: http://tns-global.ru/services/media/media-audience/dannye_issledovaniy_auditorii_smi/ (дата обращения 16.04.2016).

6. Всемирная конвенция об авторском праве от 06.09.1952 г. (пересмотренная в париже 24.07.71 г.) URL: http://www.copyright.ru/ru/library/megdunarodnie_akti/ copyright/vsemirnaya_konventsiya_avtorskom_prave/ (дата обращения 16.04.2016).

7. Статистика доменных имен за февраль 2016 г. URL: https://cctld.ru/files/stats/2016_feb.jpg (дата обращения 16.04.2016).

УДК 004.056.52

МОДЕЛИРОВАНИЕ НЕПОДСМАТРИВАЕМОГО ГРАФИЧЕСКОГО ПАРОЛЯ НА ОСНОВЕ ИСПОЛЬЗОВАНИ КОДА РИДА-СОЛОМОНА И ИССЛЕДОВАНИЕ ЕГО ХАРАКТЕРИСТИК

В. В. Архипов, В. А. Яковлев

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

Предлагается новый подход к построению таблицы сопоставления парольному символу подмножества вводных символов для парольных систем, устойчивых к атакам подсматривания на основе кода Рида-Соломона. Получены оценки стойкости системы паролирования к различным видам атак.

аутентификация, паролирование, графический пароль, атака подсматривания, неподсматриваемый пароль.

Суть НГП в том, чтобы в явном виде не указывать на парольный символ, поэтому для прохождения процедуры аутентификации пользователь указывает на вводные символы. Вводные символы образуются путем сопоставления парольному символу подмножества вводных символов. Пользователь узнает вводные символы только во время прохождения процедуры аутентификации, а после прохождения аутентификации вводные символы не представляют для него никакой ценности.

Как было отмечено ранее в [1] многие НГП можно представить в виде таблиц соответствия между парольными и вводными символами. Такая таблица имеет следующие параметры: N – кол-во парольных символов; $\boldsymbol{k}$ – кол-во вводных символов для 1 парольного; s_0 – минимальное кол-во повторений 1 символа ввода; $\widetilde{V}$ – множество вводных символов. Для увеличения стойкости к подсматриваниям таблица 1-ой аутентификации должна частично пересекаться с таблицей 2-ой аутентификации. За такое пересечение таблиц отвечает параметр s_0 – повторения символов. Задача состоит в выборе параметров таблицы соответствия, обеспечивающих наибольшую устойчивость к атакам.

Предлагается подход к построению таблицы сопоставления парольному символу подмножества вводных символов, на основе кода Рида-Соломона с параметрами [2]: q – основание кода; k – длина информационной последовательности; n – длина кода.

С помощью кода Рида-Соломона можно построить таблицы соответствия 2-мя способами:

а) случайный выбор. Из таблицы кода РС случайно выбирается N столбцов. Для каждого столбца выбирается случайно K строк. На рисунке 1 показан пример построения таблицы соответствия при $N = 10$, $K = 3$.

N	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21	22	23	24	25
C	0	1	2	3	4	1	2	3	4	0	2	3	4	0	1	3	4	0	1	2	4	0	1	2	3
	0	1	2	3	4	3	4	0	1	2	1	2	3	4	0	4	0	1	2	3	2	3	4	0	1
	0	1	2	3	4	4	0	1	2	3	3	4	0	1	2	2	3	4	0	1	1	2	3	4	0
	0	1	2	3	4	2	3	4	0	1	4	0	1	2	3	1	2	3	4	0	3	4	0	1	2

Рис. 1. Построение таблицы соответствия при $N = 10$, $K = 3$, случайный выбор

б) последовательный выбор. В таблице кода РС случайно выбирается столбец и строка. Начиная от выбранного столбца, последовательно берутся другие N–1 столбцов. Начиная от выбранной строки, последовательно берутся другие K–1 строк. На рисунке 2 показан пример построения таблицы соответствия при $N = 10$, $K = 3$.

N	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21	22	23	24	25
C	0	1	2	3	4	1	2	3	4	0	2	3	4	0	1	3	4	0	1	2	4	0	1	2	3
	0	1	2	3	4	3	4	0	1	2	1	2	3	4	0	4	0	1	2	3	2	3	4	0	1
	0	1	2	3	4	4	0	1	2	3	3	4	0	1	2	2	3	4	0	1	1	2	3	4	0
	0	1	2	3	4	2	3	4	0	1	4	0	1	2	3	1	2	3	4	0	3	4	0	1	2

Рис. 2. Построение таблицы соответствия при $N = 10$, $K = 3$, последовательный выбор

Основные виды атак на НГП:

1) *Атака подсматривания.* Злоумышленник имеет данные верной процедуры прохождения аутентификации: таблицу соответствия и вводный символ. Проанализировав эти данные, злоумышленник отбрасывает не подходящие парольные символы, что приводит к уменьшению множества возможных парольных символов. Поэтому злоумышленник не может однозначно указать, какой символ является парольным. Далее нарушитель может сделать атаку угадывания или подбора, чтобы пройти процедуру аутентификации.

После подсматривания ввода пароля злоумышленник не может однозначно указать, какой символ является парольным.

2) *Атака угадывания.* Злоумышленник пытается угадать парольный символ. Средняя вероятность угадывания парольного символа для i-го подсматривания можно записать [1]:

$$P_{\text{уг}}^{i} = \sum_{j=1}^{S_0} \frac{P(S_i)}{j}.$$

3) *Атака подбора*. Злоумышленник пытается пройти процедуру аутентификации после анализа таблиц соответствия путем ввода, наиболее часто встречаемых, вводных символов.

Выражения для вероятности подбора можно записать так [1]:

$$P_{\text{подб}}(S_i = j) = \sum_{m=1}^{N_t} \sum_{t=1}^{j} P_{conf}(m,t) \cdot \frac{t}{j},$$

где $P_{conf}(m,t)$ – вероятность m-ой конфигурации веса t; N_t – количество конфигураций веса t; $\frac{t}{j}$ – вероятность подбора для конфигурации веса t.

Под конфигурацией веса t мы понимаем расположение t блоков, среди j блоков, содержащих максимально повторяющийся вводный символ.

Аналитическое выражение для нахождения $P_{conf}(m,t)$ очень громоздко и зависит от способа построения таблицы ввода. Поэтому для вычисления $P_{conf}(m,t)$ будем использовать имитационное моделирование.

На рисунке 3 представлены графики вероятностей подбора при случайном выборе строк и столбцов для разных кодов РС.

На рисунке 4 представлены графики вероятностей подбора при последовательном выборе строк и столбцов для разных кодов РС.

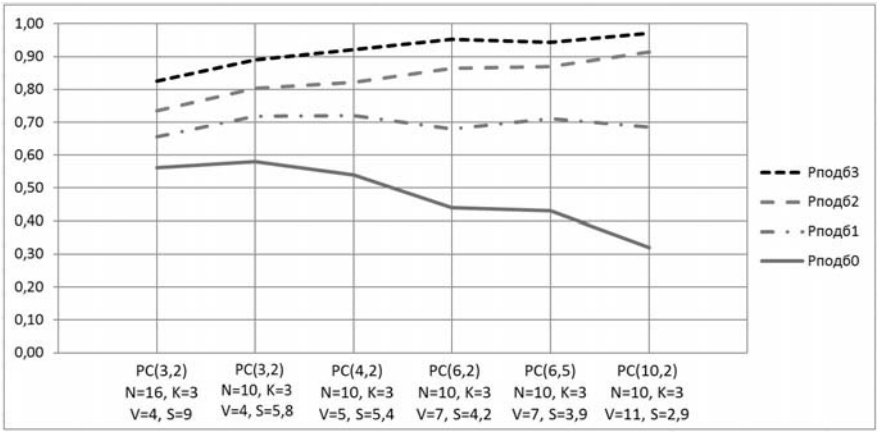


Рис. 3. Графики вероятностей подбора при случайном выборе строк и столбцов из таблицы кодов РС

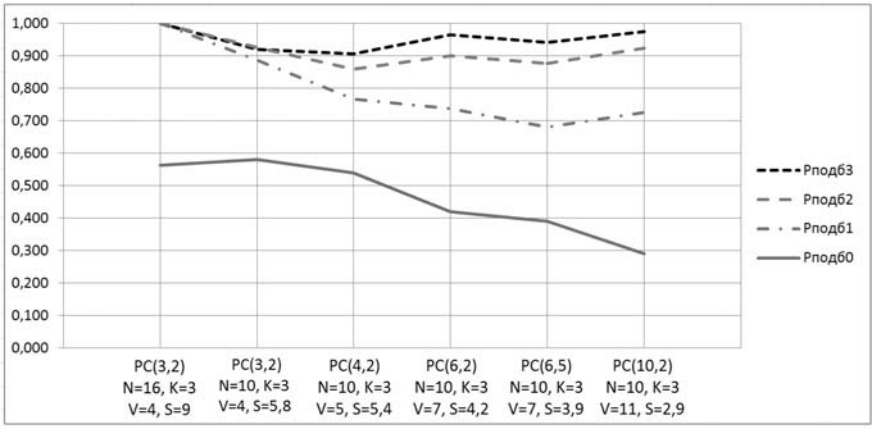


Рис. 4. Графики вероятностей подбора при последовательном выборе строк и столбцов для разных кодов РС

В таблице 1 представлены вероятности подбора для таблиц соответствия на основе кода РС и для таблиц построенных случайным образом.

Из таблицы видно, что использование кода Рида-Соломона для построения таблиц соответствия дает небольшое улучшение стойкости к атакам взлома. При выборе определнных параметров кода РС вероятность подбора уменьшается.

ТАБЛИЦА 1. Вероятности подбора

	Таблица соответствия посроенных случайным образом		Таблица соответствия на основе кодов РС (случайный выбор)		Таблица соответствия на основе кодов РС (последовательный выбор)	
	N=10, K=3, V=10, S=3	N=10, K=3, V=7, S=4	PC(10,2) N=10, K=3, V=11, S=2,9	PC(6,5) N=10, K=3, V=7, S=3,9	PC(10,2) N=10, K=3, V=11, S=2,9	PC(6,5) N=10, K=3, V=7, S=3,9
$P_{подб(0)}$	0,3	0,4	0,32	0,43	0,29	0,39
$P_{подб(1)}$	0,63	0,76	0,68	0,71	0,72	0,68
$P_{подб(2)}$	0,86	0,81	0,91	0,87	0,92	0,88

Список используемых источников

1. Архипов В.В., Яковлев В. А. Обобщенная модель неподсматриваемого графического пароля // Актуальные проблемы инфотелекоммуникаций в науке и образовании. V Международная научно-техническая и научно-методическая конференция, Санкт-Петербург, СПбГУТ, 10–11 марта 2016 г. С. 230–236.

2. Питерсон У., Уэлдон Э. Коды исправляющие ошибки. М. : Мир, 1976. 593 с.

УДК 621.377

МОДЕЛЬ НАРУШИТЕЛЯ РАСПРЕДЕЛЕННОЙ ИНФОРМАЦИОННО-ВЫЧИСЛИТЕЛЬНОЙ СЕТИ

Э. В. Бирих[1], Д. В. Сахаров[2]

[1]Управление Роскомнадзора по Северо-Западному федеральному округу
[2]Санкт-Петербургский государственный университет телекоммуникаций им. проф. М. А. Бонч-Бруевича

Модель нарушителя – (в информатике) абстрактное (формализованное или неформализованное) описание нарушителя правил разграничения доступа. Модель нарушителя определяет: категории (типы) нарушителей, которые могут воздействовать на объект; цели, которые могут преследовать нарушители каждой категории, возможный количественный состав, используемые инструменты, принадлежности, осна-

щение, оружие и проч.; типовые сценарии возможных действий нарушителей, описывающие последовательность (алгоритм) действий групп и отдельных нарушителей, способы их действий на каждом этапе.

защита информации, модель, нарушитель, сеть, функционирование.

Система защиты информации в информационно-вычислительной сети (ИВС) должна быть адекватной уровню важности, секретности и критичности защищаемой информации. Такую систему можно построить не только выявив каналы утечки информации, проанализировав возможные угрозы, последствия их реализации и оценив потери, но и опираясь на модель нарушителя и стратегии по воздействию на ИВС и ОКС [1, 2], в которой отражаются его практические и теоретические возможности, априорные знания, время и место действия, другие характеристики. Это важно для анализа риска и определения требований к составу и характеристикам системы управления безопасностью. Нарушитель руководствуется мотивацией, намерениями, владеет совокупностью знаний, умений и навыков совершения несанкционированного воздействия (НВ) с применением технических средств [3].

Модель нарушителей может иметь разную степень детализации.

Содержательная модель нарушителей отражает систему принятых руководством объекта, ведомства взглядов на контингент потенциальных нарушителей, причины и мотивацию их действий, преследуемые цели и общий характер действий в процессе подготовки и совершения акций воздействия.

Сценарии воздействия нарушителей определяют классифицированные типы совершаемых нарушителями акций с конкретизацией алгоритмов и этапов, а также способов действия на каждом этапе.

Математическая модель воздействия нарушителей представляет собой формализованное описание сценариев в виде логико-алгоритмической последовательности действий нарушителей, количественных значений, параметрически характеризующих результаты действий, и функциональных (аналитических, численных или алгоритмических) зависимостей, описывающих протекающие процессы взаимодействия нарушителей с элементами объекта и системы охраны. Именно этот вид модели используется для количественных оценок уязвимости объекта и эффективности охраны.

Цель воздействия – нарушить функционирование ИВС, добиться того, чтобы ИВС не выполняла свои задачи или выполняла их с ухудшенным качеством. Частными целями нарушителя являются [3, 4]:

1. Нарушение функционирования системы.
2. Нарушение конфиденциальности информационных ресурсов.
3. Нарушение целостности информационных ресурсов.
4. Нарушение доступности информационных ресурсов.

Общие задачи, решаемые нарушителем для достижения цели:

1. *Определение архитектуры ИВС, на которые нарушитель планирует осуществить НВ, и режимов работы их элементов*. Нарушитель осуществляет наблюдение за обменом управляющей и сигнальной информацией информационным обменом между элементами сети ИВС, определяет технологию ИВС, примерный состав, отслеживает интенсивность цифровых потоков (ЦП) между элементами ИВС, время работы основных элементов и т. д. При этом нарушитель не обнаруживается системой защиты ИВС.

2. *Определение механизмов защиты, используемых в ИВС для обеспечения защищенности информационных ресурсов.* Нарушитель осуществляет активные действия. Он определяет механизмы идентификации и аутентификации пользователей, наличие шифрования передаваемой в сети информации и т. д.

3. *Выбор последовательности действий для осуществления НВ, приводящего к ухудшению функционирования ИВС*. Нарушитель определяет НВ (нарушение конфиденциальности, целостности, доступности информационных ресурсов), которое приведет к наибольшему деструктивному эффекту, т. е. нарушению в заданный интервал времени функционирования ИВС.

4. *Реализация поставленной перед собой задачи по осуществлению НВ на ИВС*. Нарушитель выполняет активные действия, приводящие к нарушению функционирования, конфиденциальности, целостности и доступности ресурсов ИВС. В результате нарушается функционирование ИВС.

5. *Скрытие своего присутствия в атакуемой ИВС*. Проведя НВ на информационные ресурсы ИВС, нарушитель скрывает свое присутствие в атакуемой сети путем стирания записей в журналах аудита сети, уничтожения следов в сети и т. д.

6. *Оценка результатов своего воздействия на функционирование ИВС*. Оценивается решение задачи о функционировании сети с вероятностью ниже требуемой.

Приняты допущения:

1. Поток заявок, поступающих от нарушителя, и поток заявок, поступающих от системы защиты ИВС, являются простейшими потоками.

2. Время обслуживания распределено по показательному закону.

Модель нарушителя можно представить, как физическую систему массового обслуживания дискретного типа с конечным множеством состояний. Алгоритм поведения нарушителя при обслуживании поступивших заявок представлен в виде графа [5], состоящего из конечного числа возможных состояний и переходов нарушителя из одного состояния в другое.

Полученные данные показали, что на сегодняшний день отсутствует единый подход к построению модели нарушителя. Предложенный подход, несмотря на то, что имеет ряд общих классификационных признаков, неполно описывает нарушителей, а категории нарушителей, описанные в различных источниках, не являются коррелированными.

Таким образом, однозначно определена и доказана необходимость разработки типовой модели нарушителя, а также методики построения модели нарушителя, подходящей для применения в ИВС любого типа.

Список используемых источников

1. Анохин Ю. Н., Осадчий А. И. и др. Основные свойства и характеристики единого информационного пространства. Инновационная деятельность в Вооруженных Силах Российской Федерации: Труды Всеармейской научно-практической конференции, 25–26 ноября 2010 г. СПб., 2010. С. 79–83.

2. Ионов С. В., Лихачев А. М., Сборцев А. С., Кузнецов В. Е. Новые технологии построения технических систем электросвязи. М.: МО РФ, 2002. 442 с.

3. Костарев С. В. Метод обеспечения кибербезопасности производственных процессов и систем в условиях возможных нештатных ситуаций // Сборник статей Пятнадцатой международной научно-практической конференции «Фундаментальные и прикладные исследования, разработка и применение высоких технологий в промышленности и экономике». Т. 1. 25–26 апреля 2013 г. СПб., С. 27.

4. Костарев С. В., Липатников В. А., Сахаров Д. В. Проблемы анализа несанкционированного искажения протокольной информации в телекоммуникационных сетях // Научно-технический журнал по вопросам качества продукции оборонного назначения «Вестник качества». 2013. № 1 (109). С. 33–40.

5. Вентцель Е. С., Овчаров Л. А. Теория случайных процессов и ее инженерные приложения : учебное пособие для студентов ВУЗов. 3-е изд., перераб. и доп. М. : Академия, 2003. 432 с. ISBN 978-5-406-00746-4.

УДК 681.391

ОЦЕНКА ВОЗМОЖНОСТИ ПРИМЕНЕНИЯ СВЕРТОЧНЫХ КОДОВ И ДЕКОДИРОВАНИЯ ВИТЕРБИ ДЛЯ СОВРЕМЕННЫХ СИСТЕМ СВЯЗИ

Г. С. Боголепов, О. Э. Однолько, К. Д. Пономарев

Военная академия связи им. Маршала Советского Союза С. М. Буденного

В сотовых и спутниковых системах связи для уменьшения энергетических затрат применяется помехоустойчивое кодирование. В данных системах связи используется сверточное кодирование. Сверточные кодеры применяются в стандарте GSM. Для декодирования сверточных кодов применяются несколько алгоритмов, один из них – это алгоритм Витерби.

помехоустойчивое кодирование, сверточные коды, турбо-коды, алгоритм Витерби.

В современном мире активно используется передача информации через мобильные и спутниковые системы связи. Передача информации происходит в цифровом виде, это обеспечивает надежность от искажений по сравнению с аналоговой передачей. Но даже в цифровых каналах связи существуют ошибки при передаче данных. Для того, чтобы уменьшить вероятность ошибки при передаче сигналов можно увеличить энергию передатчика, так как вероятность ошибки в цифровом канале связи зависит от отношения энергии передаваемого сигнала к спектральной плотности шума. Но есть возможность применять в цифровых системах передачи данных помехоустойчивое кодирование. Использование такого кодирования позволяет уменьшить энергию передаваемого сигнала, что ведет к уменьшению энергетических затрат в системах связи. Принцип помехозащищенного кода заключается в добавлении избыточных данных в исходную информацию.

Сотовая связь появилась в конце 70-х начале 80-х годов, вначале было 9 аналоговых стандартов передачи данных, которые были заменены тремя цифровыми стандартами (GSM, D-AMPS, JDC), стандарт GSM получил наибольшее распространение. Для обеспечения помехоустойчивости в стандарте GSM применяется сверточное кодирование [1].

В сверточном кодировании при поступлении на входы кодера k исходных бит информации, на выходе получается n количество выходных бит, при этом значения выходных бит зависят не только от входных, но и от тех бит, которые поступали на входы кодера раньше. Сверточный кодер может кодировать данные непрерывно, поэтому он относиться к непрерывным кодам. Для декодирования сверточных кодов используют алгоритмы последовательного декодирования, порогового алгоритма декодирования и алгоритм по наибольшему правдоподобию – алгоритм Витерби. Алгоритм Витерби получил наибольшее распространение, он был открыт в 70-х годах. Но проблема данного алгоритма заключается в увеличении времени декодирования при поступлении на вход декодера кода с большой длиной кодового ограничения. Кодовое ограничение – это размер регистра памяти в сверточном кодере. Поэтому, сверточные коды, декодируемые алгоритмом Витерби, имеют малую величину кодового ограничения. Например, в стандарте GSM используется сверточный код с числом выходных бит из кодера 2, числом входных бит 1 и кодовым ограничением 5, на рисунке 1 изображен этот кодер.

В спутниковой системе связи использование помехоустойчивых кодов актуально в силу ограниченности энергопотребления и размерами оборудования. Имея принятые ограничения по вероятности ошибки при передаче сигнала, а также большие расстояния между передающим и принимающим устройствами, что не позволяет повторно отправлять информацию, для обеспечения надежности, делают применение сверточных кодов выгодным. В спутниковых системах, таких как например: Inmarsat и Intelsat, применяются сверточные коды.

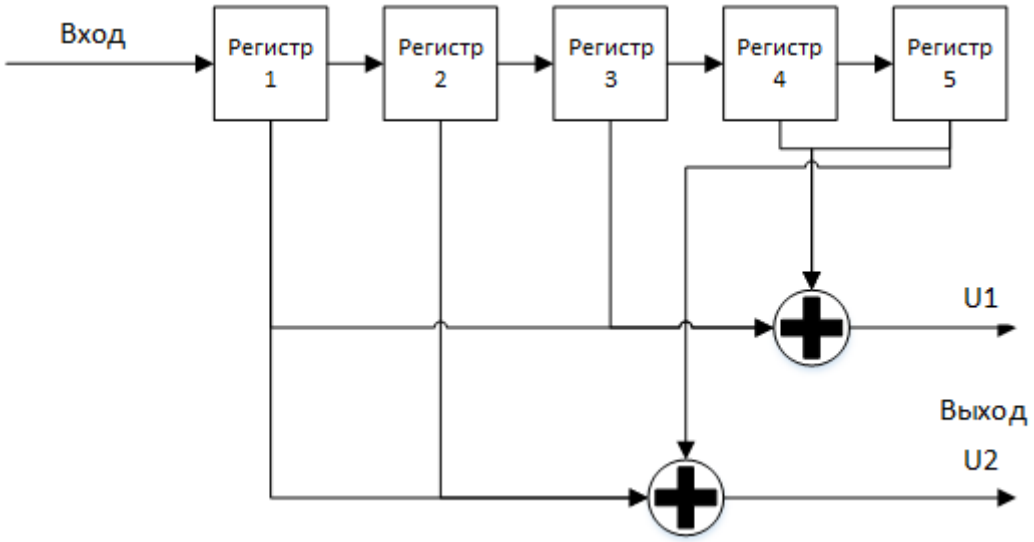


Рис. 1. Кодер, применяемый в GSM

Следует отметить, что сверточные коды обладают лучшей исправляющей способностью при увеличении памяти кода, а также при уменьшении скорости кода, скорость кода – это отношение количества входных бит на кодер и количества выходных бит с выхода кодера. Но при увеличении памяти кода увеличивается время кодирования и декодирования данных закодированных таким кодом, а уменьшение скорости кода приводит к увеличению длины закодированных данных [2, 3].

По разновидностям сверточные коды бывают систематическими, несистематическими, перфорированными и катастрофическими. О систематических сверточных кодах можно сказать, что последовательность закодированных данных состоит из информационных и избыточных битов данных, а в несистематических кодах исходная информация непосредственно не содержится. У несистематических кодов есть преимущество над систематическими в лучшей исправляющей способности, но систематические коды в отличие от несистематических не могут быть катастрофическими.

Катастрофические коды – это такие коды, которые имеют бесконечное число ошибок при декодировании при конечном числе ошибок при передаче данных.

Также для уменьшения размеров закодированных данных необходимо применять коды с кодовой скоростью как можно ближе к 1, но использование таких кодов вызывает трудности, особенно при передаче данных с большими скоростями. В таких условиях следует использовать код с кодовой скоростью вида $1/n$, а затем стирания некоторых выходных битов для получения скорости вида k/n, такие коды называются перфорированными. Реализация и использование таких кодов более простая, поэтому достаточно распространена [4, 5].

В последнее время сверточные коды в чистом виде применяются все реже им на замену приходят Турбо-коды, которые состоят из нескольких помехоустойчивых кодов, в том числе и сверточных, на рисунке 2 показан график сравнения сверточного кода и составленного на его основе Турбо-кода.

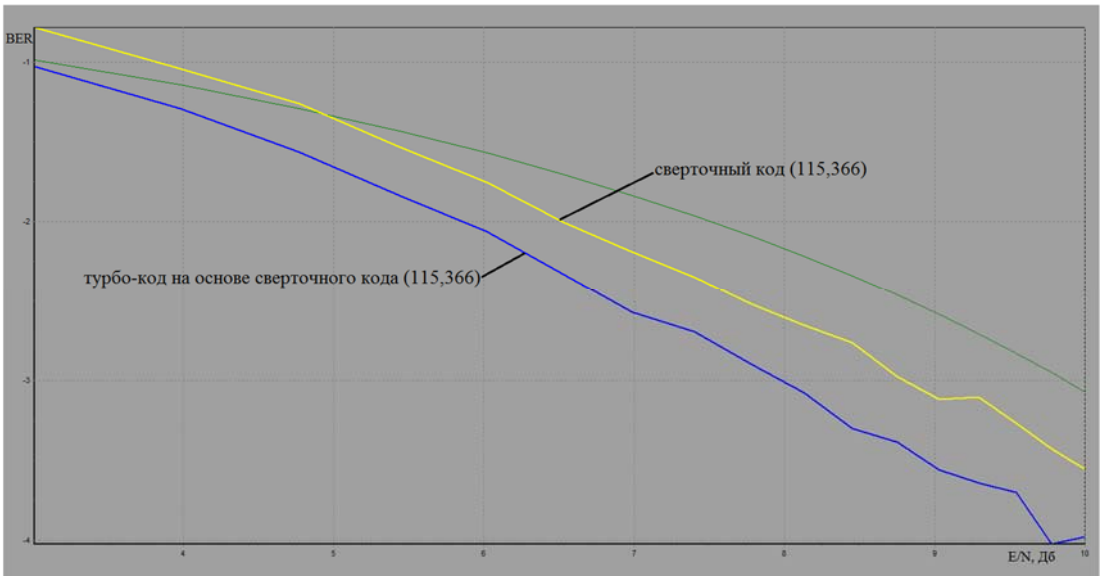


Рис. 2. Сравнение сверточного кода и Турбо-кода

Список используемых источников

1. Никитин Г. И. Сверточные коды: учеб. пособие. СПб. : СПбГУАП, 2001. 80 с.

2. Банкет В. Л. Сигнально-кодовые конструкции в телекоммуникационных системах. Одесса : Феникс, 2009. 180 с. ISBN 978-966-438-224-0 2.

3. Прокис Д. Цифровая связь / под ред. Д. Д. Кловского. М. : Радио и связь, 2000. 800 с.

4. Акчурин Э. А. Цифровые сигнальные процессоры: учеб. пособие. Самара : ПГУТИ, 2011. 217 с.

5. Витерби А. Д., Омура Д. К. Принципы цифровой связи и кодирования. М. : Радио и связь, 1982. 536 с.

Статья представлена старшим научным сотрудником, кандидатом технических наук А. С. Дворниковым.

УДК 004.932

ПОСТРОЕНИЕ ПОЛЯ ОСОБЫХ ТОЧЕК В ИЗОБРАЖЕНИЯХ НА ОСНОВЕ УРАВНЕНИЯ ГЕЛЬМГОЛЬЦА

Ю. Ф. Болтов

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

В этой статье описывается обработка изображения на основе его представления в виде скалярных полей, генерируемых уравнением Гельмгольца. Построены поля специальных точек, которые сохранили значение разности хроматической уровня. Эти поля сравниваются с полями, построенные раньше через уравнение Лапласиана.

поле, особые точки, уравнения Гельмгольца, цифровые изображения, функция Грина.

Введение

Применяя уравнения математической физики, например, Лапласиан, можно построить на изображениях скалярные поля [1, 2], являющиеся непрерывными во всей области существования кроме источников (особых точек) в которых имеются разрывы. Местоположение каждого источника и его мощность задаётся в правой части уравнения с первыми производными функции Дирака (источник типа диполя). Коэффициент, на который умножается функция Дирака, определяет мощность источника. Если коэффициент равен единице, то полученное решение, связанное с этой функцией Дирака, представляет собой функцию Грина. Определив функцию Грина для данного уравнения, несложно получить суммарное поле всех источников.

Выбрав соответствующее линейное уравнение математической физики, и используя резкие перепады яркости в изображении как источники, можно построить поле особых точек, а затем, вычитая его из исходного изображения, получим остаточное поле. После этих операций изображение представляется в виде двух частей. Первую часть можно хранить в виде значений резких перепадов цветности, использованных при построении поля особых точек, а во второй части в силу построения отсутствуют резкие перепады цветности. Важным моментом является определение области влияния каждого источника. Такой областью может быть всё изображение. Однако это влечёт за собой слишком большой объём вычислений вклада каждого источника в общее поле. Поэтому целесообразно ограничить область влияния источника за счет решения краевой задачи [1, 2]. Однако, даже при этом вычислительная нагрузка может быть чрезмерной.

Постановка задачи

Уравнение Гельмгольца отличается от Лапласиана наличием волнового члена, а его решение представляется в виде цилиндрических функций. При распространении волн в плоскости на строго определённых расстояниях от точечного источника решения обращаются в нули, образуя круглые зоны. Зону, которая связана с первым нулём, будем рассматривать как область существования решения. Очевидно, что объём вычислений значений поля в круглой зоне, образованной естественным образом, существенно меньше, чем в искусственно построенной квадратной зоне для лапласиана, и поэтому с целью ускорения обработки целесообразно исследовать возможность применения уравнения Гельмгольца для построения поля особых точек.

Решение

Уравнение Гельмгольца, которое предполагается использовать, для обработки изображений, можно записать в виде трёх скалярных уравнений, каждое из которых соответствует одной из цветовых плоскостей (R, G, B):

$$\frac{\partial^2 U_i}{\partial x^2} + \frac{\partial^2 U_i}{\partial x y^2} + k^2 U_i = \delta(x - x_0)\delta(y - y_0),$$

где $i = 1, 2, 3$, x_0 и y_0 – координаты особой точки; k – волновое число.

Частное решение каждого скалярного уравнения будет представлять собой поле точечного источника, амплитуда которого равна 1. По сути, это поле является функцией Грина для уравнения Гельмгольца и выражается через функцию Неймана нулевого порядка $Y_0(kr)$ [3, 4]:

$$r = \sqrt{(x - y_0)^2 + (y - y_0)^2}.$$

Как и в случае с лапласианом, источники, в окрестностях которых поле имеет разрывы, являются диполями, ориентированными по нормали к границе участков с различной яркостью. По аналогии с лапласианом поле этих диполей можно записать в виде:

$$G_i(x - x_0, y - y_0) = \frac{\pi}{2}\left(k_1 \frac{Y_0(kr)}{\partial x} + k_2 \frac{Y_0(kr)}{\partial y}\right),$$

где k_1 и k_2 – проекции нормали к линии контура соответственно на ось x и на ось y.

В силу свойств функций Неймана её частные производные по x и по y имеют вид:

$$\frac{\partial Y_0(kr)}{\partial x} = -Y_1(kr) \cdot \frac{\partial (kr)}{\partial x} = -k \cdot Y_1(kr) \cdot \frac{(x - x_0)}{\sqrt{(x - x_0)^2 + (y - y_0)^2}},$$

$$\frac{\partial Y_0(kr)}{\partial y} = -Y_1(kr) \cdot \frac{\partial (kr)}{\partial y} = -k \cdot Y_1(kr) \cdot \frac{(y - y_0)}{\sqrt{(x - x_0)^2 + (y - y_0)^2}},$$

где $Y_1(kr)$ – есть функция Неймана первого порядка.

Имея выражение для поля одиночного диполя с произвольной ориентацией, поле всех особых точек можно получить суперпозицией полей всех диполей, соответственно ориентированных по *x* и по *y* и перепадами градаций цветности: ΔU_{ji}^{x} и ΔU_{ji}^{y}.

$$G_{0i}(x-x_0, y-y_0) = \frac{1}{4}\sum_{j}^{(x_0,y_0)} (k_1\,\Delta U_{ji}^{x}\frac{\partial Y_0(kr)}{\partial x} + k_2\Delta U_{ji}^{x}\frac{\partial Y_0(kr)}{\partial y}). \quad (1)$$

Для вычисления функции $Y_1(kr)$ представим её диапазоне $0 \le kr \le 3$ с погрешностью $|\varepsilon| < 1{,}1\cdot 10^{-7}$ в виде следующего разложения [1]:

$$(kr)Y_1(kr) = \frac{2}{\pi}(kr)\ln\left(\frac{kr}{2}\right)J_1(kr) - 0{,}6366198 + 0{,}2212091(\frac{kr}{3})^2 + 2{,}1682709(\frac{kr}{3})^4$$
$$-1{,}3164827(\frac{kr}{3})^6 + 0{,}3123951(\frac{kr}{3})^8 - 0{,}04100976(\frac{kr}{3})^{10} + 0{,}0027873(\frac{kr}{3})^{12} + \varepsilon \quad (2)$$

где $J_1(kr)$ – функция Бесселя первого рода (разложение на многочлены этой функции в том же диапазоне и с погрешностью $|\varepsilon| < 1{,}3\cdot 10$, приведено ниже):

$$J_1(kr) = kr(\frac{1}{2} - 0{,}56249985\left(\frac{kr}{3}\right)^2 + 0{,}21093573\left(\frac{kr}{3}\right)^4 - 0{,}03954289\cdot\left(\frac{kr}{3}\right)^6 +$$
$$+0{,}00443319\cdot\left(\frac{kr}{3}\right)^8 - 0{,}00031761\cdot\left(\frac{kr}{3}\right)^{10} + 0{,}00001109\cdot\left(\frac{kr}{3}\right)^{12} \quad (3)$$

Формулы (1), (2) и (3) являются основой для быстрого вычисления суммарного поля источников типа диполя в неограниченном пространстве.

Переход к дискретному пространству

Как следует из (2), в окрестностях особых точек, также как, и в случае с Лапласианом, значение поля стремиться к бесконечности, т. е. имеет полюс первого порядка. Используя методику, изложенную в [1, 2] относительно лапласиана, определим поправки к значениям координат особых точек, которые, корректируя поведение поля в окрестности этих точек, на расстоянии нескольких пикселей от полюса не влияют на результаты вычислений поля. После соответствующих преобразований, аналогичных в [1, 2] получим:

$$G_{0i}(x-x_0, y-y) = \frac{1}{4}\sum_{j}^{(x_0,y_0)} (k_1 \Delta U_{ji}^{x} \frac{\partial Y_{(0}(kr)}{\partial x} + k_2 \Delta U_{ji}^{x} \frac{\partial Y_{(0}(kr)}{\partial y}), \qquad (4)$$

где

$$x1 = x - x_0 - 0{,}5 + \frac{0{,}068}{x - x_0 - 0{,}5}, \qquad y1 = y - y_0 - 0{,}5 + \frac{0{,}068}{y - y_0 - 0{,}5}.$$

Сравнение поправок, полученных для Лапласиана, с поправками в выражении (4) показывает, что они полностью совпадают. Такой результат можно было ожидать, так как очевидно, что частное решение уравнения Гельмгольца при малых значениях аргумента (т. е. в близости от особой точки) асимптотически совпадает с частным решением Лапласиана.

Основное отличие выражений (1–4), по сравнению с аналогичной формулой для Лапласиана заключается в наличии дополнительного параметра – волнового числа *k*. В частности, оно позволяет без решения краевой задачи ограничить вклад текущего диполя зоной, размеры которой определяются значением волнового числа. Функция Неймана первого порядка имеет первый ноль при $kr = 2{,}19$. Отсюда зону вокруг каждого диполя для расчёта его вклада в суммарное поле можно ограничить радиусом $r = 2{,}19/k$. Тогда вычисление поля по формулам: (2), (3) и (4) осуществляется значительно быстрее, чем по аналогичным выражениям для лапласиана [1], в котором дополнительно суммируются вклады множества фиктивных источников, введённых для решения краевой задачи. Возможность представления функций Неймана и Бесселя с высокой степенью точности в виде разложения по нескольким многочленам существенно сокращает объём вычислений и даёт возможность строить поле без предварительного построения матрицы для заданного окна. Однако, при прямоугольном окне виртуальные пикселы, связанные с описанием окна, можно совместить по форме и величине с физическими пикселями, что позволяет снять проблемы при вычислении поля особых точек.

При обработке круглым окном, к которому приводит использование нулей функции Неймана, виртуальные пиксели должны вписываться в окружность, что приводит к несовпадению форм виртуальных и физических пикселей. Это приводит к незначительному ухудшению качества поля диполей за счет появления незначительного «цветового шума». Поэтому данный подход целесообразен, когда допускается незначительное ухудшение качества вследствие ускорения обработки.

Использование для этой модели решения краевой задачи для квадратной зоны, как и в случае Лапласиана, сводит на нет преимущество наличия в этой модели круглого окна. Расчёты произвольного квадратного окна в случае Лапласиана занимают меньше времени.

Если для некоторого набора окон вычислить компоненты соответствующих матриц и записать их в статические массивы, то с точки зрения обработки изображения в окне эти модели будут эквивалентны, но в модели на основе волнового уравнения останется возможность варьирования волновым числом, с целью коррекции поля особых точек.

Таким образом, возможность наличие дополнительного параметра – волнового числа позволяет за счёт незначительного ухудшения качества ускорить построение поля особых точек, или при построении классического окна улучшить поле особых точек. В последнем случае необходимо сформировать требования к скорректированному полю (например, получение наименьшей разности исходного изображения и поля особых точек).

а) б) в)

Рисунок. Гравюра художницы Н. Мощевитиной: а) исходное изображение; б) поле особых точек на основе лапласиана (время обработки 250 мс); в) поле особых точек на основе Гельмгольца (время обработки 38 мс)

Выводы

Применение уравнения Гельмгольца для построения поля особых точек вместо лапласиана позволяет, либо ускорить процесс построения этого поля за счёт незначительного снижения качества, либо улучшить качество поля особых точек за счёт некоторого усложнения процесса обработки.

Список используемых источников

1. Болтов Ю. Ф. Сжатие графической информации на основе её представления в виде полевой структуры // Телекоммуникации. 2008. № 12. С. 30–35.

2. Болтов Ю. Ф. Обработка визуальной информации на основе ее представления в виде скалярных или векторных полей: концепция , матеаматические модели и алгоритмы. СПб. : СПбГУТ, 2010. 184 с.

3. Абрамовиц М. и др. Справочник по специальным функциям с формулами, графиками и математическими таблицами. М. : Наука, 1997. 832 с.

4. Корн Г., Корн Т. Справочник по математике для научных работников и инженеров. М. : Наука, 1984. 720 с.

УДК 004.7

МОДЕРНИЗАЦИЯ ПРОТОКОЛА ONVIF ДЛЯ ИСПОЛЬЗОВАНИЯ В СИСТЕМЕ «БЕЗОПАСНЫЙ ГОРОД»

А. В. Бородко

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

Рассмотрены ограничения стандарта ONVIF. Предложен новый ONVIF-совместимый сервис для построения систем с несколькими тысячами медиаисточников.

медиаданные, система видеонаблюдения, система «Безопасный город», ONVIF.

Развитие современных систем безопасности и видеонаблюдения обусловлено завершившимся переходом от аналоговой техники к цифровой, активным развитием мультимедиа аппаратуры, каналов передачи информации и программных средств для анализа цифровых информационных потоков [1].

Современный мегаполис представляет собой сложную многоуровневую структуру. Он состоит из большого количества подсистем – телекоммуникационной, транспортной, электроснабжения, а также многих других, которые функционируют и взаимодействуют между собой. Для контроля работы всех городских систем, обеспечения безопасности каждого жителя и всех уязвимых точек инфраструктуры, получения и архивирования информации обо всех важных событиях и оперативного предоставления этой информации всем заинтересованным службам необходимы не разрозненные уличные камеры видеонаблюдения, а комплексная информационная система, способная аккумулировать, объединять, анализировать и группировать разнородные данные, поступающие от множества источников. «Безопасный город» и является такой системой.

ONVIF – это стек протоколов, разработанный международным форумом ONVIF (*Open Network Video Interface Forum*) основанным компаниями Axis Communications, Bosch Security Systems и Sony в ноябре 2008 г. с целью разработки и распространения открытого стандарта для систем сетевого ви-

деонаблюдения. Так как это – открытый стандарт, то существенно снижается вероятность возникновения замыкания на поставщике и монополии, что уже приносит ощутимую экономию.

В части видеонаблюдения стек протоколов ONVIF покрывает задачи доступа к медиаданным с отдельных видеокамер и видеорегистраторов. Например, доступа к камере – один медиаисточник. Или к регистратору – например, 64 медиаисточника (по количеству каналов).

В рамках доступа к медиаисточникам масштабной системы видеонаблюдения, коей является «Безопасный город», необходимо, например, решать следующие задачи: а) получение полного списка всех медиаисточников в системе (это 5, 10, 50 тысяч камер), б) получение списка медиаисточников в выбранной географической области, поиск по названию, описанию, в) получение сведений о местоположении, тестовом описании источников, г) получение сведений об изменении состава и конфигурации источников, и так далее.

ONVIF технически этого сделать не позволяет. Так, если обратиться к спецификации Media Service на сайте ONVIF (текущая версия 2.6.1; http://www.onvif.org/specs/srv/media/ONVIF-Media-Service-Spec-v261.pdf), то можно видеть, что операции GetVideoSources, GetProfiles возвращают полные списки источников и профилей, соответственно. Что, в случае наличия 10000 медиаисточников, приводит к необходимости сформировать сообщение весом в сотни мегабайт – что даже если и будет работать на реальных сетях, то будет работать слишком медленно. В ONVIF отсутствуют операции для поиска или фильтрации источников, например, по критериям местоположения. В ONVIF в структуре данных tt:VideoSource, описывающей медиаисточник, вообще не предусмотрено полей для определения местоположения, текстового описания (http://www.onvif.org/onvif/ver10/schema/onvif.xsd). Нет операций для получения списка изменений состава конфигурации, а такие изменения в системах видеонаблюдения на 10 000 камер происходят постоянно. Для решения этих задач и создаётся сервис менеджера медиаисточников – основными принципами при создании которого явилось соответствие технологиям стека протоколов ONVIF.

Сервис менеджера медиаисточников решает задачи итеративного получения полного списка не одним, а несколькими последовательными запросами, итеративное получение списка изменений конфигурации без необходимости перечитывать полный список источников, поиск медиаисточников по местоположению и другим метаданным, – то есть те задачи, которые ONVIF не позволяет решить.

Функциональность ONVIF совместимого оборудования классифицирована в так называемые профили (*profiles*). На текущий момент профили определены для трех типов устройств – видеоисточников (*Profile S*), регистраторов (*Profile G*) и контроллеров **систем контроля и управления доступом** (*Profile C*). Профиль можно рассматривать как список требований,

объединяющий несколько обязательных или необязательных функций. В настоящее время для реализации функционала мультимедийных устройств действует профиль *S*. Спецификации ONVIF, применимые для источников медиаданных, и место разрабатываемого сервиса менеджера медиаисточников показаны на рисунке.

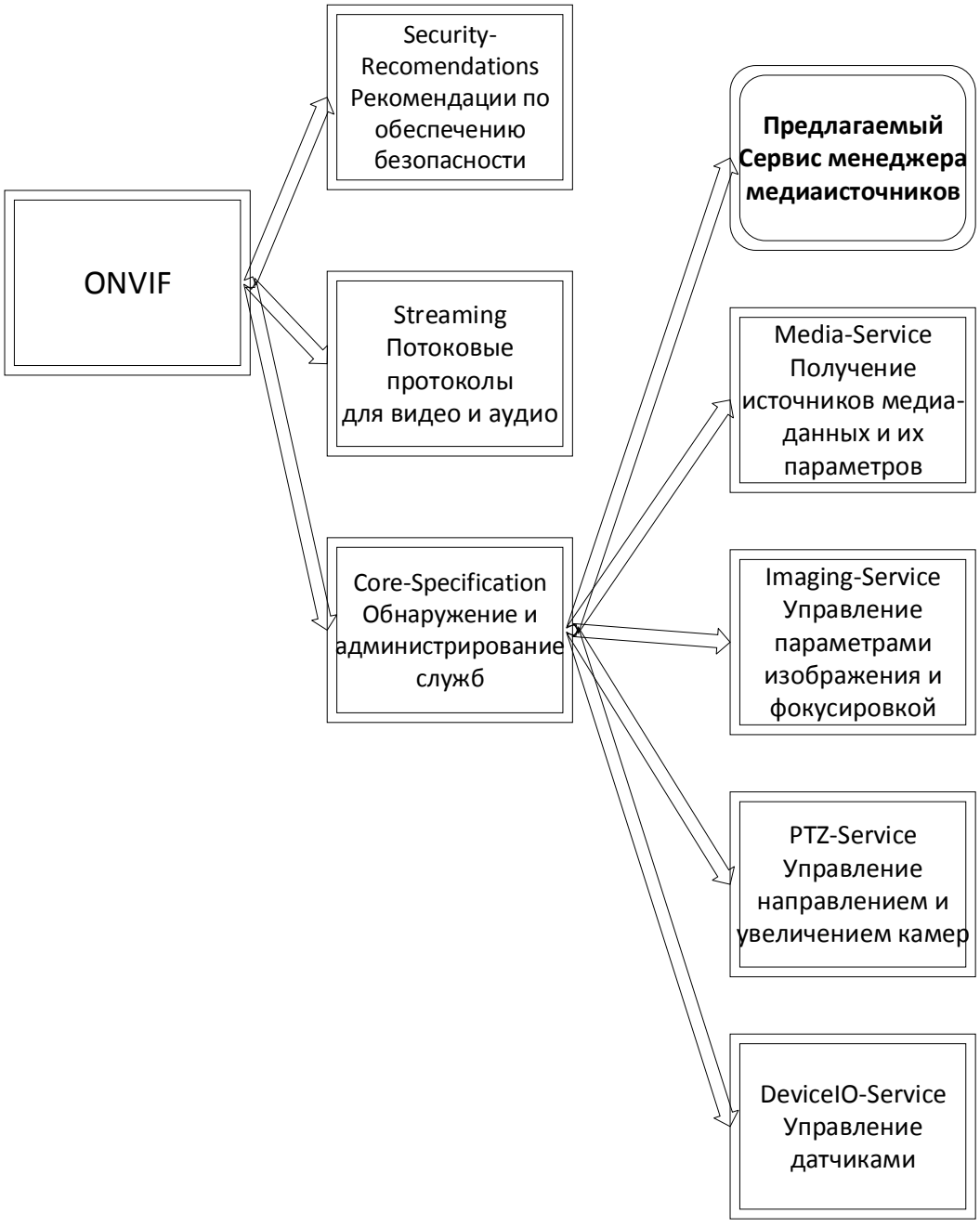


Рисунок. Основные сервисы ONVIF для медиаисточников

Требования к сервису узла определены через требования раздела 8 Device Management [2], преимущественно подразделов 8.1 Capabilities и 8.3 System, все сервисы, реализуемые данным узлом, должны быть перечислены в ответе на запрос к информационной услуге GetServices, в том числе

и сервис менеджера медиаисточников. В ответе GetServices должна содержаться информация и о сервисе менеджера медиаисточников в соответствии с [2], сервис однозначно определяется по пространству имён. Предложено присвоить сервису менеджера медиаисточников пространство имен: “urn:dev:msp:1.0”, с префиксом “msp”.

Для описания сервиса менеджера медиаисточников разработана схема в формате WSDL, фрагменты которого приведены в описаниях методов разрабатываемого сервиса. Для получения списка медиаисточников потребитель должен направить запрос GetMediaSources к менеджеру медиаисточников.

Для получения списка медиаисточников потребитель должен направить запрос GetMediaSources к менеджеру медиаисточников. Схема запроса приведена ниже.

```
<msp:GetMediaSources>
      <msp:Limit>xsd:int</msp:Limit> ?
      <msp:StartReference>xsd:string</msp:StartReference> ?
</msp:GetMediaSources>
```

В процессе эксплуатации систем, владеющие информацией о входящих в их состав медиаисточниках и их местоположении, конфигурация медиаисточников может изменяться – медиаисточники могут быть добавлены, удалены, могут быть изменены их параметры и правила доступа к ним. Вычитывать весь список медиаисточников при любом изменении конфигурации – ресурсоемко и избыточно. Эту информацию предоставляет информационная услуга GetUpdates, посредством которой клиент после первичного получения полного списка может периодически запрашивать и получать обновления сведений о медиаисточниках. Под обновлением понимается добавление, изменение или удаление сведений об одном медиаисточнике.

Для получения обновлений потребитель должен направить запрос GetUpdates к менеджеру медиаисточников. Схема запроса приведена ниже.

```
<msp:GetUpdates>
      <msp:UpdateToken>xsd:string</msp:UpdateToken>
      <msp:Limit>xsd:int</msp:Limit> ?
</msp:GetUpdates>
```

Потребитель может осуществить поиск медиаисточников по заданным критериям с помощью информационной услуги поиска FindMediaSources. Для поиска медиаисточников потребитель должен направить запрос FindMediaSources с значениями фильтра Scope к менеджеру медиаисточников. Схема запроса приведена ниже.

```
<msp:FindMediaSources>
      <msp:Scope>
            <any />
      </msp:Scope>
       <msp:MaxMatches>xsd:int</msp:MaxMatches> ?
       <msp:KeepAliveTime>xsd:duration</msp:KeepAliveTime>
</msp:FindMediaSources>
```

Если сервис менеджера медиаисточников предоставляет информационную услугу FindMediaSources, то он должен также предоставить информационную услугу GetSearchResults, обеспечивающую возможность получения результатов поиска сведений о медиаисточниках.

Для получения результатов поиска потребитель должен направить запрос GetSearchResults к менеджеру медиаисточников. Схема запроса приведена ниже.

```
<msp:GetSearchResults>
      <msp:SearchToken>xsd:string</msp:SearchToken>
      <msp:MinResults>xsd:int</msp:MinResults> ?
      <msp:MaxResults>xsd:int</msp:MaxResults> ?
      <msp:WaitTime>xsd:duration</msp:WaitTime> ?
</msp:GetSearchResults>
```

В ходе работы разработана схема описания сервиса в формате WSDL. Потребитель, используя компилятор WSDL и среду разработки программного обеспечения, встраивает описанную службу в свою систему, благодаря чему она становится совместимой с провайдером системы «Безопасный город» и сможет с ним взаимодействовать. Что и было реализовано в тестовом сервисе, разработанном в среде SmartBear SOAPUI и Visual Studio C#. Реализованный сервис позволяет дополнить ONVIF описанием метаданных и правил доступа к видеоисточникам, в частности: предоставляющим сведения о видеоисточниках, в том числе об их географическом местоположении и областях обзора, что соответствует требованиям к протоколам системы «Безопасный город».

Список используемых источников

1. Бородко А. В. Оценка показателей качества факсимильной связи : дис. … канд. техн. наук : 05.12.13 / Бородко Александр Владимирович. СПб., 2007. 231 с.

2. ONVIF Core Specification Ver. 2.10. [Электронный ресурс]. 2011. 141 с. URL: http://www.onvif.org/specs/core/onvif-core-spec-v210.pdf (дата обращения 10.02.2016).

УДК 004.9

АНАЛИЗ ИНФОРМАЦИОННЫХ ПОТОКОВ СИГНАЛА ГЕМОДИНАМИКИ ДЛЯ ПОЛУЧЕНИЯ И ИСПОЛЬЗОВАНИЯ ЕГО ФРАКТАЛЬНЫХ ХАРАКТЕРИСТИК

Л. Б. Бузюков, Т. В. Ермакова

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

Элементы самоподобия и фрактальность многих структур организма человека в настоящее время не вызывает сомнений. Это позволяет предположить, что свойства фрактальных моделей могут быть использованы в медицине. В статье проводится исследование гемодинамических сигналов на наличие фрактальных свойств, а также на возможность разработки математических методов их анализа. На основе выбранных математических методов анализа создано программное обеспечение, позволяющее осуществлять обработку сигнала с учетом его фрактальных свойств.

самоподобие, фракталы, показатель Херста, периодограмма, вейвлет – анализ, R/S анализ.

Измерения частоты ритмичности ЭКГ, различного вида давления, скорости пульсовой волны, которые разбиваются на целый ряд специфических параметров, необходимо оценить с помощью специальных методов исследования. Все эти сигналы относятся к биоэлектрическим сигналам, поступающим на входы монитора Carescape B65 и аппарата ИВЛ. Предлагается применять методы цифровой обработки биоэлектрических сигналов, представляющих собой случайные электрические сигналы в виде колебаний сложной формы. Многие параметры, например, амплитуда пульсовой волны нормированных значений не имеют и оцениваются непосредственно в динамике.

Следует заметить, что решающую роль играет форма пульсовой волны, которая в сочетании с количественными значениями позволяет наиболее правильно оценить диагноз пациента.

Статья посвящена анализу сигналов гемодинамики с использованием фрактальных методов. В их основе лежит понятие самоподобия, которое сохраняет инвариантность при изменении масштабов наблюдения.

Фрактальные структуры широко представлены в организме человека. Форму фрактала имеют легкие человека, мозг, кровеносная система и т. д. Это дает возможность предположить, что фракталы можно применить в медицине. Например, гемодинамический процесс можно рассматривать как некоторый дискретный временной ряд $X(t)$. В общем виде это можно записать так:

$$\{X(t+\Delta t)-X(\Delta t),t\in R\}\overset{\Delta}{=}\{X(t)-(0),t\in R\} \text{ для всех } \Delta t \in R\ .$$

Самоподобный процесс можно представить и в виде уравнения с использованием показателя Херста $H > 0$:

$$\{X(at),t\in R\}=\{a^{H}X(t),t\in R\}\ .$$

Обе формулы показывают, что изменение временного масштаба эквивалентно изменению пространственного масштаба состояний. Это в свою очередь означает, что наблюдается сходство статистических свойств из-за того, что статистические характеристики при масштабировании не меняются. Реализации самоподобного процесса визуально похожи независимо от масштаба времени, на котором они рассматриваются.

Поэтому при исследовании интерес представляет поведение гемодинамического сигнала именно при агрегировании.

Параметр H является индикатором самоподобности случайного процесса и характеризует свойство долговременной зависимости. Для определения параметра Херста использовался ряд методов, в частности, *R/S* метод. Но известно, что этот метод дает лишь приближенное значение параметра. Поэтому для вычисления этого параметра целесообразно пользоваться несколькими методами, чтобы можно было сравнивать полученные результаты. В этой статье кроме рассмотренных ранее *R/S* метода и метода, использующего вейвлет-анализ, проведено исследование метода оценки параметра Херста с помощью периодограммы (табл.) [1, 2].

ТАБЛИЦА. Оценка степени самоподобности, выполненная различными методами при одинаковом диапазоне масштабирование

Метод оценки	Значение параметра Херста (H)
Вейвлет-анализ	0,81±0,11
R/S статистика	0,69±0,11
Периодограмма	0,82±0,15

Очевидно, что в общем случае полностью описать случайный процесс практически невозможно и реально ограничиваются некоторыми характеристиками – математическим ожиданием, дисперсией, автокорреляционной функцией и в случае необходимости некоторыми другими характеристиками.

Моделирование проводилось в визуальной среде программирования Qt 5.4.1, на языке программирования C++. Создано приложение, с помощью которого можно визуально наблюдать различные характеристики ис-

следуемого процесса, моделировать нужные параметры, изменять их в соответствии с заданными требованиями и немедленно видеть результаты этих изменений.

Итак, рассмотрим метод определение величины H на основе периодограммного анализа. Для самоподобного случайного процесса $X=\{x\}$ вычисляется периодограмма по формуле:

$$I_N(\omega)=\frac{1}{2\pi N}\left|\sum x_k e^{jk\omega}\right|,\omega\in[0;\pi],$$

где N – длина временного ряда. Учитывая, что самоподобность влияет на характер спектра $S(\omega)$ при $\omega\to 0$, должен получаться график зависимости спектральной плотности вида:

$$I_N(\omega)\sim[\omega]^{1-2H},\omega\to 0.$$

Отсюда следует, что множество случайных точек на графике $(\log[I_N(\omega)];\log(\omega))$ будут располагаться линейно с коэффициентом наклона линии $1-2H$. В [3] показано, что на практике для вычисления оценки должны использоваться только нижние 10 % частот, т. к. описанное выше поведение справедливо только для области частот, близких к нулю. Основным недостатком метода периодограммы является большой объем вычислений при построении оценки показателя Херста. Преимуществом является устойчивость оценки. Метод периодограмм заключается в вычислении оценки СПМ $\hat{S}(\omega)$ конечной случайной последовательности длины:

$$\hat{S}(\omega)=\frac{\left|X(e^{j\omega T})\right|^2}{Nf_{Д}},$$

где $X(e^{j\omega T})$ — спектральная плотность конечной последовательности $x(n)$:

$$X(e^{j\omega T})=\sum_{n=0}^{N-1}x(n)e^{-j\omega Tn}.$$

Для сглаживания периодограммы применим весовые функции (окна), и воспользуемся модифицированной периодограммой $\hat{S}_w(\omega)$, которая принимает вид :

$$\hat{S}_w(\omega)=\frac{\frac{1}{f_{Д}}\left|X_w(e^{j\omega T})\right|^2}{\sum_{n=0}^{N-1}\left|w(n)\right|^2},$$

где: $w(n)$ – весовая функция (окно) длины N; $X_w(e^{j\omega T})$ – спектральная плотность произведения $x(n)w(n)$:

$$X_w(e^{j\omega T}) = \sum_{n=0}^{N-1} x(n)w(n)e^{-j\omega Tn} .$$

Данные вычисления выполнены в математической среде MATLAB в шкале частот f (Гц) периодограммы и рассчитываются на основе ДПФ с привлечением алгоритмов БПФ. Результаты вычислений графически представлены на рисунке.

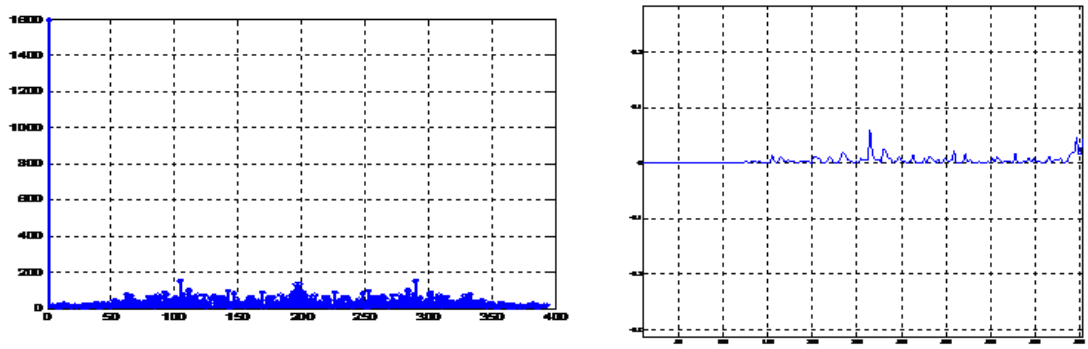


Рисунок. Модифицированная периодограмма на основе ДПФ для исследуемого сигнала гемодинамики

Проведенное измерение коэффициента Херста методом периодограмм в математической среде MATLAB подтвердило, что исследуемый сигнал обладает свойством самоподобия. Это дает основание перейти к использованию алгоритмов прогнозирования для увеличения эффективности обработки изучаемых сигналов.

Оценка коэффициента Херста, основанная на графике спектральной плотности, составляет суть метода, который обеспечивает наибольшую статистическую строгость.

Полученные фрактальные параметры сигнала гемодинамики позволяют в дальнейшем проводить анализ сигнала именно на их основе, без предварительной спектральной обработки.

Список используемых источников

1. Бузюков Л. Б., Ермакова Т. В. Использование вейвлет-анализа для исследования и оценки зависимости параметров гемодинамики от комплекса параметров специализированного измерительного устройства искусственной вентиляции легких // Актуальные проблемы инфотелекоммуникаций в науке и образовании. III Международная научно-техническая и научно-методическая конференция: сб. научных статей / СПб. : Санкт-Петербургский государственный университет телекоммуникаций им. проф. М. А. Бонч-Бруевича, 2014. С. 203–208.

2. Афончикова Т. В., Гойхман В. Ю. Анализ трафика распределенного узла коммутации с помощью вейвлет-преобразования. Информационные технологии в мире коммуникаций: сборник тезисов участников V Всероссийской научно-практической конференции 13–18 мая 2012 г. С. 14–17.

3. Шелухин И. О., Осин А. В., Смольский С. М. Самоподобие и фракталы. Телекоммуникационные приложения / Под ред. О. И. Шелухина. М. : ФИЗМАТЛИТ, 2008. 368 с.

УДК 004.49

СРАВНИТЕЛЬНЫЙ АНАЛИЗ ПОДХОДОВ К ПОИСКУ УЯЗВИМОСТЕЙ В ПРОГРАММНОМ КОДЕ

М. В. Буйневич[1], К. Е. Израилов[2], Д. И. Мостович[2]

[1]Санкт-Петербургский государственный университет телекоммуникаций им. проф. М. А. Бонч-Бруевича
[2]Государственный научно-исследовательский институ прикладных проблем

Статья посвящена анализу существующих подходов к поиску уязвимостей в программном коде. Рассматриваются такие подходы, как «черный», «белый» и «серый ящики», фаззинг-подход и тестовые случаи, ручной и автоматический, а также статический и динамический подходы. Производится выбор критериев и сравнение подходов на примере метода алгоритмизации машинного кода.

безопасность информации, поиск уязвимостей, метод алгоритмизации.

Одной из проблем безопасности информации является наличие уязвимостей в программном коде, выполняющем ее обработку. И хотя возможное направление решения проблемы путем непосредственного поиска уязвимостей в коде существует достаточно давно, тем не менее, единого метода поиска пока не создано. Существующие методы решают конкретные задачи поиска, зависящие от особенностей кода и условий работы. Реализации таких методов зависят как от применяемых в них идей и концептуальных моделей, так и от используемого представления кода (ассемблерного, алгоритмического, высокоуровневого языкового).

Создание каждого метода поиска уязвимостей является уникальным и часто плохо коррелирующим с другими. Тем не менее, в области поиска уязвимостей существует ряд широко известных подходов, «удачное» комбинирование достоинств которых позволит реализовывать такие методы эффективным образом. Для этого необходимо произвести анализ существующих подходов к поиску уязвимостей и отобрать наиболее подходящую комбинацию их составных частей, синтез которых позволит по крайне мере предположить общую схему будущего метода. Выбор критериев сравнительной оценки подходов, актуальных с точки зрения задачи поиска уязвимостей в программном коде, как раз даст возможность произвести такой отбор.

Рассмотрим существующие подходы к поиску уязвимостей в коде и произведем их сравнительный анализ по критериям на сквозном примере одного из возможных методов поиска – путем алгоритмизации машинного кода в условиях отсутствия исходного (далее – Метод) [1].

Критерии сравнительной оценки

Критериями оценки и сравнения, актуальными с точки зрения задач Метода, могут быть следующие:

1) время поиска – среднее время, затрачиваемое на поиск основной части уязвимостей, применяя данный подходом;

2) количество обнаруживаемых уязвимостей – количество уязвимостей относительно общего их количества, которое может быть найдено с применением данного подхода;

3) ложность результатов – доля уязвимостей, найденных с применением данного подхода, которые являются особенностями кода или просто найдены ошибочно;

4) покрытие кода – объем кода, обрабатываемого с применением данного подхода, относительно общего объема;

5) требуемая квалификация пользователя подхода – уровень подготовки пользователя, необходимый для применения данного подхода (выделяются 3 уровня: пользователь, инженер, эксперт);

6) возможность обойти защиту от обнаружения – наличие у данного подхода возможностей по поиску уязвимостей даже в случае защиты программного кода от этого (например, кодирование тела вирусов и их выполнение на внутренней виртуальной машине);

7) эффективность без исходного кода – возможность применение данного подхода в условиях отсутствия исходного кода без существенного снижения показателей других связанных критериев;

8) формализация конечных результатов – возможность использования полученных результатов для автоматической обработки (например, с целью выделения, определения дубликатов или обнаружения конфликтов с результатами других подходов);

9) информативность конечных результатов – качественная оценка информации в результатах применения данного подхода, используемая для локализации, проверки и обезвреживания уязвимостей;

10) основные типы уязвимостей для поиска – список типов уязвимостей, для которых применим данный подход (выделяются 3 типа: высокоуровневые, среднеуровневые и низкоуровневые);

11) особые требования к уязвимостям для поиска – наличие дополнительных особенностей уязвимостей, без которых для их поиска данный подход не применим.

«Черный», «белый» и «серый ящики»

В зависимости от доступа к тестируемому объекту выделяют 3 подхода: «*белого»*, «*черного»* и «*серого ящика»*. В первом случае, вся информация о внутреннем строении объекта доступна, во втором – имеется возможность исследования только реакции объекта на внешние воздействия, а в третьем – такая информация об объекте имеется, однако для исследования также используется тестирование воздействием. Применительно к поиску уязвимостей, подход «белого ящика» означает, что поиск осуществляется по самому программному коду, «черного» – исследуется функционирование кода при различных внешних условиях и данных, «серого» – также исследуется функционирование кода, но для проведения самого поиска и анализа его результатов используется непосредственная информация из него. Также, первый подход можно поделить на поиск по исходному коду и машинному коду, однако в рамках применения Метода имеет место только последний.

С позиции заданных критериев оценки, все подходы можно считать равноценными; хотя и есть незначительный перевес в сторону поиска именно по программному коду («белый» и «серый ящики»).

Фаззинг-подход и тестовые случаи

Суть фаззинг-подхода (от англ. *fuzzing* или *fuzz testing*) заключается в генерации полностью случайного и специализированного набора данных, подаваемых на вход тестируемого программного средства или его модуля с целью выявления программных исключений или другого явного нарушение их корректного функционирования. Проверка функционирования осуществляется выполнением отдельного прохода запуска программного средства на сгенерированном наборе данных. Подход можно считать удовлетворительными лишь для отдельных типов уязвимостей или условий применения (например, поиск программных исключений путем фаззинга данных в памяти тестируемой программы). Наиболее распространенным применением является тестирование всевозможных разборщиков файлов (браузеров, ассемблеров, компиляторов, других преобразователей данных); впрочем, из-за высоких требований к ресурсам (огромному количеству сгенерированных данных и запусков тестируемого программного средства) и низкой ценности получаемых результатов (только факт падения с указанием состояния памяти и регистров процессора) подход малоприменим в интересах Метода.

Альтернативой фаззинга может служить использование, так называемых, тестовых случаев (от англ. *test case*) – заданного набора условий и действий, согласно которым будет проверяться корректность функциони-

рования программного средства. С точки зрения Метода, подход будет заключаться в применении предопределённых шаблонов выявления уязвимостей.

С позиции заданных критериев применение тестовых случаев имеет небольшое преимущество, по сравнению с фаззингом. Очевидно, что их объединение не позволит получить новый подход, поскольку будет соответствовать применению одного подхода в другом – либо фаззингу со сценарием, либо тестовым случаям с использованием фаззинга.

Ручной и автоматический подходы

Одним из вариантов типизации подходов поиска уязвимостей в коде (не только машинном) с точки зрения субъективности оценки является их деление на ручные и автоматические. Суть ручного подхода заключается в применении труда экспертов, проводящих анализ программного кода (исходного, машинного, любого другого его представления), к его субъективной оценке на наличие и местоположение уязвимостей. Суть автоматического подхода прямо противоположна ручному и основана на применении автоматических средств поиска без участия человека. Первый подход широко применяется для поиска среднеуровневых уязвимостей, а также когда невозможно применение автоматизации. Второй же является *де-факто* для персональных компьютеров – классическим примером является антивирусное программное обеспечение; он эффективен для низкоуровневых уязвимостей, поиска по шаблонам распространенных уязвимостей и зачастую содержит эвристические алгоритмы обнаружения.

У обоих подходов есть свои сильные и слабые стороны; объединение же их достоинств возможно путем частичной автоматизации.

Статический и динамический подходы

Другим вариантом типизации подходов к поиску уязвимостей в коде (не только машинном) с точки зрения оценки эффектов тестируемого кода является их делению на статические и динамические. Суть первого заключается в анализе программного кода в статическом виде – т. е. без его непосредственного выполнения. Суть второго заключается в выполнении кода в различных представлениях и различными подходами: исходного или машинного кода на реальном оборудовании, в эмулятора и т. п.

Объединение достоинств подходов возможно в, так называемом, подходе Symbolic execution (наиболее подходящим названием его могло бы стать «статическое выполнение кода»), основанном на совокупном анализе не только графов вызовов функций и потока управления, но и всех возможных значений переменных и состояния памяти для каждой ветки выполнения из всего их множества.

Заключение

Использование результатов сравнительной оценки существующих подходов к поиску уязвимостей и комбинирование их элементов (в рамках вводимых критериев) позволит реализовывать новые методы поиска, решающие собственные задачи и обладающие всеми достоинствами этих подходов. Так, применительно к сквозному примеру Метода, наиболее подходящей его реализацией представляется сочетание подходов поиска уязвимостей по машинному коду автоматизированным подходом (как по единичным, так и целым наборам шаблонов), преимущественно статическим анализом «белого» и/или «серого ящика», по возможности без прямого выполнения кода. Такая реализация в виде соответствующего программного средства была представлена авторами на 16 Международной конференции по современным коммуникационным технологиям ICACT-2014 [2], вызвала интерес и получила одобрение научной общественности.

Список используемых источников

1. Буйневич М. В., Израилов К. Е. Метод алгоритмизации машинного кода телекоммуникационных устройств // Телекоммуникации. 2012. № 12. С. 2–6.

2. Buinevich M. V. and Izrailov K. E. Method and Utility for Recovering Code Algorithms of Telecommunication Devices for Vulnerability Search // The 16th International Conference on Advanced Communications Technology (ICACT-2014), Bongpyeong-myeon, Korea (South), on February 16–19, 2014, pp.172–176.

УДК 681.7.068, 621.375

ВИРТУАЛЬНАЯ ЛАБОРАТОРНАЯ УСТАНОВКА ДЛЯ ИССЛЕДОВАНИЯ ОДНОКАСКАДНОГО ОПТИЧЕСКОГО УСИЛИТЕЛЯ EDFA

М. С. Былина, П. А. Чаймарданов

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

В статье представлена виртуальная лабораторная установка для исследования однокаскадного оптического усилителя EDFA (Erbium Doped Fiber Amplifier) на основе кварцевого волокна, легированного ионами эрбия, предназначенная для выполнения лабораторных работ по дисциплинам кафедры «Фотоники и линий связи». Установка разработана с использованием обобщенной математической модели однокаскадного оптического усилителя EDFA с многоканальными источниками сигнала и накачки. Установка позволяет изучать процессы распространения сигналов и накачек по активированному волокну, усиления сигналов, истощения накачек, формирования попутных и встречных шумов усиленного спонтанного излучения. Результаты моделирования представляются в виде графиков, которые можно сохранить для последующего анализа

и обработки. Установка обеспечивает многовариантность объектов исследования, так как позволяет формировать усилители на основе нескольких типов эрбиевых волокон ведущих производителей и задавать различные длины этих волокон. Установка будет внедрена в учебный процесс кафедры «Фотоника и линии связи» Санкт-Петербургского государственного университета телекоммуникаций им. проф. М. А. Бонч-Бруевча.

EDFA, Erbium Doped Fiber Amplifier, оптический усилитель, волокно, легированное ионами эрбия, виртуальная лабораторная установка, многоканальный сигнал, многоканальная накачка, попутная накачка, встречная накачка, усиленное спонтанное излучение, коэффициент усиления.

В учебный план направлений подготовки бакалавров «Инфокоммуникационные технологии и системы связи» и «Фотоника и оптоинформатика» входят дисциплины «Нелинейная оптика и активные компоненты», «Оптические усилители в телекоммуникационных системах», в рамках которых изучаются процессы усиления оптического излучения в усилителях на основе активных волокон, легированных эрбием (*Erbium Doped Fiber Amplifier* – EDFA). Целью данной работы является создание виртуальной лабораторной установки, предназначенной для изучения и исследования однокаскадного оптического усилителя EDFA с многоканальными источниками сигнала и накачки (рис. 1).

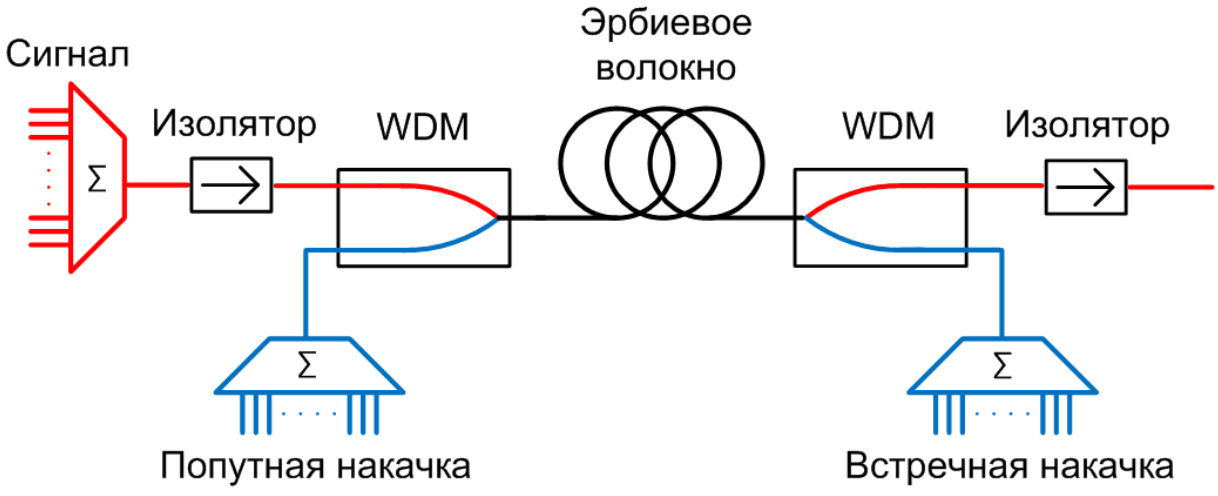


Рис. 1. Схема рассматриваемого однокаскадного усилителя EDFA

К виртуальной установке предъявлялись следующие требования: 1. Моделирование с достаточной точностью процессов усиления оптического излучения в усилителе EDFA. 2. Интуитивно понятный графический интерфейс для выбора условий исследования и получения результатов расчетов. В основу разработанной виртуальной лабораторной установки положена математическая модель усилителя, обобщающая известные модели [1, 2, 3], которой посвящена отдельная статья в данном сборнике.

Виртуальная установка может работать под операционными системами Windows, Linux и OS X, имеет русский и английский интерфейс и позволяет:

1) Задавать различные объекты исследования, изменяя параметры активного волокна, источников сигналов, попутных и встречных накачек.

2) Моделировать следующие характеристики усилителя EDFA:

– зависимости от длины волны и расстояния вдоль активного волокна мощностей сигналов, попутных и встречных накачек, УСИ в попутном и встречном направлениях; абсолютного уровня мощности сигналов с шумами УСИ («уровня сигнал+шум»); усиления сигнала и отношения сигнала к шуму;

– зависимость относительной населенности уровня N_2 от расстояния вдоль активного волокна.

3) Экспортировать результаты расчетов для последующего анализа.

Для удобства использования интерфейс виртуальной лабораторной установки разделен на два окна. Окно *«Настройки сигнала и накачки»* (рис. 2) позволяет задавать следующие параметры сигналов на входе активного волокна и накачек во встречном и попутном направлениях:

– вид сигнала – одноканальный (одна несущая длина волны), многоканальный DWDM (несколько несущих длин волн в соответствии с рекомендацией ITU-T G.694.1) или заданный произвольно в виде файла данных определенного формата.

– вид накачки – одноканальная (одна длина волны 1480 или 980 нм) или заданная произвольно в виде файла данных определенного формата.

– мощность и ширину спектра излучения каждого источника сигнала и накачки.

Изоляторы и мультиплексоры спектрального уплотнения WDM (*Wavelength Division Multiplexing*) в данной версии лабораторной установки полагаются идеальными (не вносящими потерь). В последующих версиях предполагается отказаться от этого предположения.

Окно *«Моделирование однокаскадного EDFA усилителя»* состоит из вкладок *«Параметры волокна ...»* (рис. 3) и *«Результаты моделирования»* (рис. 4–6). Вкладка *«Параметры волокна ...»* (рис. 3) предназначена для выбора марки активного волокна и его параметров: коэффициентов поглощения и усиления в различных диапазонах длин волн, параметра насыщения, длины и температуры.

На рисунках 4–6 представлены результаты моделирования усилителя с попутной накачкой на основе активного волокна марки Fibercore M-5, длиной 15 м, при температуре 25 °С. Моделирование проведено для 40-канального оптического сигнала с равномерным размещением каналов в диапазоне от 1500 до 1600 нм. Ширина канала составляла 25 ГГц, мощность сигнала в каждом канале – 1 мкВт. Накачка осуществлялась на длине волны 1480 нм, мощность накачки составляла 100 мВт.

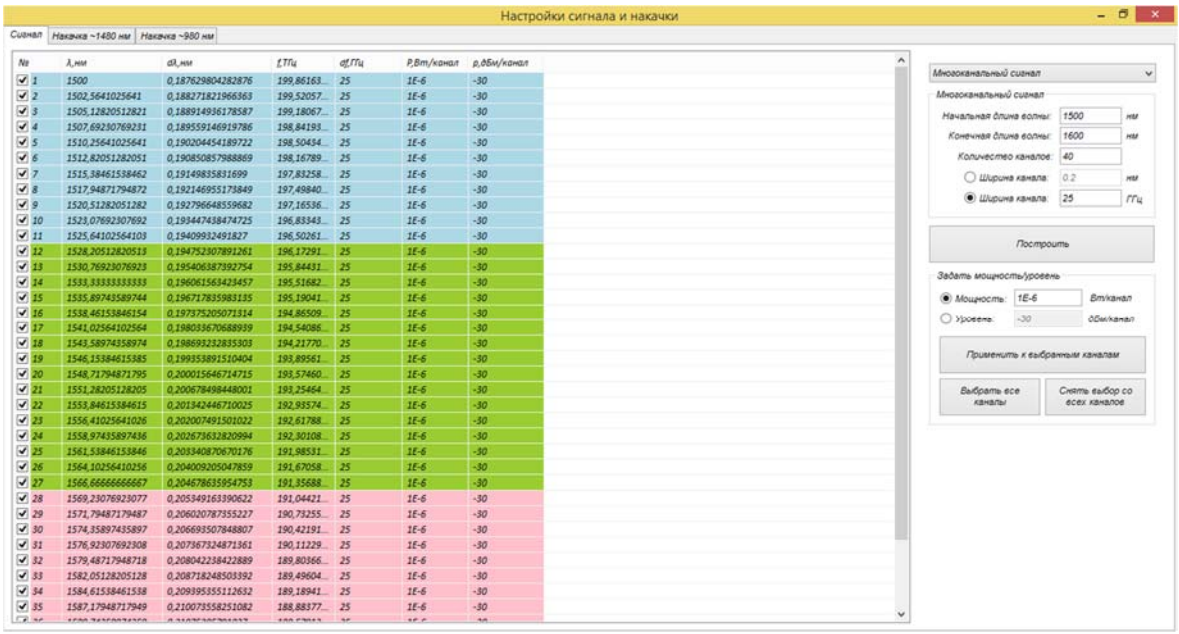


Рис. 2. Окно *«Настройки сигнала и накачки»*. Вкладка *«Сигнал»*. Задание 40-канального сигнала. Цветом выделены диапазоны длин волн *S*, *L* и *U*

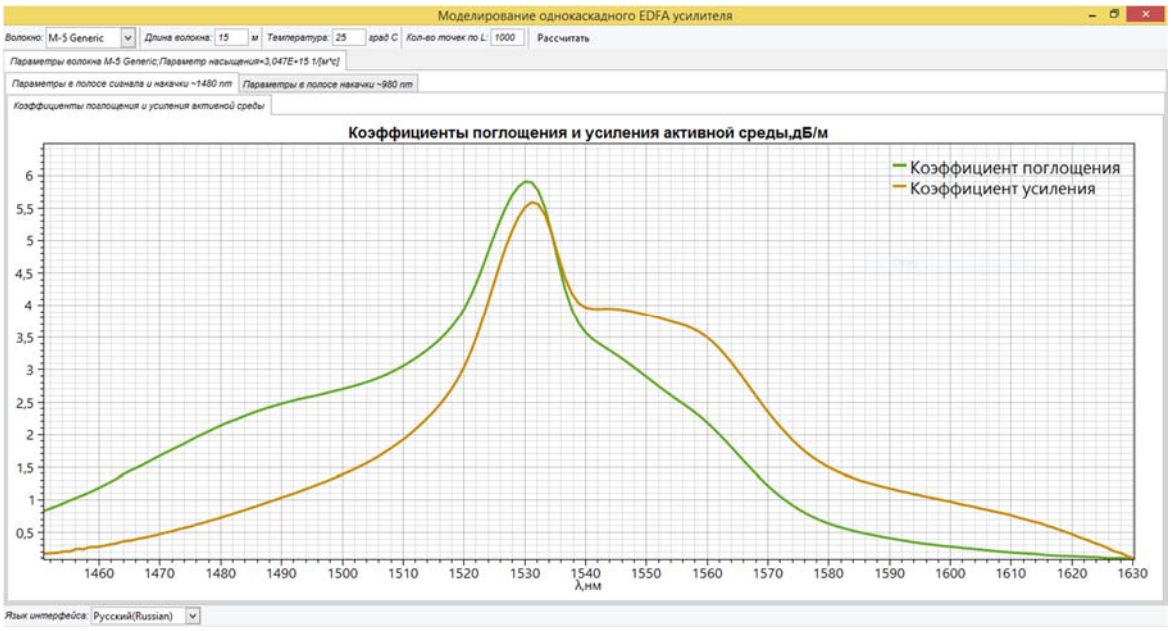


Рис. 3. Окно *«Моделирование однокаскадного EDFA усилителя»*. Вкладка *«Параметры волокна …»*. Зависимости коэффициентов поглощения и усиления для активного волокна Fibercore M-5

Авторами разработаны также методические указания к выполнению лабораторных работ на виртуальной установке по указанным выше дисциплинам. Виртуальная установка предоставляет практически неограниченный выбор объектов исследования и позволяет варьировать сложность выполнения работ от ознакомительного до исследовательского.

По мнению авторов, виртуальная лабораторная установка может представлять интерес не только для учебных заведений, но и для разработчиков

оптических усилителей, которые могут использовать ее для предварительного моделирования проектируемого усилителя.

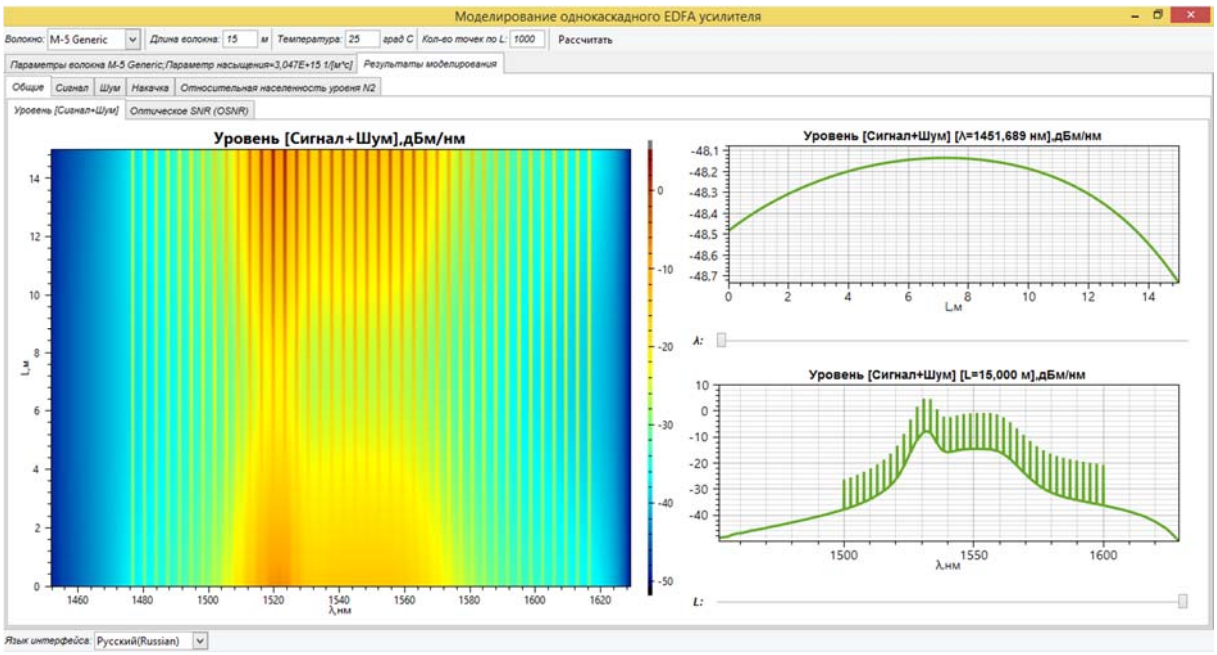


Рис. 4. Окно *«Моделирование однокаскадного EDFA усилителя»*. Зависимость у*ровня «сигнал+шум»* от длины волны и расстояния вдоль активного волокна

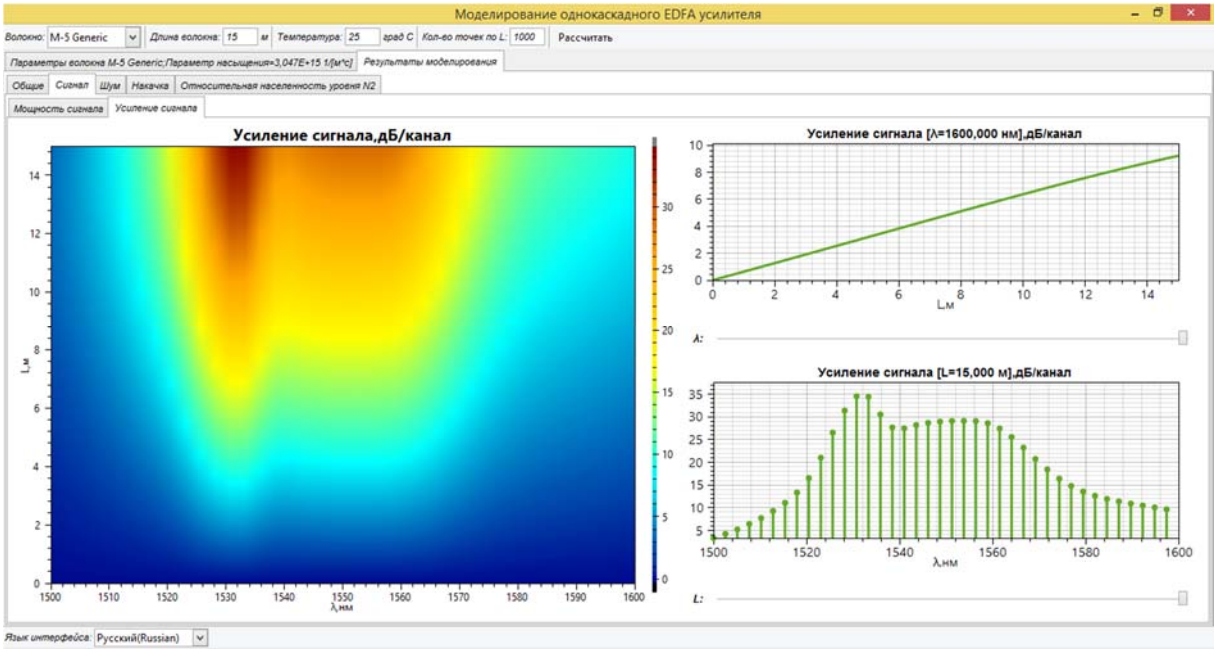


Рис. 5. Окно *«Моделирование однокаскадного EDFA усилителя»*. Зависимость усиления сигнала от длины волны и расстояния вдоль активного волокна

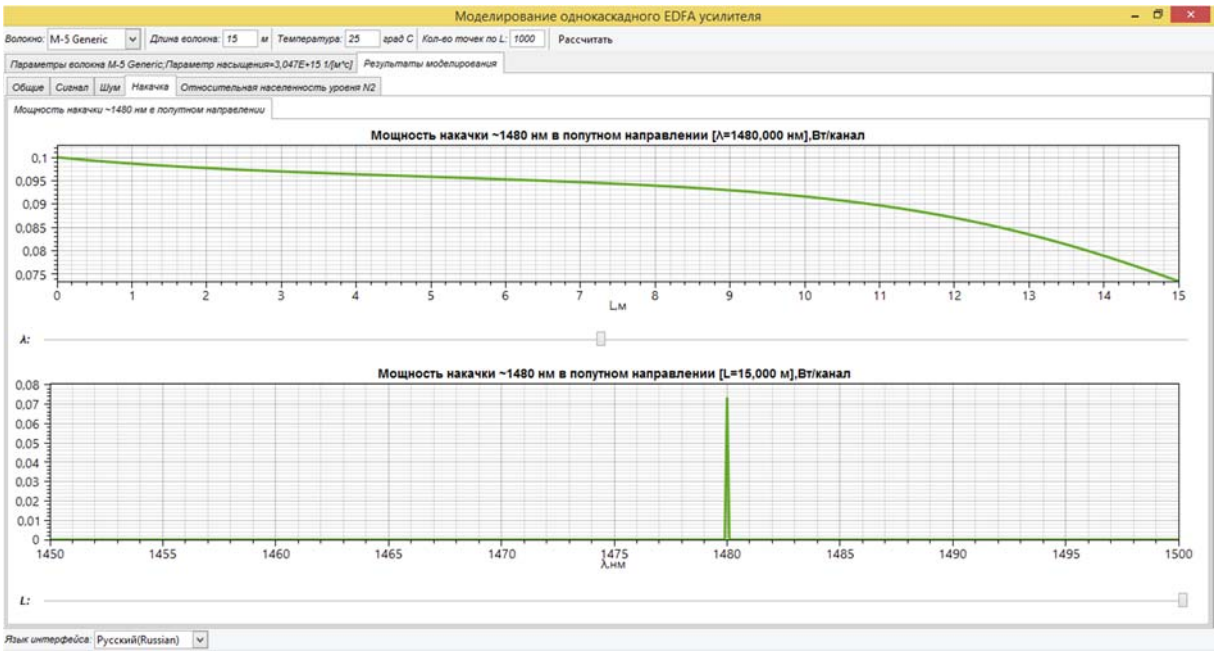


Рис. 6. Окно *«Моделирование однокаскадного EDFA усилителя»*. Зависимость мощности накачки от длины волны и расстояния вдоль активного волокна

Список используемых источников

1. Becker P. C., Olsson N. A., Simpson J. R. Erbium-Doped fiber amplifiers. Fundamentals and Technology // Academic Press, 1997. 627 p. ISBN 978-0-12-084590-3.

2. Desurvire E. Erbium-Doped fiber amplifiers. Principles and applications. John Wiley & Sons, New York, 1994. 770 pp. ISBN 0-471-58977-2.

3. Hee Gap Park, Seung Chul Yun, Young Jun Jin. Er-doped Superfluorescent Fiber Source with Thermally Stable Mean Wavelength // Journal of the Optical Society of Korea Vol. 13, No. 2, June 2009, pp. 240–244.

УДК 681.7.068, 621.375

МАТЕМАТИЧЕСКАЯ МОДЕЛЬ ОДНОКАСКАДНОГО EDFA УСИЛИТЕЛЯ С МНОГОКАНАЛЬНЫМИ ИСТОЧНИКАМИ СИГНАЛА И НАКАЧКИ

М. С. Былина, П. А. Чаймарданов

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

В работе предложена математическая модель однокаскадного оптического усилителя на основе кварцевого волокна, легированного активными частицами – ионами эрбия Er^{3+}. Модель состоит из кинетических уравнений, позволяющих рассчитывать населенности энергетических уровней активных частиц, и уравнений распространения, описывающих изменение мощностей сигналов, накачек и шума усиленного спонтанного излучения вдоль активированного волокна. Особенностью данной модели является

возможность проведения расчета оптического усилителя, использующего несколько источников попутной и встречной накачки и предназначенного для усиления многоканального сигнала. Основными результатами расчета усилителя являются мощности излучения, коэффициент усиления и отношение сигнала к шуму для каждого канала, попутные и встречные шумы усиленного спонтанного излучения. Справедливость модели подтверждена сопоставлением результатов расчетов с результатами, полученными другими исследователями.

EDFA, оптический усилитель, волокно, легированное ионами эрбия, математическая модель, многоканальный сигнал, многоканальная накачка, попутная накачка, встречная накачка, усиленное спонтанное излучение, коэффициент усиления.

Оптические усилители (ОУ), создаваемые на основе кварцевого волокна, легированного ионами эрбия, (*Erbium Doped Fiber Amplifier* – EDFA) широко используются в волоконно-оптических системах передачи с применением технологии плотного спектрального мультиплексирования (*Dense Wavelength Division Multiplexing* – DWDM) для усиления многоканального оптического сигнала. Целью данной работы является разработка математической модели однокаскадного ОУ EDFA, которая может быть использована разработчиками этих для проверки справедливости принимаемых проектных решений. Предлагаемая модель отличается от известных [1, 2] возможностью моделирования ОУ с многоканальными источниками сигнала и накачек, а также учетом зависимости его параметров от температуры.

Схема однокаскадного ОУ EDFA представлена на рисунке 1. Она включает активное волокно, многоканальные источники входного оптического сигнала и попутной и встречной накачек, мультиплексоры WDM (*Wavelength Division Multiplexing*) для объединения сигнала и накачки в активном волокне, а также изоляторы, предотвращающие попадание остаточного излучения накачек и встречных шумов усиленного спонтанного излучения (УСИ) в линию и/или в предыдущие каскады усилителя.

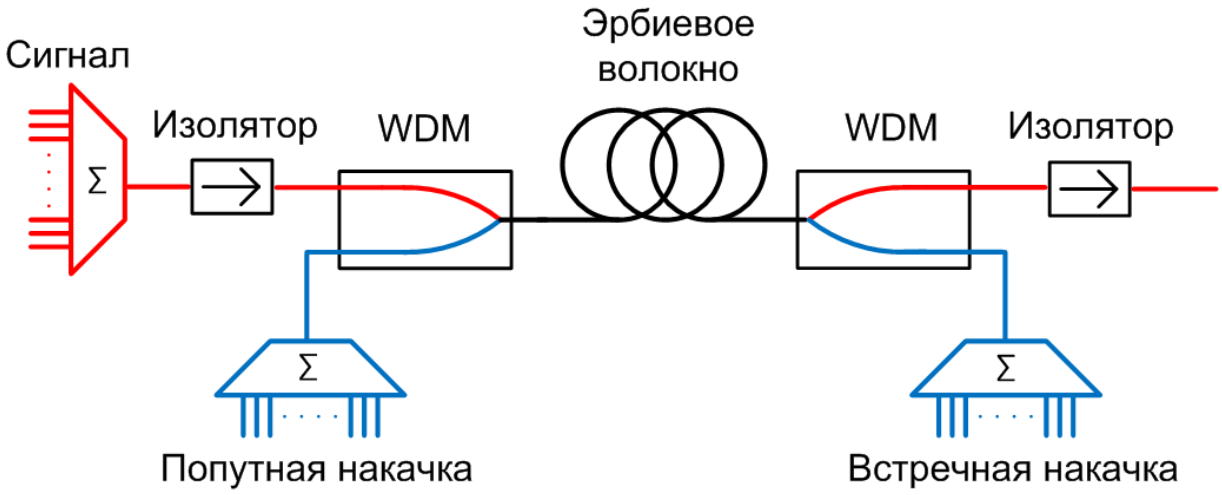


Рис. 1. Схема рассматриваемого однокаскадного усилителя EDFA

Принцип работы ОУ EDFA обычно описывается трехуровневой квантовой системой, в соответствии с которой ион эрбия Er^{3+} в активном волокне в каждый момент времени может находиться на одном из трех энергетических уровней с энергиями $E_3 > E_2 > E_1$. Уровень 1 является основным, а уровень 2 – метастабильным, то есть среднее время жизни τ иона на этом уровне существенно превышает среднее время жизни τ_{32} иона на уровне 3. Концентрацию N_i ионов, находящихся на i-ом уровне, называют населенностью этого уровня.

Накачка ОУ EDFA может осуществляться оптическим излучением с длинами волн 980 и 1480 нм. Фотоны накачки с длиной волны 980 нм, поглощаясь ионами Er^{3+}, вызывают их переходы с уровня 1 на уровень 3, а оттуда – на уровень 2. Фотоны накачки с длиной волны 1480 нм вызывают переходы ионов Er^{3+} с уровня 1 на уровень 2. При достаточной мощности накачки можно добиться инверсной населенности уровней ($N_2 > N_1$), создающей условия для усиления сигнала, фотоны которого могут вызывать вынужденные излучательные переходы ионов Er^{3+} с уровня 2 на уровень 1.

Изменения населенностей N_1, N_2, N_3 описываются системой кинетических уравнений [1, 2]:

$$\begin{cases} \frac{dN_3}{dt} = R_{13}N_1 - R_{31}N_3 - A_{32}N_3 = 0, \\ \frac{dN_2}{dt} = W_{12}N_1 + R_{12}N_1 - W_{21}N_2 - R_{21}N_2 - A_{21}N_2 + A_{32}N_3 = 0\ , \\ \frac{dN_1}{dt} = -R_{13}N_1 - W_{12}N_1 - R_{12}N_1 + R_{21}N_2 + A_{21}N_2 + R_{31}N_3 = 0, \end{cases} \quad (1)$$

где R_{ij} и W_{ij} – вероятности вынужденных переходов с уровня i на уровень j, W_{ij} – вероятности спонтанных переходов с уровня i на уровень j. Модель полагается стационарной, то есть N_1, N_2, N_3 постоянны во времени.

Решение (1) имеет вид:

$$N_1 = N\frac{\frac{A_{32}(R_{21}+W_{21}+A_{21})}{A_{32}A_{21}}}{\frac{(W_{21}+A_{21})(R_{13}+A_{32})}{A_{32}A_{21}} + \frac{R_{21}(R_{13}+A_{32})}{A_{32}A_{21}} + \frac{A_{32}(W_{12}+R_{12})}{A_{32}A_{21}} + \frac{R_{13}}{A_{21}}},$$

$$N_2 = N\frac{\frac{A_{32}(W_{12}+R_{12}) + A_{32}R_{13}}{A_{32}A_{21}}}{\frac{(W_{21}+A_{21})(R_{13}+A_{32})}{A_{32}A_{21}} + \frac{R_{21}(R_{13}+A_{32})}{A_{32}A_{21}} + \frac{A_{32}(W_{12}+R_{12})}{A_{32}A_{21}} + \frac{R_{13}}{A_{21}}}, \quad (2)$$

$$N_3 = N\frac{\frac{R_{13}(R_{21}+W_{21}+A_{21})}{A_{32}A_{21}}}{\frac{(W_{21}+A_{21})(R_{13}+A_{32})}{A_{32}A_{21}} + \frac{R_{21}(R_{13}+A_{32})}{A_{32}A_{21}} + \frac{A_{32}(W_{12}+R_{12})}{A_{32}A_{21}} + \frac{R_{13}}{A_{21}}},$$

где $N = N_1 + N_2 + N_3$ – концентрация ионов Er^{3+}.

Поскольку $\tau_{32} << \tau$, предположим, что ионы эрбия с уровня 3 сразу переходят на уровень 2, то есть $A_{32} = 1 / \tau_{32} \rightarrow \infty$, и, учитывая, что $A_{21} = 1 / \tau$, получим:

$$N_1 = N\frac{\tau W_{21}+\tau R_{21}+1}{(\tau W_{21}+1)+\tau R_{21}+\tau(W_{12}+R_{12})+\tau R_{13}}, \quad (3)$$

$$N_2 = N\frac{\tau(W_{12}+R_{12})+\tau R_{13}}{(\tau W_{21}+1)+\tau R_{21}+\tau(W_{12}+R_{12})+\tau R_{13}},\ N_3 = 0.$$

Вероятности переходов R_{ij} и W_{ij} согласно [1, 2] определяются как:

$$W_{12} = \sum\frac{(P_s+P_{ASE}^-+P_{ASE}^+)\cdot a_{12}}{h\nu_s\tau\varepsilon},\ W_{21} = \sum\frac{(P_s+P_{ASE}^-+P_{ASE}^+)\cdot g_{21}^*}{h\nu_s\tau\varepsilon},$$
$$R_{12} = \sum\frac{(P_{p1480}^+ + P_{p1480}^- + P_{ASE}^- + P_{ASE}^+)\cdot a_{12}}{h\nu_p\tau\varepsilon} \quad (4)$$
$$R_{21} = \sum\frac{(P_{p1480}^+ + P_{p1480}^- + P_{ASE}^- + P_{ASE}^+)\cdot g_{21}^*}{h\nu_p\tau\varepsilon},$$
$$R_{13} = \sum\frac{(P_{p980}^+ + P_{p980}^-)\cdot a_{31}}{h\nu_{p980}\tau\varepsilon},\ \varepsilon = \frac{\pi b_{eff}^2 N}{\tau}$$

где h – постоянная Планка, ν_s – частота сигнала, ν_{p1480} и ν_{p980} – частоты накачек 1480 нм и 980 нм, ε – параметр насыщения волокна, a_{12} и g_{21}^* – коэффициенты поглощения и усиления в полосе сигнала и накачки 1480 нм, a_{13} – коэффициент поглощения в полосе накачки 980 нм, b_{eff} – эффективный радиус распределения ионов эрбия по сечению сердцевины легированного волокна, P_s – мощность сигнала, P_{p1480}^+ и P_{p1480}^-, P_{p980}^+ и P_{p980}^-, P_{ASE}^+ и P_{ASE}^- – мощности накачек 1480 и 980 нм и шумов УСИ (ASE) в попутном (+) и встречном (–) направлениях.

Из (3) и (4) следует:

$$N_{2.\text{отн}} == \frac{\sum\frac{(P_s+P_{ASE}^-+P_{ASE}^+)\cdot a_{12.s}}{h\nu_s\varepsilon} + \sum\frac{(P_{p1480}^+ + P_{p1480}^- + P_{ASE}^- + P_{ASE}^+)\cdot a_{12.p}}{h\nu_{p1480}\varepsilon} + \sum\frac{(P_{p980}^+ + P_{p980}^-)\cdot a_{31.p}}{h\nu_{p980}\varepsilon}}{\sum\frac{(P_s+P_{ASE}^-+P_{ASE}^+)\cdot (a_{12.s}+g_{21.s}^*)}{h\nu_s\varepsilon} + \sum\frac{(P_{p1480}^+ + P_{p1480}^- + P_{ASE}^- + P_{ASE}^+)\cdot (a_{12.p}+g_{21.p}^*)}{h\nu_{p1480}\varepsilon} + \sum\frac{(P_{p980}^+ + P_{p980}^-)\cdot a_{31.p}}{h\nu_{p980}\varepsilon} + 1}, \quad (5)$$
$$N_{1.\text{отн}} = 1 - N_{2.\text{отн}}$$

где $N_{1.\text{отн}} = N_1 / N$ и $N_{2.\text{отн}} = N_1 / N$ – относительные населенности уровней N_1 и N_2.

Для учета зависимости a_{12}, a_{13} и g_{21}^* от температуры T справедливы выражения [3]:

$$a_{12}(\lambda,T) = a_{12}(\lambda,\infty)\cdot e^{\frac{\beta_{12}(\lambda)}{K\cdot T}},\ a_{13}(\lambda,T) = a_{13}(\lambda,\infty)\cdot e^{\frac{\beta_{13}(\lambda)}{K\cdot T}},$$
$$g_{21}^*(\lambda,T) = g_{21}^*(\lambda,\infty)\cdot e^{\frac{\beta_{21}(\lambda)}{K\cdot T}} \quad (6)$$

где K – постоянная Больцмана, $a_{12}(\lambda, \infty)$ и $\beta_{12}(\lambda)$, $a_{13}(\lambda, \infty)$ и $\beta_{13}(\lambda)$, $g^*_{21}(\lambda, \infty)$ и $\beta_{21}(\lambda)$ – коэффициенты, которые можно определить по известным зависимостям соответствующих коэффициентов поглощения и усиления от длины волны при двух разных температурах.

Распределение мощностей сигнала и накачек по длине эрбиевого волокна описывается уравнениями распространения [1, 2]:

$$\begin{gathered}\frac{dP_{p1480}^{\pm}}{dz} = \mp P_{p1480}[a_{12}(1 - N_{2.\text{отн}}) - g_{21}^{*}N_{2.\text{отн}}] \mp \alpha_{p.\text{доп}}P_p, \\ \frac{dP_{p980}^{\pm}}{dz} = \mp P_{p980}[a_{13}(1 - N_{2.\text{отн}})] \mp \alpha_{p.\text{доп}}P_p\ , \\ \frac{dP_s}{dz} = P_s[g_{21}^{*}N_{2.\text{отн}} - a_{12}(1 - N_{2.\text{отн}})] - \alpha_{s.\text{доп}}P_s, \\ \frac{dP_{ASE}^{\pm}}{dz} = \pm P_{ASE}^{\pm}[g_{21}^{*}N_{2.\text{отн}} - a_{12}(1 - N_{2.\text{отн}})] \pm 2g_{21}^{*}N_{2.\text{отн}}hv_s\Delta v \mp \alpha_{s.\text{доп}}P_{ASE}^{\pm},\end{gathered} \quad (7)$$

где $\alpha_{p.\text{доп}}$ и $\alpha_{s.\text{доп}}$ – коэффициенты, учитывающие потери в активном волокне, которые вызваны релеевским рассеянием и поглощением (кроме поглощения ионами эрбия) излучения в материале активного волокна.

Выражения (7) позволяют найти мощности сигнала, накачек и шумов УСИ в любой точке волокна.

Для проверки правильности предложенных соотношений было проведено моделирование двух ОУ EDFA с многоканальным входным сигналом с равномерным расположением 100 каналов в диапазоне 1500–1600 нм и мощностью 1 мкВт/канал. Расчеты проведены при параметрах, приведенных в таблице. Некоторые результаты представлены на рисунках 2 и 3.

ТАБЛИЦА. Параметры моделируемых ОУ EDFA

Параметр	Усилитель 1	Усилитель 2
Марка активного волокна	М-5	I-4
Параметр насыщения активного волокна, 1/(м·с)	$3{,}047 \cdot 10^{15}$	$3{,}091 \cdot 10^{15}$
Температура, ^{0}C	25	0
Длина активного волокна, м	15	10
Вид накачки	попутная	встречная
Длина волны накачки, нм	980	1480
Ширина спектра накачки, нм	1,0	1,0
Мощность накачки, мВт	100	50

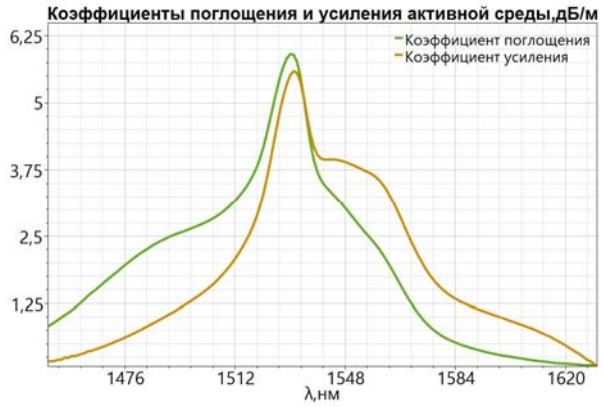
Аналогичные расчеты были проведены с помощью программы Fibercore GainMaster. Из рисунков 2*в* и 3*в* видно, что результаты моделирования хорошо совпадают, что подтверждает справедливость предложенной модели.

Список используемых источников

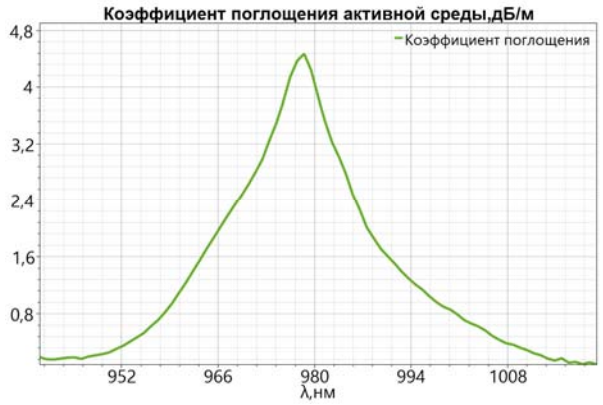
1. Becker P. C., Olsson N. A., Simpson J. R. Erbium-Doped fiber amplifiers. Fundamentals and Technology // Academic Press, 1997. 627 p. ISBN 978-0-12-084590-3.

2. Desurvire E. Erbium-Doped fiber amplifiers. Principles and applications. John Wiley & Sons, New York, 1994. 770 pp. ISBN 0-471-58977-2.

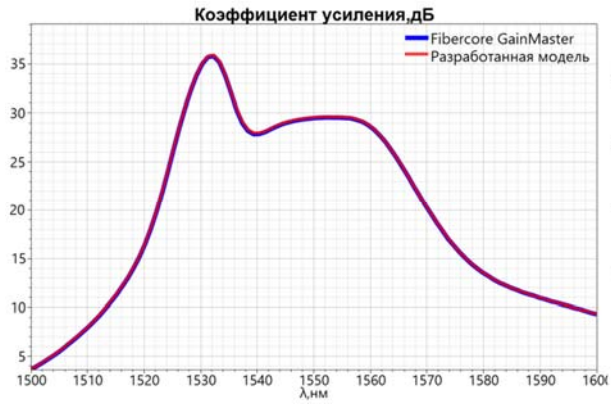
3. Hee Gap Park, Seung Chul Yun, Young Jun Jin. Er-doped Superfluorescent Fiber Source with Thermally Stable Mean Wavelength // Journal of the Optical Society of Korea Vol. 13, No. 2, June 2009, pp. 240–244.



а)

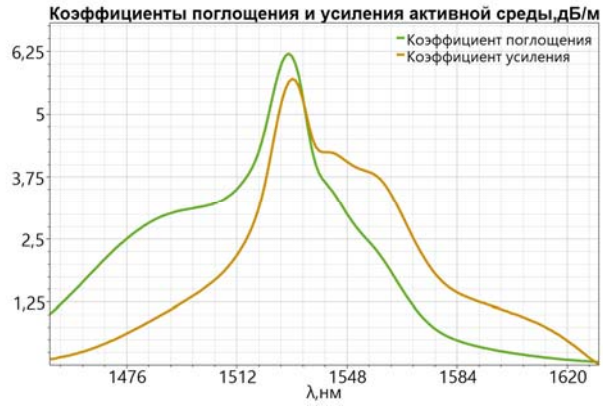


б)



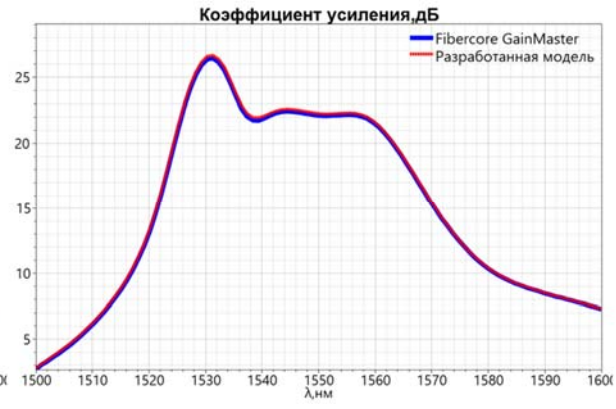
в)

Рис. 2. Результаты расчета усилителя 1



а)

б)



в)

Рис. 3. Результаты расчета усилителя 2

а), б) коэффициенты поглощения и усиления активной среды при заданной температуре, в) коэффициент усиления усилителя

УДК 004.042:004.91;351.9

ПРОБЛЕМНЫЕ ВОПРОСЫ СОЗДАНИЯ И ИСПОЛЬЗОВАНИЯ НАБОРОВ ОТКРЫТЫХ ДАННЫХ ОРГАНОВ ГОСУДАРСТВЕННОЙ ВЛАСТИ

Л. А. Виткова, О. Н. Рябова, Д. В. Сахаров

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

Открытые данные являются частью глобальных концепций Государственной политики открытости и Государственной политики инноваций. Однако при создании и использовании наборов открытых данных возникает ряд проблем. В статье описаны понятие, концепция и структура открытых данных, существующие проблемы их создания и распространения, возможные пути решения.

открытые данные, стандарт открытости, общедоступные данные, открытое правительство, открытые ресурсы, публичные данные, мониторинг.

После выхода Указа Президента от 7 мая 2012 года N 601 «Об основных направлениях совершенствования системы государственного управления» у государственных органов появилось обязанность размещать в сети Интернет данные, содержащиеся в информационных системах органов государственной власти Российской Федерации в форме открытых данных.

Открытые данные являются частью Концепции Государственной политики открытости, Государственной политики инноваций. В основе идеологии открытых данных лежит законодательно закрепленная мысль о том, что граждане имеют право знать, получать информацию, созданную на деньги налогоплательщиков, должны иметь доступ к информации по запросу и по умолчанию. Обязанность раскрытия информации регламентирована многими документами, но после подписания в июне 2013 г. Хартии Открытых данных G8 к ним прибавились серьезные международные обязательства [1].

Определение: под открытыми данными понимается информация, созданная в пределах своих полномочий государственными органами, органами местного самоуправления или организациями, подведомственными государственным органам, органам местного самоуправления, либо поступившая в указанные органы и организации, которая подлежит размещению в сети Интернет в формате, обеспечивающем её автоматическую обработку в целях повторного использования без предварительного изменения человеком (машиночитаемый формат), и может свободно использоваться в любых соответствующих закону целях любыми лицами независимо от формы её размещения [2, 3].

Следует обратить внимание, что отличительными признаками открытых данных является не только общедоступность информации, но также ее представление в машиночитаемом формате. Понятие открытых данных может применяться не только к государственному сектору, но и к любым наборам информации, если она не является информацией ограниченного доступа и не отнесена к государственной тайне. Одновременно этим законом защищаются права обладателей информации, доступ к которой ограничен в соответствии с федеральными законами, и права субъектов персональных данных.

Суть концепции открытых данных: полнота (информация должна быть предоставлена в полном объеме); первичность (публикация данных «сырыми, как есть», без фильтрования); своевременность (оперативное открытие данных общественности, опубликованные наборы должны быть актуальными); доступность (без каких-либо уровней доступа, такие данные по определению открыты и доступны всем желающим для ознакомления и дальнейшего использования); пригодность к машинной обработке; отсутствие дискриминации по доступу (данные должны открываться одинаково как на разных типах браузеров, так и в разных операционных системах); обязательное использование открытых форматов (использование специальных форматов XML, CSV, RDF и JSON, а не DOC, PDF и т. д.); лицензионная чистота (процесс получения данных должен быть юридически чист).

Какие именно сведения должны быть открыты, определено в Перечне общедоступной информации, размещаемой государственными органами и органами местного самоуправления в Интернете в форме открытых данных [4]. Установлены конкретные форматы представления данных, а также требования к структуре наборов данных, которые, помимо файлов данных, представленных в определенном формате, должны содержать реестр набора, паспорт набора, указание на должностное лицо, ответственное за размещение набора открытых данных, периодичность обновления, указание на предыдущие наборы [5]. Развитием работы по открытию государственных данных является постепенный переход к более перспективным современным моделям открытых данных – RDF (*Resource Description Framework*), а в последующем и к модели связанных данных (*Linked data*).

Существующий международный опыт позволяет корректно решить вопрос лицензий. Для открытых данных применяется подход «some rights reserved» – «некоторые права сохранены», в отличие от стандартного подхода копирайта «все права сохранены». Подобный подход реализует семейство лицензий Open Data Commons (ODbL), которые по сути представляют собой контрактное соглашение для пользователей Баз данных, требующим от них специфического поведения в обмен на предоставление доступа к БД. Эти соглашения предполагают, что Пользователь вправе использовать (в том числе повторно) открытые данные свободно, бессрочно, безвозмездно и без ограничения территории использования, в том числе имеет

право копировать, публиковать, распространять открытые данные, видоизменять открытые данные и объединять их с другой информацией, использовать открытые данные в коммерческих целях, использовать для создания программ для ЭВМ и приложений. Владелец (создатель, публикатор) открытых данных обязан требовать от Пользователя выполнения только следующих условий:

a) использовать открытые данные только в законных целях;

b) убедиться, что он не искажает открытые данные при их использовании;

c) сохранять ссылку на источник информации при использовании открытых данных и, по возможности, дать ссылку на соглашение, в соответствии с которым используются открытые данные.

На сегодняшний день наборы открытых данных размещены на официальных сайтах практически всех министерств и ведомств. Созданы государственные информационные порталы, предоставляющие площадку для работы с наборами открытых данных, на которых аккумулируется методологическая, аналитическая, экспертная и техническая информация. На основе размещаемых наборов данных созданы и успешно работают некоторые бизнес-проекты. Однако бум создания большого числа наборов данных и стремительное развертывание информационных проектов по открытости сопровождается вполне закономерным отставанием в области использования этих данных, неготовностью гражданского и бизнес-сообщества, выявлением новых аспектов и проблем.

Проблемы и возможные решения:

– выложенные данные потенциально полезны, но для подавляющего числа возможных пользователей неинтересны [6, 7, 8]. Решение: раскрытие государственными органами той информации, которая реально востребована. Оценка востребованности [9]. На ресурсах, содержащих наборы открытых данных, проводить мониторинг скачиваний, создать автоматическую систему слежения за распространением наборов. Возможно, использовать методы мониторинга, подобные тем, что применяются для защиты информации.

– наборы открытых данных имеют довольно низкий уровень связности, часто плохо описаны – информация, позволяющая работать с данными, минимальна, для осуществления программирования или просто осмысленного использования набор данных необходимо изучать самостоятельно [7, 8, 10]. Решение: развитие журналистики данных, создание партнерских отношений с коммерческими структурами, проведение своими силами серьезной исследовательской работы.

– пользователи сами должны искать простые и удобные инструменты для работы с открытыми данными в типовых форматах, новое информационное неравенство [6, 10, 11, 12]. Решение: Размещение средств просмотра, визуализации, а также средств для разработчиков приложений на порталах открытых данных.

– сегодня весь массив существующих наборов открытых данных напоминает ранний Интернет в том смысле, что информации много, но ориентироваться в ней непросто. Решение: Нужно, чтобы открытые данные отыскивались обычными машинами поиска (Google, Яндекс и т. д.). Разработка большого числа разнообразных приложений, использующих информацию, размещенную в форме открытых данных, в том числе для мобильных устройств. Основной целью следующего этап раскрытия данных является переход от накопления опубликованных наборов к построению системы управления информацией

Какие риски несет раскрытие открытых? Большая часть аккумулируемой органами власти информации относится к чьим-то правам – граждан или юридических лиц. Развитие технологий (в частности, технологии больших данных) в ближайшее время существенно увеличит риски извлечения секретных и конфиденциальных (в том числе персональных) данных из раскрываемой государственными органами информации. Нельзя недооценивать возможность умышленной или неумышленной неверной интерпретации данных, применения к ним неподходящих методов анализа. Более сложной проблемой может стать синергетический эффект при агрегировании сведений из множества открытых источников. Продукт агрегации будет принадлежать его авторам и может создать почву для манипуляций недобросовестных лиц [10, 13].

Эксперты указывают также на риск того, что из наших открытых данных другие страны-конкуренты извлекут намного больше пользы в ущерб российским компаниям. Международный опыт раскрытия данных показывает, что серьезной обработкой открытых данных могут заниматься лишь люди и организации, располагающие необходимыми знаниями, опытом, вычислительными ресурсами и высококвалифицированными кадрами, и в этом плане Россия пока не входит в число лидеров. Бессистемное открытие данных, находящихся в распоряжении госорганов, при сопоставлении информации может сработать против граждан, против независимости и целостности страны [10, 13, 14].

Оценка, определение стратегических задач – поле деятельности правительственной комиссии и экспертного сообщества. Непосредственные создатели наборов открытых данных – госструктуры различного уровня, должны проводить мониторинг использования созданных наборов откры-

тых данных, поскольку именно им придется нести бремя расходов на предоставление открытых данных и реагирование на последствия их незапланированного или несанкционированного применения.

Список используемых источников

1. Хартия открытых данных «Группы восьми» [Электронный ресурс] // Портал открытых данных Российской федерации. Минэкономразвития России, 2016 г. URL: http://data.gov.ru/hartiya-otkrytyh-dannyh-gruppy-vosmi (дата обращения 27.02.2016).

2. Об информации, информационных технологиях и о защите информации: федер. закон Рос. Федерации от 27 июля 2006 г. № 149-ФЗ: принят Гос. Думой Федер. Собр. Рос. Федерации 8 июля 2006 г.: одобр. Сов. Федерации Федер. Собр. Рос. Федерации 14 июля 2006 г. // Рос. газ. 2006. 29 июля.

3. О внесении изменений в федеральный закон «Об информации, информационных технологиях и о защите информации» и федеральный закон «Об обеспечении доступа к информации о деятельности государственных органов и органов местного самоуправления: федер. закон Рос. Федерации от 07 июня 2013 г. № 112-ФЗ: принят Гос. Думой Федер. Собр. Рос. Федерации 24 мая 2013 г.: одобр. Сов. Федерации Федер. Собр. Рос. Федерации 29 мая 2013 г. // Рос. газ. 2013. 11 июня.

4. Распоряжение Правительства Рос. Федерации, 10 июля 2013, № 1187-р [Электронный ресурс] // Government.ru: официальный портал Правительства РФ. URL: http://government.ru/media/files/41d47b3285a74fa56c88.pdf (дата обращения 17.04.2016).

5. Методические рекомендации по реализации принципов открытости в ФОИВ. Протокол Правительственной комиссии по координации деятельности открытого правительства от 26 декабря 2013 г. N АМ-П36-89пр) [Электронный ресурс] // Портал открытых данных. URL: http://data.gov.ru/metodicheskie-rekomendacii-po-realizacii-principov-otkrytosti-v-federalnyh-organah-ispolnitelnoy (дата обращения 21.03.2016).

6. Дмитриева Н. Е., Жулин А. Б., Солонцова Л. В., Стырин Е. М. Пять шагов к открытости: итоги первого экспертного мониторинга открытости ФОИВ: публичный доклад // Нац. исслед. ун-т «Высшая школа экономики». М. : Изд. дом Высшей школы экономики, 2015.

7. План мероприятий «Открытые данные Российской Федерации». Протокол заседания Правительственной комиссии по координации деятельности открытого правительства от 25 декабря 2014 г. № 10) [Электронный ресурс] // Портал открытых данных. URL: http://opendata.open.gov.ru/upload/iblock/2bd/2bd533adb07b9f91c53d286f3aca5d 39.pdf (дата обращения 21.03.2016)

8. Колесов А. «Открытые данные» и «открытое правительство» – в чем разница? [Электронный ресурс] // Издание PC Week/RE («Компьютерная неделя») 20.01.2014. URL: http://pcweek.ru/gover/article/detail.php?ID=158850 (дата обращения 27.02.2016).

9. Методика мониторинга и оценки востребованности открытых данных. [Электронный ресурс] // Официальный сайт Минфина России. URL: http://minfin.ru/common/upload/library/2014/12/main/metodika_ocenki.pdf (дата обращения 07.04.2016).

10. Храмцовская Н. В. Открытые данные: к чему готовиться? // Делопроизводство и документооборот на предприятии. 2013. № 11 [Электронный ресурс] // Портал открытых данных. URL: http://data.gov.ru/hartiya-otkrytyh-dannyh-gruppy-vosmi (дата обращения 27.02.2016).

11. Бегтин И. Открытые данные как основа открытого государства [Электронный ресурс] // Блог И. Бегтина. URL: ivan.begtin.name (дата обращения 27.02.2016).

12. Владимирский А. Н. День защитника Открытых данных. [Электронный ресурс] // Сайт Экспертного центра. URL: http://d-russia.ru/den-zashhitnika-otkrytyx-dannyx.html (дата обращения 27.02.2016).

13. Марков А. П. Открытые данные в информационных системах открытых данных [Электронный ресурс] // Блог группы компаний «Эшелон», 11.02.2013. URL: s3r.ru/2013/02/zakonodatelstvo/open_data (дата обращения 27.02.2016).

14. Дорожная карта «Открытые данные Российской Федерации на 2015–2016 гг.» [Электронный ресурс] // Портал открытых данных. URL: http://open.gov.ru/events/5511205/ (дата обращения 29.03.2016).

УДК 621.391

О МАЖОРИТАРНОМ ДЕКОДИРОВАНИИ УКОРОЧЕННОГО КОДА МАКСИМАЛЬНОЙ ДЛИНЫ ПО *K* ЛИНЕЙНО-НЕЗАВИСИМЫМ ЭЛЕМЕНТАМ

С. С. Владимиров

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

В работе рассматривается алгоритм мажоритарного декодирования укороченного кода максимальной длины по k линейно-независимым элементам. Приводится способ укорочения кодов максимальной длины и предлагаются варианты оптимальных укороченных кодов согласно минимальному кодовому расстоянию. Рассматривается вариант применения алгоритма для обнаружения ошибок в комбинации укороченного кода максимальной длины.

код максимальной длины, мажоритарное декодирование, помехоустойчивое кодирование, вероятностные характеристики, обнаружение ошибок/

Код максимальной длины представляет из себя подвид эквидистантного помехоустойчивого кода (т. е. кода, в котором расстояние между любыми двумя различными кодовыми словами одинаково), кодовые слова которого представляют собой псевдослучайные двоичные рекуррентные последовательности максимальной длины, так называемые М-последовательности, построенные над двоичным полем Галуа [1].

Последовательность максимальной длины – это псевдослучайная двоичная последовательность максимального периода над двоичным расширенным полем Галуа GF(2^m), образуемым порождающим полиномом $p(x)$, который должен обладать свойствами неприводимости и примитивности. Для формирования М-последовательности используется аппаратная схема либо программный алгоритм.

Аппаратная схема реализуется на основе регистра сдвига с линейной обратной связью, который строится, исходя из вида порождающего полинома поля Галуа $p(x)$. Следовательно, полином $p(x)$ можно считать порождающим полиномом как М-последовательности, так и соответствующего ей кода максимальной длины.

В программном алгоритме М-последовательность рассматривается как рекуррентная последовательность $\{\mathbf{s}\}$, выраженная через функцию-след $T(x)$ элемента поля Галуа [1, 2]:

$$\{\mathbf{s}\} = [s_0, s_1, \dots, s_{2^m-2}] = \left[T(\varepsilon^z), T(\varepsilon^{z+1}), \dots, T\left(\varepsilon^{z+2^m-2}\right)\right] = \\ = \left[T(c), T(c\varepsilon), \dots, T\left(c\varepsilon^{2^m-2}\right)\right],$$

где $c = \varepsilon^z$ – начальная фаза M-последовательности, которая является элементом поля Галуа GF(2^m).

Функция-след $T(x)$ для элемента ε^i поля GF(2^m) рассчитывается как

$$T\left(\varepsilon^i\right) = \varepsilon^i + \left(\varepsilon^i\right)^2 + \left(\varepsilon^i\right)^{2^2} + \dots + \left(\varepsilon^i\right)^{2^{m-1}} = \sum_{j=0}^{m-1} \left(\varepsilon^i\right)^{2^j}.$$

Совокупность М-последовательностей $\{\mathbf{s}\}$, построенных над полем Галуа GF(2^m) для возможных начальных фаз, образует помехоустойчивый (n, k) код максимальной длины, где количество информационных элементов k равно степени поля Галуа m, а длина кода n равна периоду М-последовательности $2^k - 1$. Этот код можно рассматривать как систематический, предполагая, что информационными являются первые k элементов последовательности, и как несистематический – в этом случае информационными элементами является начальная фаза М-последовательности. Минимальное кодовое расстояние такого кода равно $2^k - 1$.

Укорочение кода максимальной длины производится путем отбрасывания элементов с конца кодового слова. Например, если взять код максимальной длины (15, 4), и отбросить один символ с конца каждого кодового слова, то будет получен укороченный код (14, 4). В таблице 1 показан пример укорочения комбинации кода максимальной длины (15, 4) до 14, 12 и 8 разрядов.

ТАБЛИЦА 1. Пример укорочения комбинации кода максимальной длины (15, 4)

Параметры кода	Кодовая комбинация
(15,4)	0 0 1 1 0 1 0 1 1 1 1 0 0 0 1
(14,4)	0 0 1 1 0 1 0 1 1 1 1 0 0 0
(12,4)	0 0 1 1 0 1 0 1 1 1 1 0
(8,4)	0 0 1 1 0 1 0 1

Такие укороченные коды теряют свойство эквидистантности. С укорочением кодовых слов уменьшается и минимальное кодовое расстояние получающегося помехоустойчивого кода. Графики изменения минимального кодового расстояния с изменением длины кода показаны на рисунке 1. Из укороченных КМД на основе кода (15,4) можно выделить коды (14,4), (12,4) и (8,4), имеющие минимальное кодовое расстояние, равное 7, 5 и 3, соответственно. Они гарантированно исправляют соответственно 3, 2 и 1 кратные ошибки.

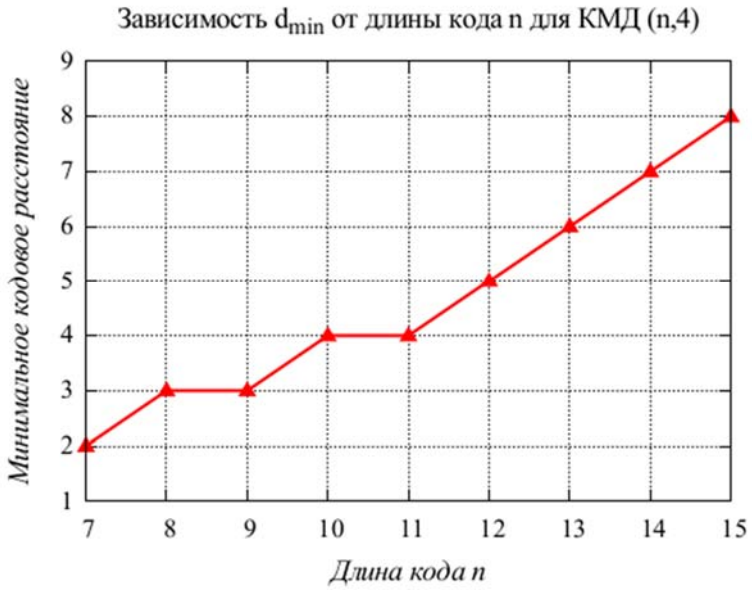


Рис. 1. Графики изменения минимального кодового расстояния укороченного кода максимальной длины с изменением длины кода

Для решения задачи декодирования кода максимальной длины выбираются k линейно-независимых элементов последовательности $\{\mathbf{s}\}$, а именно $s_{i_1}, s_{i_2}, s_{i_3}, \ldots, s_{i_k}$, из которых составляется система уравнений:

$$s_{i_1} = T\left(\varepsilon^{z+i_1}\right) = T\left(c\varepsilon^{i_1}\right) = f_1(a_0, a_1, \ldots, a_{k-1}),$$
$$s_{i_2} = T\left(\varepsilon^{z+i_2}\right) = T\left(c\varepsilon^{i_2}\right) = f_2(a_0, a_1, \ldots, a_{k-1}),$$
$$\ldots$$
$$s_{i_k} = T\left(\varepsilon^{z+i_k}\right) = T\left(c\varepsilon^{i_k}\right) = f_k(a_0, a_1, \ldots, a_{k-1}),$$

где a_0, a_1, …, a_{k-1} – коэффициенты разложения начальной фазы c кода максимальной длины по левому степенному базису поля Галуа, то есть, двоичное представление начальной фазы c [1, 2].

Данную систему уравнений можно преобразовать в матричный вид:

$$\boldsymbol{S} = \boldsymbol{\Theta} \cdot \mathbf{A},$$

где **S** – вектор-столбец k линейно-независимых элементов; **Θ** – матрица коэффициентов, имеющая однозначное соответствие с позициями линейно-независимых элементов в комбинации кода максимальной длины и не зависящая от начальной фазы; **A** – вектор-столбец коэффициентов начальной фазы c (равен начальной фазе) [1, 2].

Если эта система уравнений линейно-независима, то ее решение относительно элементов a_0, a_1, …, a_{k-1} дает векторное представление элемента $c = \varepsilon^z$, определяющего начальную фазу последовательности $\{\mathbf{s}\}$. Формула для решения вышеприведенной системы уравнений имеет вид:

$$\mathbf{A} = \mathbf{\Theta^{-1}} \cdot \mathbf{S},$$

где $\mathbf{\Theta^{-1}}$ – обратная матрица для матрицы **Θ** [1, 2].

Таким образом, любые k линейно-независимых элементов комбинации кода максимальной длины позволяют вычислить ее начальную фазу. Если же в кодовой комбинации есть ошибка, то те комбинации k линейно-независимых элементов, которые попадают на ошибку, дадут при вычислении начальной фазы c другой результат. Перебором всех k-элементных линейно-независимых комбинаций **S** и соответствующих им обратных матрицы организуется мажоритарная обработка [1, 2].

Этот алгоритм верен и для систематического и для несистематического кода максимальной длины. Отличие состоит в том, что для несистематического кода информационные элементы получаются сразу (они являются начальной фазой кодовой комбинации), а в систематическом коде их необходимо рассчитать по полученной начальной фазе.

Линейно-независимые элементы удобно вычислить заранее. При программной реализации декодера их удобно хранить в виде так называемых масок, которые при поэлементном логическом умножении с кодовой комбинацией дают значения k линейно-независимых элементов. В таблице 2 показаны примеры масок для кодов (14,4), (12,4) и (8,4).

ТАБЛИЦА 2. Примеры масок для кодов (14,4), (12,4) и (8,4)

(14,4)		(12,4)		(8,4)	
№	Маска	№	Маска	№	Маска
1	11110000000000	1	111100000000	1	11110000
2	11100010000000	2	111000100000	2	11100010
…	…	…	…	…	…
615	00000000010111	303	000000010111	44	00010111
616	00000000001111	304	000000001111	45	00001111

На рисунке 2 показан вариант использования алгоритма для обнаружения ошибок в кодовой комбинации укороченного кода максимальной длины.

Результаты моделирования алгоритма обнаружения ошибок для укороченного кода (8, 4) показаны на рисунке 3. Код обнаруживает все ошибки за исключением тех, которые приводят к преобразованию кодовой комбинации в другую разрешенную кодовую комбинацию. Для каждой кодовой комбинации кода (8, 4) есть всего 15 таких ошибок из 255 возможных комбинаций ошибочных разрядов.

Рис. 2. Алгоритм обнаружения ошибок в кодовой комбинации укороченного кода максимальной длины по k линейно-независимым элементам

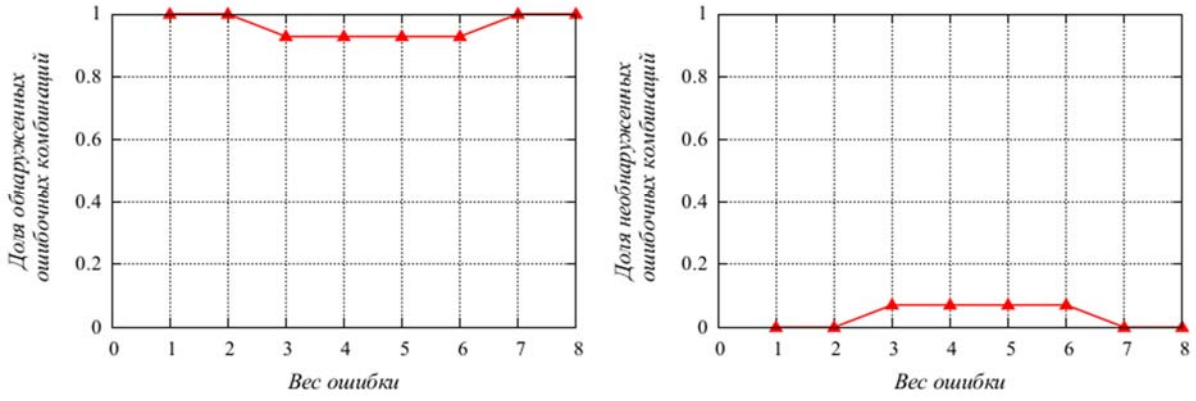


Рис. 3. Результаты использования укороченного кода (8, 4) для обнаружения ошибок

Список используемых источников

1. Когновицкий О. С. Двойственный базис и его применение в телекоммуникациях. СПб : Линк, 2009. 424 с. ISBN 978-5-98595-020-5.

2. Владимиров С. С. Моделирование процессов мажоритарного декодирования комбинации эквидистантного кода по К линейно-независимым элементам // Научно-технические ведомости Санкт-Петербургского государственного политехнического университета. Информатика. Телекоммуникации. Управление. 2010. Т. 3. № 101. С. 149–156.

УДК 004.056

ЗАДАЧИ ПОСТРОЕНИЯ СИСТЕМЫ ОБЕСПЕЧЕНИЯ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ ТИПОВОГО ОБЪЕКТА МЧС РОССИИ

Д. С. Власов

Северо-Западный региональный центр МЧС России

В статье раскрывается содержание основных задач построения системы обеспечения информационной безопасности типового объекта МЧС России. Во-первых, это анализ современного состояния вопроса информационной безопасности на объектах МЧС России. Во-вторых – синтез комплекса средств противодействия угрозам нарушения информационной безопасности для типового объекта защиты МЧС России. В-третьих – формирование политики обеспечения информационной безопасности объекта МЧС России регионального уровня. И в-четвертых – оценка эффективности системы обеспечения информационной безопасности типового объекта МЧС России.

угрозы информационной безопасности, политика информационной безопасности, оценка эффективности системы обеспечения информационной безопасности.

Тема неразрывно связана с «Концепцией информационной безопасности МЧС России» [1], определяющей систему взглядов на существующую проблему обеспечения безопасности информации. Ее обострение обусловлено ростом количества угроз информационной безопасности объектам сложных организационно-технических систем во всех сферах жизнедеятельности государства и потенциальным ущербом от их «успешной» реализации – с одной стороны и отсутствием на сегодняшний день необходимой организации полноценной защиты информации в подразделениях МЧС России – с другой. Разрешением указанного противоречия является обеспечение информационной безопасности МЧС России с системных позиций – то есть, разработка системы обеспечения информационной безопасности для всех типовых объектов, в частности, региональных центров МЧС России.

Если говорить об экономической составляющей проблемы, то в условиях сокращения средств на обеспечение информационной безопасности решение лежит в плоскости оптимизации стоимости защитных мероприятий путем риск-менеджмента ценности защищаемых активов и актуальности угроз при отрицательном балансе потенциального ущерба от реализации последних. Позитивным фактором здесь является то, что все объекты информатизации МЧС России являются в основном типовыми, например, региональный центр [2], и поэтому разработанная для них система обеспечения информационной безопасности может быть растиражирована, а при некоторой адаптации – и отмасштабирована по вертикали.

В этих обстоятельствах актуальным является исследование, направленное на повышение степени защищенности и обеспечение информационной безопасности типового объекта МЧС России и внешних и внутренних угроз путем разработки соответствующей системы, что потребует ответа на целый ряд концептуальных вопросов путем постадийного решения соответствующих научно-технических и научно-методических задач. Во-первых, это анализ современного состояния вопроса информационной безопасности на объектах МЧС России. Во-вторых – синтез комплекса средств противодействия угрозам нарушения информационной безопасности для типового объекта защиты МЧС России. В-третьих – формирование политики обеспечения информационной безопасности объекта системы управления МЧС России регионального уровня. И, в-четвертых – оценка эффективности системы обеспечения информационной безопасности регионального центра МЧС России. Далее раскроем их содержание.

Стадия 1: Анализ состояния

Для решения данной задачи необходимо собрать и систематизировать фактологию и выводы комплексных проверок состояния защиты информации на объектах МЧС России. Потребуется осуществить мониторинг внешних и внутренних угроз безопасности инфотелекоммуникационной структуры типового объекта и произвести их предварительную классификацию. Также следует провести анализ требований руководящих документов и государственных стандартов по обеспечению информационной безопасности и защите информации – ввиду их массовости, большого разнообразия и противоречивости это является далеко не тривиальным [3, 4]. В результате должны быть уточнены потребности и ревизованы возможности построения системы обеспечения информационной безопасности (далее – Система) типового объекта МЧС России. Первым прагматичным шагом в направлении построения Системы должна стать разработка инфологической схемы типового объекта класса регионального центра, для которой должны быть промоделировано множества угроз информационной безопасности [5] на предмет получения некой базовой модели.

Стадия 2: Синтез комплекса

Множественность выявленных внешних и внутренних угроз предполагает симметричную множественность защитных мер, приводящую к комплексности применение методов и средств противодействия (защиты информации) [6]. В целях минимизации множества защитных мер следует определить подмножество актуальность угроз информационной безопасности соответствующим способом, опирающимся, в том числе, на методику определения ущерба информационным ресурсам типового объекта от нарушений информационной безопасности. Также потребуется методика технико-экономического анализа средств защиты информации для типового объекта МЧС России. И собственно, необходимо осуществить синтез комплекса мер противодействия угрозам нарушения информационной безопасности для объекта уровня регионального центра МЧС России – вопрос метода формирования подобного комплекса остается открытым и требует дополнительных исследований. Но использование в его составе алгоритмов риск-менеджмента можно считать аксиоматичным.

Стадия 3: Формирование политики

Для того чтобы комплекс мер противодействия угрозам заработал необходима воля руководства, выраженная в соответствующей политике обеспечения информационной безопасности, поэтому ее формирование и проведение «в жизнь» – вопрос далеко «не праздный». Однако, ввиду «псевдоочевидности» и «ненаучности» ее содержания (инструкции, процедуры, регламенты и проч.) этому аспекту защиты информации уделяется незаслуженно мало внимания, в том числе, и со стороны научного сообщества. Как результат – отсутствие апробированных и научно-обоснованных рекомендаций по формированию и проведению политики обеспечения информационной безопасности в структуре МЧС России.

Подтверждением такого состояния вопроса могут служить результаты «пилотного проекта» по внедрению DLP-системы в контур информационной безопасности объекта класса регионального центра МЧС России, когда потенциально высокие функциональные возможности системы по перекрытию каналов утечки персональных данных натолкнулись отсутствие в политике обеспечения информационной безопасности объекта процедур интеграции средств и подсистем защиты информации.

Налицо потребность в надлежащих механизмах адаптации типовой политики обеспечения информационной безопасности для объектов МЧС России).

Стадия 4: Оценка эффективности

Оценка эффективности обеспечения информационной безопасности требуется как для оперативного управления процессом защиты информации, так и для средне- и долгосрочного планирования развития Системы. Отсутствие на сегодня комплексной методологии оценки эффективности систем подобного класса приводит к неоптимальным управленческим решениям и, как следствие, «хаотизации» вышеуказанного процесса. Ключевыми методологическими вопросами здесь являются следующие: 1) выбор и обоснование состава критериев и показателей эффективности Системы; 2) выбор и обоснование инструментария оценки эффективности защитных мер и средств; 3) организация и планирование полунатурного эксперимента по проверке эффективности защитных мер и средств на типовом объекте МЧС России; 4) обобщение и интерпретация результатов оценки эффективности Системы и 5) выработка научно-обоснованных рекомендация по ее совершенствованию. Таким образом, все ответственные лица МЧС России должны быть «вооружены» комплексной методикой [7] оценки эффективности системы обеспечения информационной безопасности типового объекта МЧС России.

Если возвращаться к экономической составляющей, то затраты на разработку подобного научно-методического средства не идут ни в какое сравнение с потерями от наиболее практикуемого способа принятия управленческих решений в сфере информационной безопасности и защиты информации методом «проб и ошибок».

Заключение

В статье поднята проблематика информационной безопасности в МЧС России, которую предлагается решать, в том числе, построением системы обеспечения информационной безопасности для регионального центра в качестве типового объекта защиты информации. Ожидается получение следующих научных результатов, обладающих несомненной новизной, а именно: базовой модели угроз нарушения информационной безопасности типового объекта МЧС России; метода формирования комплекса средств противодействия угрозам нарушения информационной безопасности для типового объекта; механизма адаптации политики обеспечения информационной безопасности для типового объекта регионального уровня; комплексной методики оценки эффективности системы обеспечения информационной безопасности типового объекта МЧС России. Можно прогнозировать определенную теоретическую и практическую значимость совокупности этих научных результатов для реализации и совершенствования «Концепции информационной безопасности МЧС России».

Список используемых источников

1. Чижиков Э. Н. Защита информации в информационных системах МЧС России // Информационные технологии, связь и защита информации МВД России. 2012. № 2. С. 14–17.

2. Приказ МЧС России от 1 октября 2004 г. № 458 «Об утверждении положения о территориальном органе МЧС России – региональном центре по делам гражданской обороны, чрезвычайным ситуациям и ликвидации последствий стихийных бедствий».

3. Буйневич М. В., Примакин А. И. Категориальный анализ проблем гармонизации нормативно-правовой базы информационной безопасности // Информационная безопасность регионов России (ИБРР-2015): материалы IX Санкт-Петербургской межрегион. конф., Санкт-Петербург, 28–30 окт. 2015 г. СПб. : СПОИСУ, 2015. С. 34–35.

4. Буйневич М. В., Владыко А. Г., Доценко С. М., Симонина О. А. Организационно-техническое обеспечение устойчивости функционирования и безопасности сети связи общего пользования. СПб. : СПбГУТ, 2013. 144 с. ISBN 978-5- 89160-087-4.

5. 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.

6. Стельмашонок Е. В. и др. Безопасность современных информационных технологий: монография. СПб. : СПбГИЭУ. 2013. 408 с.

7. Буйневич М. В., Рамазанов А. И., Хуснулин Р. Г. К вопросу о разработке структуры комплексной методики оценки выполнения операторами требований безопасности // Актуальные проблемы инфотелекоммуникаций в науке и образовании: сборник науч. трудов. II Междунар. научно-техн. и научно-метод конф., Санкт-Петербург, 26–27 февраля 2013 г. СПб. : СПбГУТ, 2013. С. 867–871.

Статья представлена научным руководителем, доктором технических наук, профессором М. В. Буйневичем.

УДК 303.732

ЭРГОНОМИКА ИНФОРМАЦИОННОГО ВЗАИМОДЕЙСТВИЯ, КАК ФАКТОР УСКОРЕНИЯ ПРОЕКТИРОВАНИЯ ИНФОРМАЦИОННЫХ СИСТЕМ

М. Ю. Волщуков, А. Ю. Иванов

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

Настоящий период обуславливается существенным влиянием эргономики при проектировании информационных систем. Все большее внимания уделяется вопросам критичности информационного обмена между техническими системами и человеком в современных условиях, а также влиянию инженерно-психологического аспекта на изменение к проектированию информационных систем. Использование методов решения вопросов эргономики информационного обмены при проектировании информационных

систем повысит качество подготовки требований на формализацию предметной области, что в свою очередь позволит сократить количество итераций, а соответственно и время на разработку системы.

эргономика, инженерная психология, предметная область, информационные системы.

Эра локальных информационных систем закончилась. Изменилось понимание информационной системы как среды взаимодействия человека и машины. Это уже не просто система, автоматизирующая определенный технологический процесс и/или локальные процессы взаимодействия человека и машины, а сложная, интегрированная и взаимосвязанная совокупность систем, информационных, технических, организационных, обеспечивающая решение большого круга задач, обусловленных общей средой проживания и функционирования общественных групп.

На настоящем этапе развития становятся критичными вопросы информационного обмена между техническими системами и человеком. Взаимодействие человека и машины вышло на новый уровень развития. Развитие информационных технологий наряду с инженерно-психологи-ческим подходом их применения оказывает значимое влияние на проектирование ИС.

Развитие вычислительной техники, систем передачи данных, интерфейсных систем оказало сильное влияние на увеличение производительности машин и управление ими. Повышение скоростей, уменьшение допусков, усложнение динамики, а также взаимосвязь и взаимодействие с группами людей и машин требуют от оператора умения предвидеть ситуации, устойчивых навыков управления, быстрой реакции. Разработка машин и систем, полностью использующих, а временами и превышающих возможности человека является технической задачей, решение которой требует понимания того, как ведут себя люди в определенных ситуациях, где применяются системы человек − машина. Важным становится максимально учитывать человеческие ограничения, связанные с его физическими возможностями по взаимодействию со средой, которая становится цифровой.

Раньше большая часть задач, связанных с наличием человека в технических системах, могла быть решена методом проб и ошибок либо на основе здравого смысла. Пользователю (оператору) приходилось приспосабливаться к неудобствам управления, но это происходило за счет усталости, плохой работы системы и ошибок управления. Работая иногда на пределе психофизиологических возможностей и в неблагоприятной производственной среде, человек допускает ошибки, «цена» которых в современном производстве резко возросла. В большинстве случаев действия операторов оказываются неправильными не из-за низкой их квалификации, а по причине несоответствия конструктивных (возможностей представления информации) особенностей техники возможностям человека, а это говорит о том, что

изменения условий трудовой деятельности, за которыми не поспевает биологическая перестройка организма человека, обусловливают возникновение целого ряда негативных явлений.

Таким образом, требование учитывать в процессе разработки системы влияние взаимодействия человека и машины становится критичным, и делать это следует таким образом, чтобы можно было предсказать результаты разработки в виде критериев производительности системы и ее влияния на смежные с ней системы. Прогнозирование поведения человека-оператора необходимо вести методами, совместимыми с описанием действия машины, т. е. моделировать и прогнозировать поведение оператора как компоненты системы человек-машина.

Согласно статистическим данным на долю человеческого фактора сейчас приходится от 40 до 70 % всех отказов технически сложных систем. Согласно мировой статистики 80 % катастроф в авиации и 64 % [1] на морском флоте происходят в результате ошибок, называемых логическими и моральными. О высоких нагрузках на психику и общее состояние операторов сложных систем свидетельствуют реальные данные из жизни. Так, например, при на предпосадочном снижении у командира авиалайнера частота переноса взгляда на приборы колеблется от 100 до 200 раз в мин. [1]. Длительность фиксации взгляда на каждом приборе составляет 0,66 с; приходится совершать руками около 30 движений в мин. В результате – пульс при посадке 150 ударов в минуту, кровяное давление 200 мм рт. ст. Также, например, при добыче угля средняя глубина шахт составляет 1000 м. горнорабочий всегда находится под высоким психологическим и эмоциональном напряжение. В результате – его пульс более 100 ударов в минуту, повышенное кровяное давление, порядка 180 мм рт. ст. Доктор при проведении операции должен в максимально короткий срок, порядка одной, двух секунд принять единственное правильное решение, которое может спасти пациенту жизнь. В результате – он испытывает высокое физическое и психологическое напряжение.

Аналогичным образом выглядит ситуация в других сферах человеческой деятельности, автоматизация которых позволяет повысить эффективность работы, сократить количество итераций при выполнении бизнес-процессов.

Данные примеры показывают, что как бы ни была совершена техника, ее эффективное и безопасное применение в конечном итоге зависит от того, насколько полно согласованы конструктивные параметры (важнейшей компонентой становится аудио-видео представление данных) с оптимальными условиями работы человека, с его психофизиологическими возможностями и особенностями [2]. Следовательно, возникает необходимость изучения (моделирования) работы машин (систем) и деятельности операторов в едином комплексе «человек-техника-среда».

Соответственно, чтобы использовать результат моделирования, не обязательно давать точные и подробные сведения. Модели могут быть результативны, даже если они только помогают инженеру осмыслить поведение людей и дают возможность выделить существенные факторы развития ситуации, или если они помогают разработать специальные эксперимент или модель для решения специфических вопросов.

В настоящий момент нашей жизни внешняя среда уже стала цифровой. Информационный обмен в виде спецификаций обмена становится ключевым фактором взаимодействия между информационными системами, средой и людьми. Информационный обмен является общенаучным понятием, включающим в себя обмен данными между людьми, обмен сигналами между живой неживой природой, людьми и устройствами. Информационные системы стали более сложными, состоящими из большого количества компонентов и выполняющими разноплановые задачи. Связующим фактором, гарантирующим целостное встраивание вновь разрабатываемых систем, становится требование подготовки разносторонних спецификаций информационного обмена между цифровой средой, компонентами системы и человеком с возможностями моделирования ситуаций.

Эргономика в совокупности с инженерной психологией позволяет решить целый спектр задач при создании информационных систем [2]. Одной из ключевых задач, является рационализация, оптимизация и сокращение итераций при проектировании ИС.

На современном этапе часто используют термин дизайн системы, где, по нашему мнению, следует выделять раздел по взаимодействию среды и проектируемой системы.

В заключении, проектирование информационных систем является основополагающей фазой при ее создании. Конечный результат всецело зависит от выбора правильного подхода при проектировании с тщательной проработкой функциональных требований, как самой системы, так и требований по взаимодействию с цифровой средой. В связи, с чем на первый план выходит необходимость использования всех эргономических возможностей новых информационных технологий совместно с инженерно-психологическими подходами их применения для взаимодействия среда – пользователь − машина.

Список используемых источников

1. Пономаренко В. А., Чунтула А. В. Человек и безопасность полетов: Научно-практические аспекты снижения авиационной аварийности по причине человеческого фактора. М. : Когито-Центр, 2013. 288 с. ISBN 978-5-89353-417-7.

2. Баканов А. С., Обознов А. А. Эргономика пользовательского интерфейса: от проектирования к моделированию человеко-компьютерного взаимодействия. М. : Изд-во «Институт психологии РАН», 2011. 176 с.

УДК 621.315

ЦИФРОВИЗАЦИЯ МАЛОКАНАЛЬНЫХ СИСТЕМ ПЕРЕДАЧИ ПО ВЫСОКОВОЛЬТНЫМ ЛИНИЯМ

К. И. Воронков, М. А. Мендельсон

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

Рассматривается задача цифровизации аналоговых систем передачи по высоковольтным линиям с помощью аппаратуры К-ЛЭП, представляющей три взаимосвязанных и в тоже время функционально взаимно независимых блока – мультиплексора, модема и высокочастотного блока. Показывается, что при таком подходе решается задача цифровизации систем ВЧ связи в короткие сроки и получается значительный эффект за счет минимального объема капитальных затрат и монтажных работ. При этом достигается большая пропускная способность и дополнительная гибкость использования различных вариантов загрузки взаимодействующих систем ВЧ связи.

ВЧ связь по ЛЭП, адаптивные высокоскоростные модемы, гибкий мультиплексор, высокочастотный блок.

Основная тенденция развития средств связи, в том числе в энергосетях, связана с широким использованием пакетной передачи на основе протокола IP [1]. Это позволяет объединить разнородные сети связи в единую IP-сеть, что, в свою очередь, повышает экономические показатели сети путем эффективного использования ее пропускной способности за счет учета особенностей передаваемой информации речь, данные и др. При этом в электроэнергетике широко начинают использоваться волоконно-оптические линии связи (ВОЛС). Однако, несмотря на применение ВОЛС, каналы ВЧ связи по-прежнему остаются и будут востребованными на тех направлениях, где требуется передавать ограниченный объем цифровой информации, и где применение ВОЛС не представляется целесообразным по технико-экономическим обстоятельствам [2]. Т. к. большинство существующих систем ВЧ связи по линиям электропередачи (ЛЭП) являются аналоговыми, необходимо осуществить их цифровизацию. Это позволяет повсеместно интегрировать ведомственную сеть связи электроэнергетики в общегосударственную цифровую сеть и даст возможность широко использовать резервирование каналов связи на различных направлениях. Таким образом, в сети связи предприятий электроэнергетики актуальна потребность в оборудовании для получения цифровых услуг (в первую очередь телемеханики, межмашинного обмена, Ethernet, и др.), а также сопряжение цифровых каналов, получаемых по системам ВЧ связи с магистральной цифровой сетью.

В данной работе рассматривается решение указанной задачи на основе аппаратуры К-ЛЭП [3].

При ее разработке изначально произведено разбиение аппаратуры ВЧ связи на три функциональных блока, допускающих как совместное, так и взаимно независимое их использование: гибкий субпервичный мультиплексор (ГМ-2-СП), высокоскоростной модем (М-АСП-ПГ-ЛЭП) и высокочастотный блок (ВЧБ). В ВЧБ осуществляется сопряжение аппаратуры с высокочастотным трактом линии электропередачи. Представленное разбиение на функциональные блоки позволяет в зависимости от потребностей пользователя выполнять цифровизацию системы связи с использованием минимально необходимого количества устройств, что заметно снижает текущие расходы предприятия.

Упрощенная структурная схема организации связи по ЛЭП приведена на рисунке.

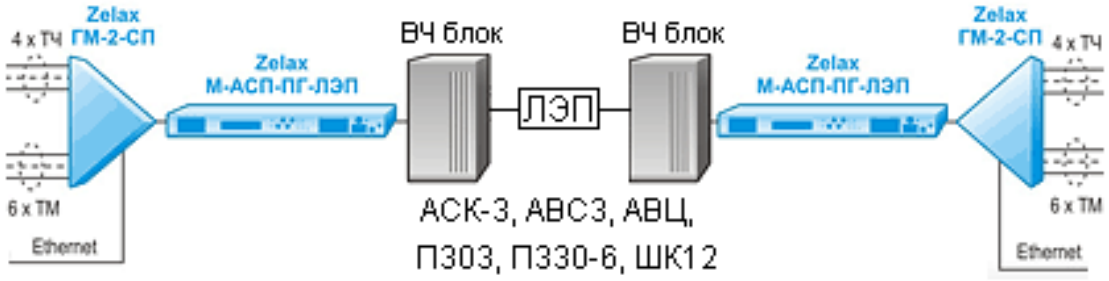


Рисунок. Упрощенная схема организации ВЧ связи по ЛЭП

Следует учитывать, что в составе аналоговых систем ВЧ связи имеются мощные ВЧ элементы, которые образуют интерфейс аппаратуры ВЧ связи с ЛЭП, содержащие мощный выходной усилитель, входные и выходные фильтры и т. д. Набор этих элементов функционально и конструктивно практически не зависит от того, является ли аппаратура цифровой или аналоговой. Поэтому с целью снижения затрат при цифровизации систем ВЧ связи указанный набор ВЧ элементов при его удовлетворительном состоянии может использоваться как составная часть новой цифровой системы, что также позволяет снизить затраты при цифровизации систем ВЧ связи.

Другим актуальным свойством аппаратуры является обеспечение возможности работы используемых блоков как в цифровом, так и в аналоговом режиме, что важно для современной аппаратуры, предназначенной для работы в тяжелых помеховых условиях ЛЭП.

Блок мультиплексора ГМ-2-СП содержит в своем составе многоканальное устройство сжатия речевых сигналов, и широкий набор интерфейсов передачи данных, позволяющих эффективно использовать доступную скорость передачи в канале связи. Мультиплексор дает возможность передать до 4-х телефонных сигналов со сжатием, 6 сигналов телемеханики (ТМ) или межмашинного обмена (ММО), 8 сигналов данных с ЧМн в тональной и надтональной области, потока данных Ethernet через синхронный канал или один (два) канальный интервал потока Е1, а также подключение к сети

Ethernet. Кроме того, мультиплексоры в соответствии с информацией, получаемой от модема М-АСП-ПГ-ЛЭП, обеспечивают адаптацию количества активных каналов пользователя в зависимости от скорости передачи суммарного потока, устанавливаемой в соответствии с помеховой обстановкой в линии связи. Изменение количества активных каналов осуществляется по значениям приоритетов, назначенных пользователем различным каналам (телефон, ТМ, ММО, Ethernet).

Телефонные порты мультиплексора могут работать в двухпроводных режимах FXS/FXO и в 4-проводном режиме с возможностью включения встроенных эхокомпенсаторов и эхозаградителей. В двухпроводных режимах поддерживается импульсный и частотный (тональный) набор номера, обеспечивается режим FXS-FXS с возможностью генерации сигналов «КПВ» и «Занято». В 4-проводном режиме обеспечивается поддержка двухчастотной сигнализации АДАСЭ 1200/1600 Гц, ТДН-1200 и передача сигналов модемов ТМ с ЧМн. При установке опционных модулей мультиплексор может иметь выход для подключения к каналу Е1.

Мультиплексор позволяет передавать речевой сигнал со скоростью 5,9 кбит/с или 7,0 кбит/с. Для реализации разнообразных цифровых транзитных соединений в состав мультиплексора может быть включен опционный модуль СП-IP**.** Этот модуль за счет наличия двух портов Ethernet дает возможность реализации цифровых соединений нескольких мультиплексоров между собой по сети IP без дополнительного внешнего оборудования в виде маршрутизаторов или коммутаторов. Это предоставляет возможность удобной интеграции цифровых каналов ВЧ связи в составе IP сети.

С помощью высокоскоростных модемов М-АСП-ПГ-ЛЭП осуществляется передача данных через системы ВЧ связи, а также по групповым и линейным трактам АСП, со скоростями до 80 кбит/с в полосе 12 кГц, до 25,6 кбит/с в полосе 4 кГц, и до 51,2 кбит/с в полосе 8 кГц. Высокая помехозащищенность сигналов модемов достигается за счет применения в них каскадного кодирования с внутренним решетчатым кодированием и внешним кодом Рида-Соломона. Модемы версии ЛЭП подключаются к аппаратуре ВЧ связи в тракт промежуточной частоты (ПЧ) в пределах полосы частот 4-112 кГц. Модемы могут использоваться для работы по трактам ПЧ систем АСК-3, АВС3-1, АВЦ, П-303 и П-330-6 и др. Имеется возможность использовать эти модемы для работы по широкополосному каналу ШК-12 или предгрупповому тракту в полосе 12...24 кГц. При использовании этих модемов в системах ВЧ связи, в которых ширина полосы тракта ПЧ превышает ширину спектра сигнала модема, в незанятой модемом части полосы частот аппаратуры ВЧ связи сохраняется возможность стандартной загрузки каналами ТЧ.

В модемах предусмотрен выбор 5–6 скоростей работы в ручном и автоматическом режимах. В автоматическом режиме обеспечивается динамическая адаптация скорости передачи к качеству линии связи, и помеховой обстановке в ней.

Модемы обеспечивают передачу данных от цифровых интерфейсов V.35, E1 и Ethernet.

Управление и контроль работы модемом/мультиплексором может осуществляться с передней панели модема/мультиплексора при помощи ЖКИ и клавиатуры; с ПК через порт RS-232/USB/Ethernet; с удалённого модема/мультиплексора. Имеется возможность обновления, встроенного ПО, включения шлейфов и индикации аварийных состояний.

Модемы и мультиплексоры также могут использоваться самостоятельно, решая функционально те задачи, которые ставятся в конкретном применении.

ВЧБ в направлении передачи предназначен для приема группового сигнала от модема М-АСП-ПГ-ЛЭП в полосе частот 16–32 кГц, переноса его в полосу частот линейного сигнала в диапазоне 24–1000 кГц и усиления до уровня, необходимого для передачи по ЛЭП. ВЧБ в направлении приема предназначен для приема сигнала, расположенного в заданном месте диапазона частот 24–1000 кГц, выполнения функций фильтрации принимаемого сигнала и переноса его в полосу частот 16–32 кГц для передачи его модему М-АСП-ПГ-ЛЭП. ВЧБ имеет варианты исполнения на 40 и 80 Вт с разнесенными/смежными частотами полос передачи и приема при ширине полосы 4, 8, 12 или 16 кГц.

Эффективность применения

Экономический эффект в рассматриваемом варианте осуществления цифровизации достигается за счет минимального объема капитальных затрат и монтажных работ, которые связаны с приобретением и установкой комплексов К-ЛЭП (отдельных блоков) на тракты ПЧ систем ВЧ связи, и при необходимости высокочастотного блока Зелакс. В условиях дефицита средств, а также с учетом специфических особенностей и значительной протяженности ЛЭП, при необходимости передачи ограниченного объема информации использование К-ЛЭП оказывается наиболее целесообразным, поскольку потребность в дополнительно устанавливаемой аппаратуре минимальна, цифровизация осуществляется в короткие сроки.

Получение значительно большей пропускной способности в цифровизированной системе ВЧ связи по сравнению с обычными аналоговыми системами достигается за счет применения высокоэффективных методов модуляции и кодирования цифровых сигналов, а также цифрового сжатия речи. Кроме того, улучшение качества функционирования цифровизированных систем ВЧ связи имеет место за счет перехода к новой элементной базе

и цифровым методам обработки сигналов. Использование пакетной передачи позволяет обеспечить дополнительную гибкость использования различных вариантов загрузки взаимодействующих систем ВЧ связи.

Таким образом, использование цифровизированной аппаратуры ВЧ связи предлагает экономичную альтернативу ВОЛС для передачи речи и данных. Несомненным достоинством системы ВЧ связи по ЛЭП состоит в том, что для передачи информационных сигналов используется собственная инфраструктура электросети. Это позволяет предприятиям связи энергоэнергетики быть независимыми от операторов других сетей связи, а отсутствие дополнительных текущих расходов на содержание каналов связи делает ВЧ связь экономически выгодной. Использование цифровых каналов ВЧ связи по ЛЭП дает возможность создания в выбранных направлениях также резервных каналов, что обеспечивает выполнение требований в части их организации по различным путям и через различные среды распространения сигналов.

С помощью комплексов К-ЛЭП решается задача интеграции сетей и систем ВЧ связи в современную цифровую сеть путем передачи по ним цифровых потоков. Эти комплексы имеют широкий набор интерфейсов, обладают возможностью адаптации скорости в зависимости от помеховой обстановки в каналах связи, что обеспечивает удобство их использования в различных применениях.

Выводы

Цифровизация аппаратуры ВЧ связи с использованием разбиения на функциональные блоки является экономичной альтернативой ВОЛС для передачи речи и данных в ведомственной сети электроэнергетики с возможностью интеграции в современную цифровую сеть.

Адаптация скорости и возможность назначения приоритетов каналам аппаратуры ВЧ связи в зависимости от имеющейся в наличии доступной скорости передачи в конкретной помеховой обстановке обеспечивают гибкое и максимальное использование имеющейся пропускной способности ВЧ тракта по ЛЭП.

Пользователю К-ЛЭП предоставляется возможность обновления программного обеспечения и гибкие возможности управления комплексом.

Список используемых источников

1. IEC 62488-1 Ed.1. Power line communication systems for power utility applications. Part 1 : Planning of analogue and digital power line carrier systems operating over EHV/HV/MV electricity grid. IEC, 2012.

2. Брауде Л. И., Скитальцев В. С., Шкарин Ю. П. Состояние и перспективы развития высокочастотной связи в электроэнергетике // Энергетик. 2013. № 6. С. 44–46.

3. К-ЛЭП Аппаратура ВЧ связи. URL: http://www.zelax.ru (дата обращения 17.04.2016).

УДК 621.395

МЕТОД ОЦЕНКИ ВЕРОЯТНОСТНО-ВРЕМЕННЫХ ХАРАКТЕРИСТИК СЕТИ НА БАЗЕ ПОДСИСТЕМЫ IMS С УЧЕТОМ ПОВТОРНЫХ ПЕРЕДАЧ СИГНАЛЬНЫХ СООБЩЕНИЙ

Гамиль Абдуллах

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

В докладе предложено модель процесса установления соединения через подсистемы IMS по протоколу SIP поверх транспортного протокола UDP (User Datagram Protocol). Предложены формулы для оценки времени задержки сигнальных сообщений, участвующих в процессе установления сессий, с учетом их повторных передач по IP-сети из-за различного рода сбоев и отказов.

IMS, SIP, повторная передача сообщений, качество обслуживания.

Постановка задачи

Развитие систем электросвязи последних десятилетий привело к появлению архитектуры IMS (*IP multimedia subsystem*). Появление концепции IMS как решения для построения мультисервисных сетей привело к эволюционному переходу сети связи общего пользования к сети нового поколения. Ядро подсистемы IMS является основой её архитектуры, составляющее из набора функции управления сеансами при обслуживании пользователей [1].

После регистрации абонентского оборудования (*User Equipment, UE*) IMS, находящимися в домашних сетях, пользователей могут инициировать сеансов связи с другими зарегистрированными пользователями IMS. На рисунке 1 приведен поток обмена сигнальными сообщениями по протоколу SIP поверх транспортного протокола UDP между основными элементами сети, принимающими участие в установлении соединения с помощью платформы IMS двух операторов.

Отметим, что при передаче сообщений возможно два случае:

1. Сообщение передается без ошибок, т. е. успешная передача SIP-сообщения.

2. Сообщение передается с ошибкой, т. е. сбой передачи SIP-сообщения. В этом случае происходить повторная передача сообщения.

Повторная передача увеличивает задержку передачи сигнальных SIP-сообщений и при повышении определённого времени (таймаута), эти сообщения сбрасываются. Штриховая линия на рисунке 1 отражает механизм

повторной передачи сообщения, состоящего из 7 фаз, представляющих возможные сообщения, для которых предложен этого механизма. Далее подробнее рассмотрим модель оценки времени задержки SIP-сообщений при установлении соединения и их механизм возможной повторной передачи по IP-сети.

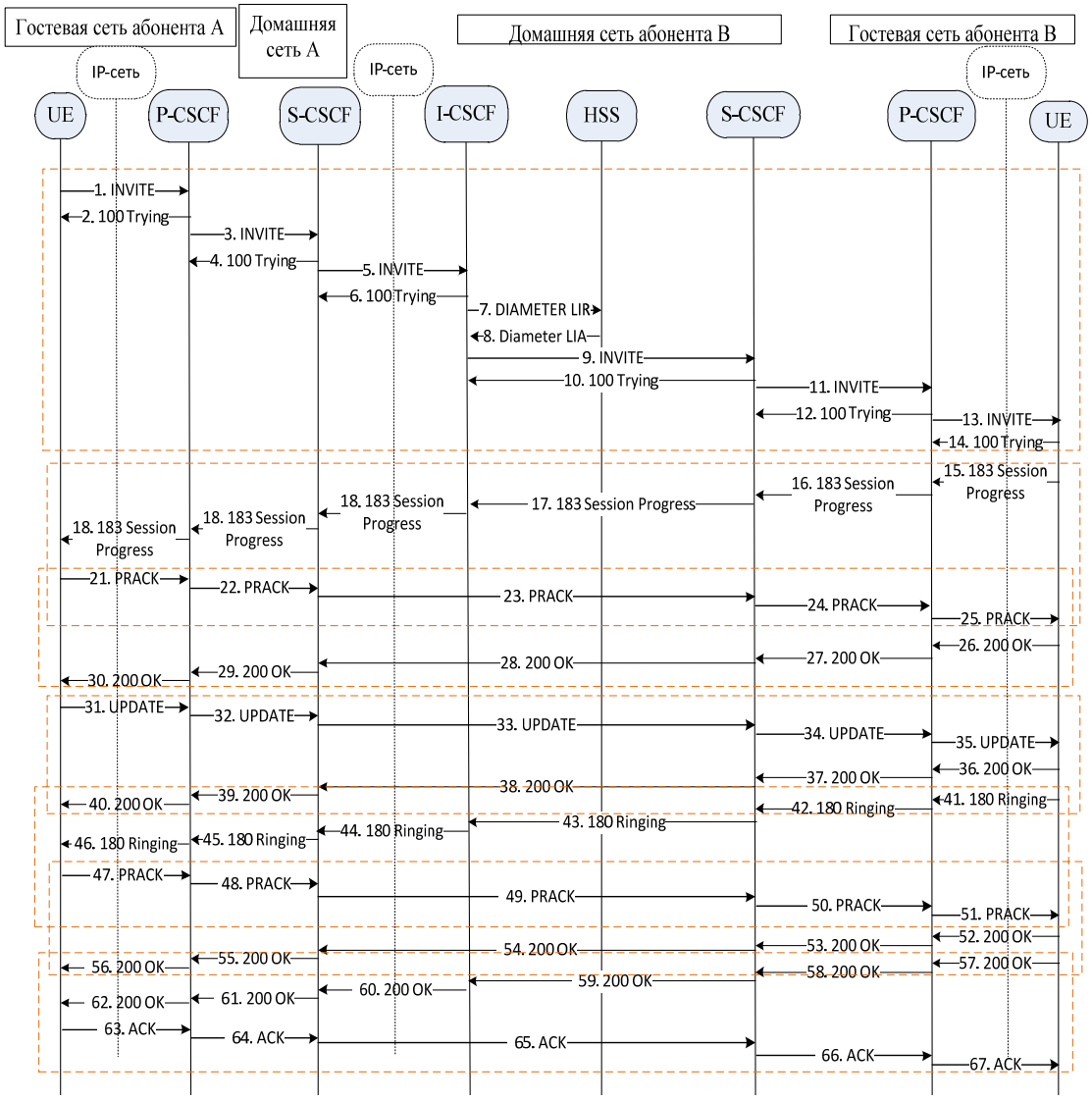


Рис. 1. Диаграмма установления соединения

Механизм повторной передачи SIP-сообщения

SIP использует экспоненциальное поведение повторной передачи, таким образом, если отправитель сообщения SIP не получает ответ через некоторое время, он повторно отправляет запрос через некоторое время ожидания. В случае возникновения различных сбоев запускается механизм повторной передачи сообщения. Контроль протокола SIP осуществляется двумя типами повторных передач:

– для сообщения INVITE;

– для «не-INVITE» транзакций. К этому типу относиться все SIP-сообщений, присущие в процессе установления сессии кроме INVITE.

Механизм передачи сообщений 100-TRYING, 183 SESSION PROGRESS и 180-RINGING является надежным [2], поэтому будем предполагать, что эти сообщения передаются без ошибок.

Повторная передача сообщений на уровне протокола SIP происходит с использованием таймеров, контролирующих процесс ретрансляции. Так, в момент передачи сообщения INVITE запускаются таймер *T1* и таймер T_{INVITE}, ограничивающий время ожидания ответа (сообщения типа 100 Trying или 180 Ringing). При срабатывании таймера *T1* происходит повторная передача запроса INVITE, и таймер запускается заново, но уже с удвоенным значением. Этот процесс продолжается после каждой повторной передачи до истечения таймера T_{INVITE}. Аналогично процесс повторной передачи организован и для не-INVITE сообщений за исключением того, что перед повторной передачей время удваивается, пока не достигнет таймера *T2*, а затем устанавливается равным *T2* для всех последующих повторных передач сообщений до таймера $T_{не-INVITE}$ со значением 64.*T1*. Эти передачи могут понижать производительность сигнализации в SIP-сети.

Вероятностью повторной передачи (q) является вероятность потери транзакции сообщений (l). Например, вероятность повторной передачи сообщения INVITE означает, что пакет (запрос INVITE, содержащий *K1* фреймов) передан с ошибкой или этот пакет был получен, но предварительный ответ (183 SESSION PROGRESS, содержащий *K2* фреймов) передан с ошибкой. Следовательно, вероятность повторной передачи сообщения INVITE можно найти по формуле:

$$q_{inv} = 1 - ((1-l)^{k_1+k_2}).$$

Предположим, что задержка передачи INVITE и не-INVITE сообщений по IP-сети равна, т. е. время, затраченное на n последовательных ретрансляций INVITE и не-INVITE сообщений до момента начала его успешной передачи, одинаковое. Из [2], нетрудно убедится, что это время задаётся формулой:

$$(2^1-1)T1,(2^2-1)T1,\ldots,(2^N-1)T1=(2^n-1)T1.$$

Тогда, среднее значение задержки передачи i-сообщения при установлении сессий поверх протокола UDP с учетом его возможных передач можно найти следующим образом:

$$D_{\text{повтор}} = \sum_{i=1}^{R} D^i = \sum_{i=1}^{R} \frac{1}{1-q^N} \cdot [(1-q) + (1-q)q \cdot T_1 + (1-q)q^2 \cdot 3T_1 + (1-q)q^3 \cdot 7T_1 + \cdots$$
$$+(1-q)q^{N-1} \cdot (2^{N-1}-1)T_1] = \sum_{i=1}^{R} T_1 \cdot \left[\frac{(1-q)(1-(2q)^N)}{(1-q^N)(1-2q)} - 1 \right] \quad (1)$$

где N – Максимальное число повторных передач SIP-сообщений; R – количество SIP-сообщений, необходимые для успешного установления соединений, и $R=9$.

Вероятность $P(q)$ успешного установления сессии по протоколу SIP с учётом повторных передач, может быть вычислена по формуле:

$$P(q)=(1-q^N)^R.$$

Численный анализ

Для численного анализа было сделано предположение, что моделью множества узлов, участвующих в процессе установления сессий, служит СМО с неоднородным потоком заявок, в которой входящий поток сообщений является пуассоновским, длительность обслуживания *i*-сообщений распределена по экспоненциальному закону с интенсивностью μ_i, средним значением задержки на обслуживание b_i, и коэффициентом вариации V_{b_i}. С использованием метода средних значений можно показать, что среднее время ожидания заявок определяется по формуле Поллачека-Хинчина [3]:

$$w_i=\frac{\sum_{i=1}^{R}\lambda_i b_i^2(1+V_{b_i}^2)}{2(1-\alpha)} \qquad (i=1,\cdots,R). \qquad (2)$$

И так, среднее время установления соединения складывается из средних задержек передачи сообщений по сети и средних задержек обработки сообщений на узлах, а также из средних значений задержек с учетом возможных повторных передач сообщений – $D_{\text{повтор}}$. Следовательно, среднее значение времени установлений соединений в подсистемы IMS D_{ims} определяется в соответствии с формулами (1) и (2) следующим образом [4]:

$$D_{ims}=7D_{UE1}+10D_{ip-\text{сеть}}+\frac{8}{\mu_i-12\lambda_i}+\frac{8}{\mu_i-12\lambda_i}+10D_{ip-\text{сеть}}$$
$$+\frac{4}{\mu_i-5\lambda_i}+\frac{8}{\mu_i-12\lambda_i}+\frac{8}{\mu_i-12\lambda_i}+10D_{ip-\text{сеть}}+6D_{UE2}+D_{\text{повтор}}$$

Будем считать, что максимальное число повторных передач N = 7, вероятность повторной передачи сообщений $q\le 10^{-1}$ и T1=0,5*c*. Время обработки в узлах сети не зависит от типа сообщений. Среднее время обслуживания в узлах IMS (P-CSCF, S-CSCF, I-CSCF) равно $b_{P,I,S-CSCF}=0,4\,мс$, а среднее время обслуживания в пользовательском оборудовании $b_{UE}=0,1\ мс$. Примем величину задержки сообщений SIP по IP-сети $b_{ip-\text{сеть}}=\frac{1}{3}RTT=33,3\,мс.$

На рисунке 2 изображён график зависимости вероятности $\overline{P}(q)$ потери вызова от вероятности (q) повторной передачи сигнального сообщения. Из графика видно что, даже при ненадёжной работе IP-сети, когда из десяти пакетов теряется один, вероятность потери вызова не превышает 10^{-6}, что удовлетворяет требование международных стандартов – вероятность потери IP-пакетов в сетях нового поколения не должна превышать 10^{-3} [5].

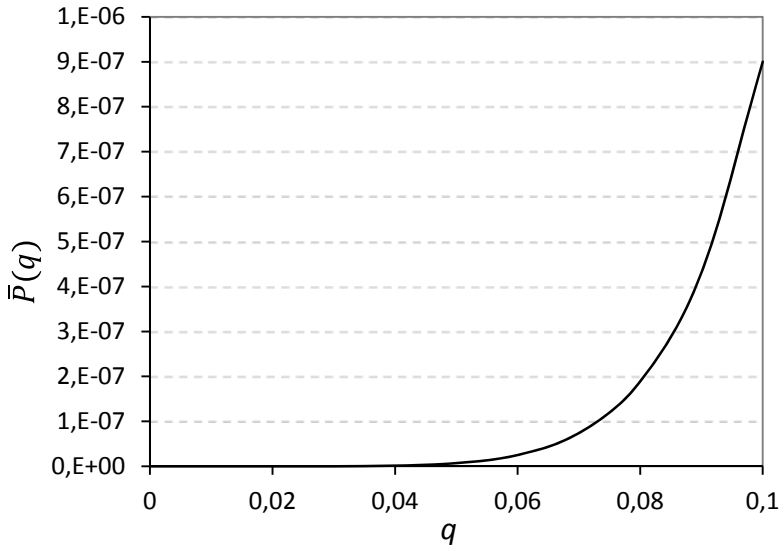


Рис. 2. Вероятность потеря вызова

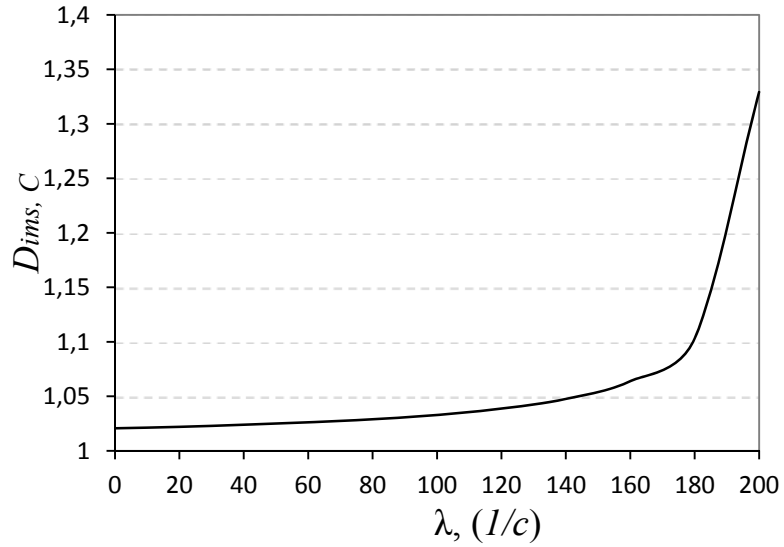


Рис. 3. Зависимость среднего времени установления соединения D_{ims} от интенсивности поступления вызовов (сообщений потока SIP)

На рисунке 3 представлена зависимость среднего времени установления соединения от интенсивности поступления вызовов. Анализ результатов вычислений показывает, что при допустимых значениях вероятности

$q \le 10^{-3}$, среднее время установления соединения не превосходить 1,4 *с*, это удовлетворяет нормам МСЭ, устанавливающего ограничение 3 *с* на время установления соединения для местных соединений.

Результаты численного анализа не противоречат требованиям международных стандартов к нормативным значениям задержек установления сессии по протоколу SIP, что подтверждает адекватность использования предложенных формул в статьи.

Список используемых источников

1. Гольдштейн Б. С., Соколов Н. А., Яновский Г. Г. Сети связи: учебник для ВУЗов. СПб. : БХВ-Петербург, 2010. – 400 с.

2. Rosenberg J., Schulzrinne H., Camarillo G. et al. SIP: Session Initiation Protocol. IETF RFC 3261. – 2002.

3. Алиев Т. И. Основы моделирования дискретных систем. СПб. : СПбГУ ИТМО, 2009. – 363 с.

4. Гамиль А. А., Куликов Н. А. Построение модели задержки сигнального трафика в сети связи на базе подсистемы IMS // Электросвязь. 2014. № 9. С. 8–13.

5. ITU-T Recommendation Y.1541, Network Performance Objectives for IP-Based Services. 2002.

Статья представлена научным руководителем, доктором технических наук, профессором Б. С. Гольдштейном.

УДК 621.391

АНАЛИЗ ТРАФИКА И КАЧЕСТВА ОБСЛУЖИВАНИЯ В БЕСПРОВОДНЫХ САМООРГАНИЗУЮЩИХСЯ СЕТЯХ

И. А. Герасимова, А. И. Парамонов

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

Статья посвящена анализу развития технологий беспроводных самоорганизующихся сетей связи, а также особенностей трафика и требований к качеству обслуживания в таких сетях. Приведенные в статье материалы являются результатами исследований в области развития Интернета Вещей (IoT) и характеристик, производимого IoT трафика.

самоорганизующиеся сети, трафик Machine-to-Machine, M2M, качество обслуживания QoS, системы диспетчерского управления и сбора данных SCADA.

Самоорганизующиеся беспроводные сети представляют собой децентрализованные беспроводные сети, не имеющие постоянной структуры. Подобные сети требуют минимального конфигурирования и имеют возмож-

ность быстрого развертывания, что позволяет применять их при чрезвычайных ситуациях, в военных целях, а также и для множества иных приложений при допустимой стоимости реализации [1]. Наряду с отмеченными тенденциями, в настоящее время происходит интенсивное развитие технологий Machine-to-Machine (M2M) в самоорганизующихся сетях. Сети M2M представляют собой реализацию концепции IoT для физических или виртуальных вещей. Они развиваются благодаря снижению стоимости, и развитию технологий радиосвязи, а также росту объема успешного применения устройств M2M.

С развитием вычислительной техники и проникновения IT в области деятельности, которые не были вовлечены в инфокоммуникационную систему, растет доля трафика M2M, что увеличивает влияние такого трафика на качество предоставления услуг связи. Например, на сегодняшний день в сетях подвижной связи большую часть трафика составляет трафик, который производится различными приложениями, работающих на мобильных устройствах абонентов. Кроме этого, значительную долю трафика составляет трафик модемов, выполняющих различные функции, например, контроль доставки грузов, различного рода сигнализации, сбор показаний измерительных приборов и т.п. Можно предполагать, что в скором будущем количество устройств в сети может превысить численность населения (т. е. количество абонентов), что подтверждает концепцию IoT. При этом M2M трафик оказывает значительное влияние на процессы эксплуатации сетей и на качество обслуживания.

На сегодняшний день существует множество прогнозов роста трафика M2M в мире. По результатам анализа различных прогнозов [2] построен обобщенный прогноз изменения доли M2M устройств подключенных к сетям подвижной связи (рис. 1). Количество устройств M2M к 2022 г. составит 30 млрд, из которых 2,6 млрд будут мобильные устройства. Также предполагается, что к 2022 г. количество устройств, генерирующих трафик M2M, составит больше 60 % от общего количества устройств [2].

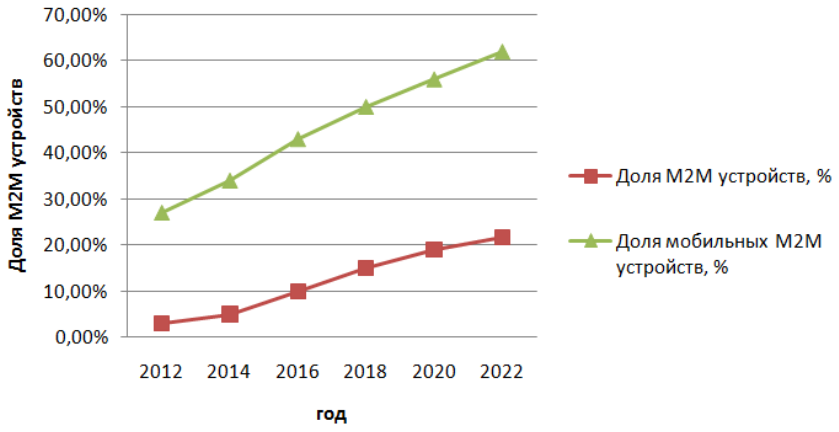


Рис. 1. Доля M2M-устройств, подключенных к сетям подвижной связи

Трафик M2M представляет собой поток данных, при этом его отличие от трафика Human-to-Human (H2H) является то, что инициаторами передачи данных являются автоматические устройства.

В зависимости от протокола взаимодействия передача трафика M2M может наступить при: воздействии внешних факторов, которые приводят к передаче данных (например, изменение физических параметров, которые контролируются датчиком), истечении определенного интервала времени, по различным техническим причинам (например: передача служебных данных) [3, 4].

В зависимости от условий, приводящих к передаче данных, можно выделить следующие основные три типа M2M трафика:

Опосредованный трафик – генерируется автоматическими системами с использованием активных устройств, т. е. устройство может быть инициатором передачи данных. Данный трафик является реакцией на различные случайные события. Свойства такого трафика зависят от свойств контролируемых процессов.

Псевдодетерминированный трафик – генерируется автоматическими системами с использованием пассивных датчиков. На сегодняшний день получили распространение системы диспетчерского управления и сбора данных SCADA, строящиеся по принципу главный-подчиненный. В таких системах датчики выступают в качестве пассивных устройств (подчиненных) и осуществляют передачу данных по запросу от главного устройства. В данном случае свойства трафика определяются алгоритмом выбора интервала времени между моментами передачи запросов данных.

Служебный трафик – характерен для систем с активными датчиками. Генерируется при наступлении некоторых внешних (обычно, случайных) событий, приводящих к необходимости выполнения служебных операций по поддержанию работоспособности системы и диагностики состояния датчиков [5].

В целях исследования свойств трафика M2M была разработана имитационная модель и проведен анализ трафика опроса датчиков. Имитационная модель (SCADA) построена в системе моделирования AnyLogic (рис. 2).

Результаты моделирования в виде реализаций трафика представлены на рисунках 3, 4, 5.

На рисунке 3 представлена реализация трафика опроса датчиков SCADA при выборе кратных периодов опроса.

Рисунок 4 иллюстрирует трафик опроса датчиков SCADA при выборе случайных периодов опроса датчиков.

На рисунке 5 приведена реализация трафика трафик опроса датчиков при выборе некратных периодовопроса.

По результатам моделирования можно сделать о том, что некратные периоды сканирования датчиков позволяют снизить пиковые значения трафика.

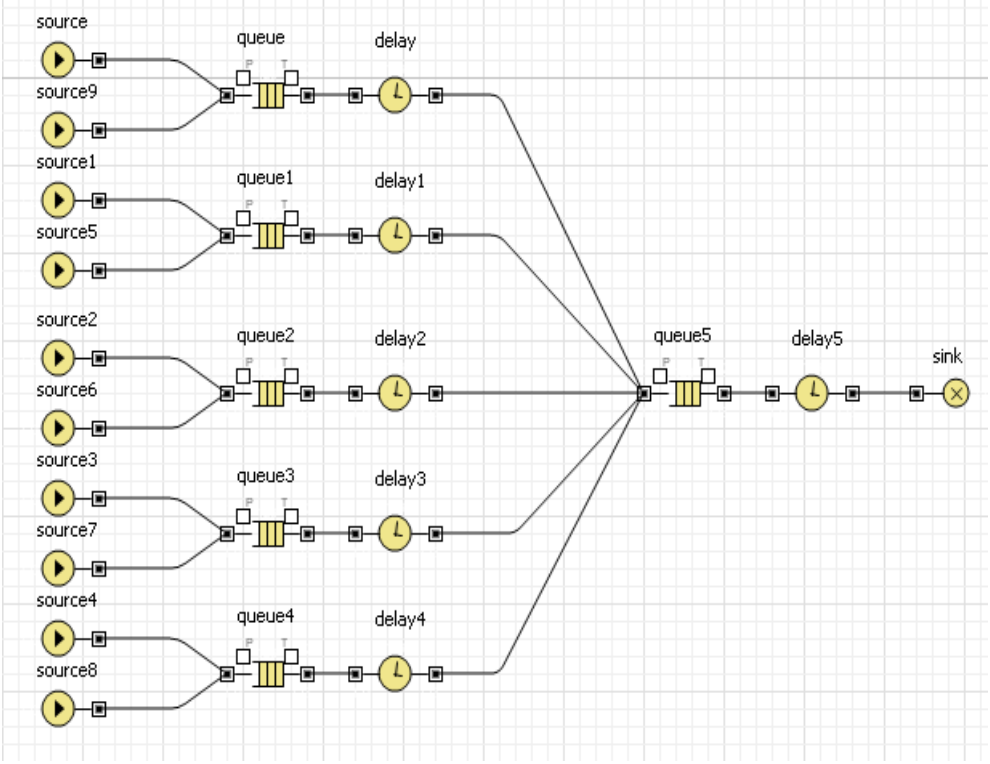


Рис. 2. Модель сети в AnyLogic

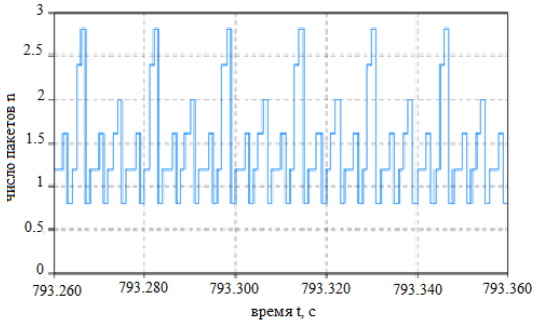


Рис. 3. Реализация трафика опроса датчиков при выборе кратных периодовопроса

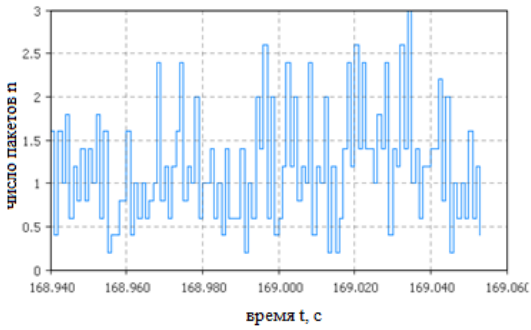


Рис. 4. Реализация трафика опроса датчиков при выборе случайных периодов опроса

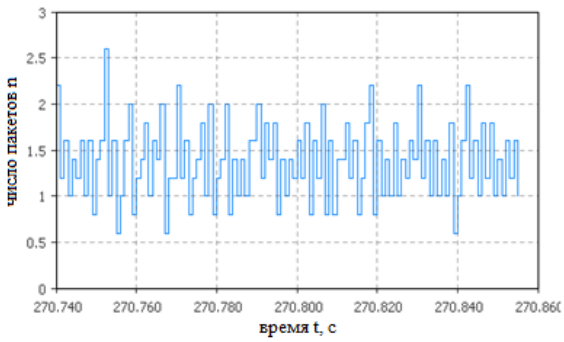


Рис. 5. Реализация трафика опроса датчиков при выборе некратных периодов опроса

Из вышесказанного можно сделать следующие выводы, что:

1) Свойства трафика M2M различны из-за различных типов самоорганизующихся сетей.

2) Свойства трафика зависят от целевого назначения самооранизующихся сетей.

3) Необходимы дальнейшие исследования по управлению трафиком и влиянию трафика M2M на QoS в сетях связи за счет динамичного роста числа устройств, генерирующих трафик M2M.

Список используемых источников

1. Голдсмит А., Медар М., Эффрос М. Самоорганизующиеся беспроводные сети: пер. с англ. И. Е. Сацевич [Электронный ресурс] // Наука – это жизнь. URL: http://nauka.relis.ru/26/0110/26110002.htm (дата обращения 26.02.2016).

2. Matt Hatton. Measuring M2M // 11th World Telecommunication / ICT Indicators Symposium (WTI S-13) Mexico City, México, 4–6 December, 2013. P. 10.

3. Кучерявый А. Е., Прокопьев А. В., Кучерявый Е. А. Самоорганизующиеся сети. СПб. : Любавич, 2011. 312 с.

4. Беспроводные самоорганизующиеся сети [Электронный ресурс] // Сайт компании ООО «Кросс-Автоматика». URL: http://crossgroup.su/solutions/adhoc.html (дата обращения 26.02.2016).

5. Парамонов А. И. Модели потоков трафика для сетей M2M // Электросвязь. 2014. № 4. С. 9–14.

УДК 004.031.43

КОМПЛЕКС МЕР БЕЗОПАСНОСТИ ОБЪЕКТОВ СВЯЗИ

Е. Ю. Герлинг, Е. И. Кулишкина

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

В данном докладе рассматривается комплекс мер объектовой безопасности объекта связи. Проанализированы уязвимые места объекта и предложены универсальные методы информационной и объектовой безопасности. Для обеспечения безопасности объекта предлагается использовать системы контроля и управления доступом, охранной сигнализации, видеонаблюдения, сбора и обработки информации, организация каналов внешней связи, организовать режим доступа, инструктаж персонала.

режим доступа на объект, объектовая безопасность.

В современном мире для успешного функционирования предприятия и достижение им заданных результатов необходимо придерживаться строгого и чёткого выполнения правил, предусматривающих защиту объекта

от внешних и внутренних угроз, а также обеспечивающих конфиденциальность данных, хищение или вскрытие которых однозначно приведёт к разрушительному ущербу системе безопасности в целом.

Объекты связи – особо важные объекты. Стоит внимательно подходить к обеспечению всесторонней безопасности данных объектов. Для предотвращения террористических актов, случайной или сознательной порчи дорогостоящего оборудования, как посторонними лицами, так и сотрудниками объекта и других действий вредоносного характера необходимо применять целый ряд мероприятий, контролирующих перемещение и действие персонала объекта связи. Внешние угрозы, направленные на пассивные носители информации (например, хищение информации в процессе её передачи по сети), также должны быть приняты во внимание, при формировании системы безопасности на объекте. На объектах связи постоянная передача информации по сети является обязательной функцией, следовательно, необходимо сделать упор на должную защиту каналов и всей коммутационной сети в целом.

Согласно Постановлению Правительства Российской Федерации от 30 октября 2014 г. N 1130 [1], объекты связи подразделяются на 3 категории в зависимости от степени угрозы совершения на объектах (территориях) террористических актов и возможных последствий их совершения и с учетом оценки состояния защищенности объектов. Объекты 1-ой категории – объекты (территории) федерального и межрегионального значения, противоправные действия на которых могут нанести ущерб государственной безопасности страны, привести к особо крупному экономическому ущербу. Объекты (территории) категории 2 – объекты (территории) регионального значения, противоправные действия на которых могут привести к экономическому ущербу в отношении промышленных предприятий, организаций социальной сферы и других организаций. Объекты (территории) категории 3 – локальные объекты (территории), противоправные действия, на которых могут привести к выводу из строя или ограничению деятельности объектов категории 1 и 2.

Объект связи является режимным предприятием, поэтому доступ в различные помещения объекта, а также доступ к функциональным системам строго разграничен [2]. Для всех сотрудников объекта создаются инструкции, в которых описаны не только служебные обязанности, но и действия в чрезвычайных ситуациях (например, пожар). Также сотрудники подписывают договор о неразглашении коммерческой и служебной тайны. Существует типовой договор, применяемый в организациях. В таком договоре прописаны обязанности, которые безоговорочно должен выполнять сотрудник на объекте связи. К таким обязанностям можно отнести:

– использование полученной информации исключительно для целей организации и в порядке, предусмотренном в Договоре;

– незамедлительно сообщать о факте раскрытия коммерческой или служебной тайны, а также принять все необходимые меры к недопущению разглашения информации;

– не копировать и не разглашать информацию, составляющую коммерческую тайну.

Согласно последнему пункту, на многих объектах связи вводятся такие ограничения для сотрудников, как запрет на использование собственных электронных носителей (USB-флешки, дискеты, CD-диски), а в некоторых случаях сотрудникам необходимо сдавать свои телефоны. Все эти действия направлены исключительно на сохранение информации в пределах объекта и недопущение её разглашения.

В Договоре прописываются не только обязанности, но также и сфера действия, что обеспечивает сохранение информации в пределах допустимого круга лиц, между которыми заключен договор.

Несомненно, за нарушение любых пунктов Договора сотрудники должны нести ответственность. Данный пункт также отражен в Договоре. В нём описывается, какое наказание понесёт сотрудник за нарушение своих обязанностей относительно сохранения коммерческой и служебной информации. Обычно, наказанием является штраф, увольнение, но если разглашённая информация является государственной тайной, т. е. при разглашении такой информации наносится вред государству, то наказание определяется согласно ст. 26 Федерального Закона РФ от 21.07.1993 N 5485-1 (ред. от 08.03.2015) «О государственной тайне» [3].

Антитеррористическая защищенность объектов (территорий) независимо от их категории обеспечивается путем осуществления ряда мероприятий в целях [1]:

– воспрепятствования неправомерному проникновению на объекты;

– выявления потенциальных нарушителей режимов, установленных на объектах и (или) признаков подготовки или совершения террористического акта;

– пресечения попыток совершения террористических актов на объектах и минимизации возможных последствий и ликвидации угроз террористических актов.

Помимо защиты непосредственно самой информации необходимо организовать защиту объекта в целом. Создание и применение комплекса физической защиты значительно повышает эффективность функционирования объекта связи. К задачам физической защиты можно отнести:

– предотвращение фактов несанкционированного доступа на объект;

– задержка злоумышленника, т. е. создание условий для препятствия его действиям;

– пресечение несанкционированных действий на территории объекта.

К основным системам обеспечения безопасности на объекте относятся:

– система контроля и управления доступом [4];
– система охранной сигнализации;
– система видеонаблюдения.

Система контроля и управления доступом может решать такие задачи, как оперативный контроль местонахождения персонала и время его нахождения на объекте [4]. Система контроля и управления доступом состоит из следующих технических средств:

– преграждающие управляемые устройства в составе преграждающих конструкций и исполнительных устройств (турникеты, управляемые калитки, двери с электромагнитными замками или электромеханическими защелками и т. д.);

– устройства для ввода идентификационных признаков в составе считывателей, кода наборных панелей, различных идентификаторов и т. д.;

– устройства управления в составе аппаратных и программных средств.

При помощи программных средств реализуется функция расчёта отработанного сотрудниками времени, что необходимо для соблюдения дисциплины на объекте. Чёткая дисциплина сотрудников необходима для более полной защищённости данных и бесперебойного функционирования предприятия. Контроль также подразумевает под собой, что ни один сотрудник не может передать свою карту, для прохода другого. Поэтому при утере или иных случаях отсутствия карты у сотрудника дальнейшие действия определяются службой безопасности объекта в соответствии с заранее разработанным регламентом. Служба безопасности должна вести каждодневный учёт сотрудников. Объекты связи необходимо оборудовать специальными техническими средствами пропускного режима. Для входной двери на считывателе необходимо установить правило «antipassback», которое подразумевает запрет на повторный проход. Использует три режима: строгий (запрет прохода вплоть до выхода), временной (в течение указанного времени система запрещает повторный проход вплоть до выхода), мягкий (система не запретит доступ, но в журнале будет отмечен факт нарушения правила «antipassback»). Для наиболее важных помещений объекта предлагается использовать режим двойной идентификации. Данный режим требует наличие двух идентификаторов (например, *Proxy*-карта и отпечаток пальца).

Для контроля перемещения и действий сотрудников объекта предусмотрена система видеонаблюдения. Под контроль системы видеонаблюдения попадают все важные помещения объекта, включая коридоры. Система видеонаблюдения позволяет четко идентифицировать любого сотрудника,

находящегося на объекте, и проследить его путь следования и действия в рабочее время. Данная система позволяет предотвратить умышленные незаконные действия сотрудников.

Все данные, передаваемые с сетевых камер и IP-видеосерверов, отображаются на рабочем места дежурного сотрудника службы безопасности. В системе должны быть предусмотрены такие функции камер, как детектирование движения с помощью встроенного датчика движения с использованием зон детекции, управление видеосистемой по событиям в СКУД через механизм сценариев управления, управление камерами с интерактивных планов помещений, возможность организации взаимодействия между несколькими рабочими местами видеомониторинга при помощи механизма удалённого вызова сценариев управления.

Система видеонаблюдения используется для наблюдения за всеми точками прохода на объекте. Камеры должны быть расположены на всех точках, где присутствует система контроля и управления доступом. Также должен быть контроль над главным входом на объект и его периметром, непосредственно в проходной, где может быть размещён такой сервис, как распознавание лиц. Это обеспечит предотвращение несанкционированного доступа со стороны не только сотрудников, но и лиц, не причастных к объекту связи. Камера также должны транслировать обстановку в коридорах объекта, в местах постоянного пребывания сотрудников. Необходим контроль действий службы охраны на их рабочем месте.

В обеспечении безопасности охраняемых объектов связи значение имеет надёжное и качественное освещение. Поэтому объекты связи должны быть оборудованы техническими средствами охранного освещения. В их состав входят: осветительные приборы, кабельные и проводные сети, аппаратура управления.

Система охранной сигнализации подразумевает под собой совокупность технических средств для обнаружения нарушителя на охраняемом объекте и подачи извещения о тревоге для принятия мер по задержанию злоумышленника. Основными задачами охранной системы является обнаружение, формирование и передача извещения о факте нарушения, обеспечение постановки объекта на охрану и снятия с охраны. Извещателями системы охранной сигнализации оборудуются все двери объекта (контроль открывания двери), как уличные, так и внутренние, а также окна (контроль открывания окна и разбития стекла). В особо важных помещениях устанавливаются извещатели объемные, контролирующие объем помещения и обеспечивающие второй рубеж охраны.

От эффективности функционирования охранной системы в целом зависит возможность и уровень решения пропускного и внутриобъектового режимов. Создание надежной системы охраны предприятия определяется принятием правильного решения на основе анализа потенциальных угроз

безопасности охраняемого объекта и реальной оценки возможностей для создания эффективной системы охраны с учетом имеющегося выбора сил и средств.

Все рассмотренные выше системы должны быть автоматизированы. Это позволит добиться эффективной безопасности на предприятии. Немаловажен и выбор необходимого оборудования. На российском рынке широко представлен ассортимент необходимого для данных систем оборудования отечественных производителей.

Список используемых источников

1. Требования к антитеррористической защищенности объектов (территорий), находящихся в ведении Министерства связи и массовых коммуникаций Российской Федерации, Федеральной службы по надзору в сфере связи, информационных технологий и массовых коммуникаций, Федерального агентства связи, Федерального агентства по печати и массовым коммуникациям, а также подведомственных им организаций : утв. постановлением Правительства РФ от 30 октября 2014 г. № 1130. URL: http://base.consultant.ru/cons/cgi/online.cgi?req=doc;base=LAW;n=170622;fld=134;dst=100001,0;rnd=0.8603240501536981 (дата обращение 26.03.2016).

2. Андрианов В. И., Красов А. В., Липатников В.А. Инновационное управление рисками информационной безопасности : учеб. пособие. СПб. : СПбГУТ, 2012. 396 с. ISBN 978-5-91891-0 92-4.

3. О государственной тайне, статья 26 : закон РФ от 21 июля 1993 №5485-1 (ред. от 8 марта 2015 г.). URL: http://base.consultant.ru/cons/cgi/online.cgi?req=doc;base=LAW;n=176315;fld=134;from=2481-9;rnd=189271.05013113336921238;;ts=01892711609260604 8119906 (дата обращение 26.03.2016).

4. Прудников С. В., Баскаков С. А. Системы контроля доступа : учеб. пособие. СПб. : СПбГУТ, 2013. 75 с.

УДК 621.39

РЕФЛЕКТОМЕТРИЯ АБОНЕТСКОГО УЧАСТКА PON

С. Ф. Глаголев, А. С. Дюбов, В. Б. Рудницкий
В. Р. Сумкин, В. А. Хричков

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

Особенность абонентского участка PON – это наличие большого числа соединений при малой длине волокна. Промышленные рефлектометры при тестировании такого тракта работают на пределе своих возможностей, кроме этого, их стоимость и время измерения неприемлемо большие. Использование полупроводниковых лазеров красного света для генерации зондирующих сигналов позволяет улучшить основные па-

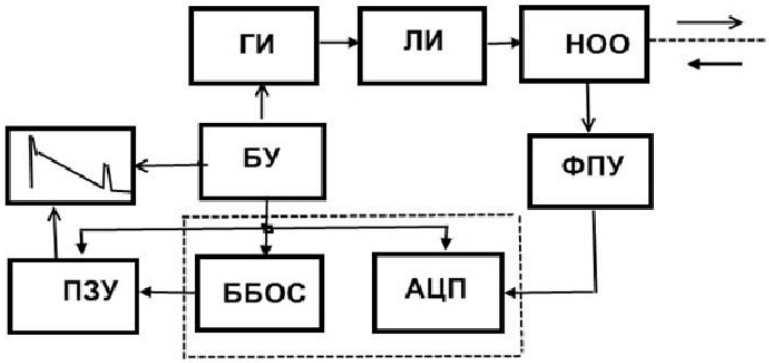
раметры рефлектометра при существенном снижении его стоимости. Дополнительные преимущества можно получить при использовании метода интегральной рефлектометрии.

PON, абонентский участок, оптический рефлектометр, лавинные фотодиоды, полупроводниковые лазеры красного света, интегральная рефлектометрия.

В настоящее время широкополосный абонентский доступ (ШПАД) основан на технологии пассивных оптических сетей (PON). Наибольшее внедрение эта технология получила в многоквартирных домах, где она экономически целесообразна [1].

При строительстве и эксплуатации PON возникают проблемы тестирования абонентского (АУ), обусловленные большим количеством разъемных и неразъемных соединений, а также небольшой длиной АУ (десятки метров). В [2] показано, что от качества монтажа АУ зависит надежность работы сети в целом. Большинство специалистов считает, что для выявления некачественных соединений и дефектов необходимо применять оптические рефлектометры (ОР). Однако эффективность использования ОР крайне низкая [3] вследствие того, что при тестировании АУ используется зондирующие импульсы (ЗИ) только с минимальной длительностью $t_{зи} = 5$ нс. Кроме этого, стоимость ОР с необходимыми для тестирования АУ характеристиками достаточно большая. В связи с этим возникает задача поиска технических решений для упрощения и удешевления конструкции ОР, предназначенного для просмотра коротких неоднородных волоконно-оптических трактов.

Упрощенная структурная схема ОР приведена на рисунке 1. Самым сложным и дорогостоящим узлом является ББОС (совместно с АЦП). Информационная производительность ББОС современных ОР составляет около 5 Гбит/с (тактовая частота выборок не менее 400 МГц, число разрядов АЦП около 12).



ГИ - генератор импульсов, ЛИ - лазерный излучатель, НОО - направленный ответвитель, БУ - блок управления, ФПУ - фотоприемное устройство, ПЗУ - постоянное запоминающее устройство, ББОС - блок быстрой обработки сигнала

Рис. 1. Упрощенная структурная схема ОР

Частота повторения ЗИ определяется максимальной дальностью просмотра. Максимальная дальность просмотра современных ОР около 300…400 км, а частота повторения ЗИ – примерно 200Гц. Это соответствует числу накоплений кривой сигнала обратного рассеяния (СОР) примерно $3{,}6 \times 10^4$ (при регламентированном времени накопления [4], равному 180 с).

Если сузить область применения ОР только просмотром коротких АУ, то частоту ЗИ можно значительно повысить. При максимальной длине просмотра 200 м можно выбрать частоту повторения ЗИ примерно 400 кГц. Это позволяет перейти к более простому принципу последовательного накопления, когда за один период зондирования берется только один отсчет кривой СОР. Соответственно, более чем на три порядка сокращается информационная производительность ББОС. При сохранении прежних значений характеристик ОР ($t_{зи} = 5$ нс и число накоплений $3{,}6 \times 10^4$) в данном случае число точек кривой СОР, накопленных за одну секунду, равно 10. При максимальной длине шкалы ОР 100 м и шаге дискретизации 0,25 м необходимо накапливать 400 точек кривой СОР, что обеспечивается за общее время измерения, равное 40 с. Таким образом, если пожертвовать многофункциональностью и универсальностью, то можно создать более простой и дешевый ОР, специализированный на тестировании коротких трактов.

Еще большего эффекта можно достичь, если перейти на более короткую длину волну излучения ЗИ. Это обусловлено следующим:

– с уменьшением длины волны света возрастает СОР по закону λ^{-4}. Так, уровень СОР на длине волны 650 нм на 15 дБ больше уровня СОР на длине волны 1550 нм;

– при $\lambda \leq 1000$ нм в ФПУ применяются кремниевые лавинные фотодиоды (Si ЛФД), к преимуществам которых относятся меньшая стоимость и, самое главное, меньшая пороговая мощность (примерно на 10 дБ) в сравнении с InAsGa ЛФД, применяемыми в промышленных ОР [5];

– с уменьшением λ сильнее проявляются дефекты волоконно-оптических соединителей, в частности, шероховатости и загрязнения торцов волокон, неплотный контакт соединяемых торцов и др.;

– так как с уменьшением λ возрастает СОР, то ширина «мертвой зоны» уменьшается, что очень важно при тестировании коротких трактов;

– для рефлектометрии АУ наиболее привлекательной является длина волны излучения 650 нм (красный свет). Полупроводниковые лазеры на этой длине волны давно используются для визуальной дефектоскопии волоконно-оптических трактов. Недостатком рефлектометрии «красным светом» является искажение результата измерения суммарного затухания АУ, так как коэффициент затухания волокна на этой длине волны равен примерно 5 дБ/км, что намного больше коэффициента затухания на рабочих

длина волн (0,2…0,4 дБ/км). Однако при малой длине волокна это не так важно, а при необходимости это приращение затухания можно учесть. Гораздо важнее, что увеличение уровня СОР и снижение пороговой мощности ФПУ приводит к повышению отношения сигнала к шуму (ОСШ) на 25 дБ. Это увеличение ОСШ можно использовать для удешевления ОР и улучшения пользовательских показателей ОР, как это показано в следующем примере.

В таблице показано сравнение характеристик лучшего современного ОР ($\lambda = 1310/1550$ нм, $t_{зи} = 5$ нс) и предлагаемого ОР ($\lambda = 650$ нм, $t_{зи} = 2$ нс).

ТАБЛИЦА. Параметры рефлектометров

Длина волны, нм	1550/1310	650
Максимальное расстояние, м	20000	200
Длительность ЗИ, нс	5	2
Разрешение шкалы «X», см	25	10
Лавинный фотодиод	InAsGa	Si
Мощность ЗИ, мВт	100	20
Мертвая зона, м	5	1
Время измерения, с	10	2
Шумовая дорожка, дБ	0,1	0,05
Производительность процессора, Мбит/с	5000	5

При реализации ОР с разрешением горизонтальной шкалы 10…20 см, возникают технические трудности генерации мощного короткого импульса накачки ЛИ длительностью 1…2 нс. Задача существенно облегчается при использовании метода интегральной рефлектометрии [6], в котором в качестве зондирующего сигнала используется импульс, длительность которого выбирается из выражения $t_{зи} \geq 2L_{макс}/v$, где $L_{макс}$ – максимальная длина тестируемого участка, v – скорость распространения света в световоде. В методе интегральной рефлектометрии (МИР) фронт ЗИ мало на что влияет, а срез ЗИ (по сути, выключение ЛИ), определяет разрешение горизонтальной шкалы ОР и должен иметь длительность около 1 нс, что несложно обеспечить. Еще одним преимуществом МИР является увеличение отношения сигнала к шуму и, как следствие, повышение быстродействия обработки СОР.

Вывод. Применение в ОР метода интегральной рефлектометрии, а также полупроводниковых лазеров красного света и позволяет упростить алгоритм обработки СОР и создать более дешевый ОР, оптимизированный на тестирование АУ небольшой длины в PON.

Список используемых источников

1. Никульский И. Е. Технологии PON: вчера, сегодня, завтра // Вестник связи. 2009. № 3. С. 23–27.
2. Рудницкий В. Б., Сумкин В. Р., Салтыков А. Р. Тестирование абонентского участка PON // Фотон-Экспресс. 2013. № 5. С. 26–27.
3. Глаголев С. Ф., Рудницкий В. Б., Салтыков А. Р. Проблемы рефлектометрии PON // Фотон-Экспресс. 2014. № 8. С. 20–21.
4. Листвин А. В., Листвин В. Н. Рефлектометрия оптических волокон. М. : ЛЕСА-Парт, 2005. 208 с. ISBN 5-902367-03-4.
5. http://www.azimp.ru/catalogue/avalanche_photodiodes/
6. Архангельский В. Б., Глаголев С. Ф., Марченко К. В., Былина М. С. Интегральный оптический рефлектометр // Фотон-Экспресс. 2008. № 5–6. С. 38–43.

УДК 621.315.2

ПОКАЗАТЕЛИ НАДЕЖНОСТИ ВОЛОКОННО-ОПТИЧЕСКИХ ЛИНИЙ СВЯЗИ И МЕТОДЫ ИХ ОЦЕНКИ

С. Ф. Глаголев, Г. В. Колотовкина, Е. А. Храпова

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

Волоконно-оптические линии широко применяются в телекоммуникационных сетях самых разных уровней – от межконтинентальных магистралей до корпоративных и домашних компьютерных сетей. Одна из основных тем, которую нужно рассматривать при проектировании любой волоконно-оптической трассы связи – показатели надежности ВОЛС и методы их оценки в зависимости от технологии строительства оптических линий связи (подземные, воздушные, подводные).

оптическое волокно, показатели надежности, оценка надежности, технологии строительства, технологии спектрального уплотнения.

Для того, чтобы рассмотреть параметры надежности ВОЛС, нужно вспомнить различные современные методы строительства ВОЛС. На данный момент существуют три основных варианта прокладки ВОК: подземный, воздушный, подводный. Каждый из этих методов имеет свои преимущества и недостатки и подразделяется на различные варианты, в зависимости от условий и местности. Так подземный способ подразделяется на основные три группы: прокладка непосредственно в грунт, в защитной трубе и прокладка ВОК в кабельную канализацию. Воздушный метод строительства также подразделяется на несколько вариантов: подвес, прокладка в грозозащитном тросе, навивная технология прокладки и на основе самонесущего ВОК. Подводный метод прокладки зависит от метода укладки кабеля на дно морей и океанов и таким образом может быть проложен либо

в траншею с помощью плуга, либо с помощью подводного кабелеукладчика, в результате чего на дне кабель засыпается песком.

В настоящее время при передачи любой информации по линиям связи любому оператору нужно выполнить основную задачу по транспортировке сигнала с заданной достоверностью и с заданным временем доставки, чтобы пользователь мог воспользоваться услугами в любое удобное для него время. В этом случаи вопросы надежности играют основную роль при проектировании волоконно-оптических линий связи для более эффективного предоставления услуг.

В первую очередь при рассмотрении технологий строительства оптических линий связи с точки зрения параметров надежности, нужно вспомнить об основных критериях:

– отказы, которые приводят к нарушению функционирования ВОЛС и соответственно к потере трафика;

– интенсивность отказов, которая показывает среднее число отказов в единицу времени (час) на 1 км трассы;

– среднее время восстановления связи;

– среднее время между отказами (наработка на отказ);

– вероятность безотказной работы, которая показывает, что в заданные интервалы времени на линии не возникает отказа;

– коэффициент готовности – вероятность того, что линия в исправном состоянии в любой выбранный момент времени;

– коэффициент простоя – вероятность того, что в любой выбранный момент времени линия находится в состоянии отказа.

Основными критериями при расчете ВОЛС являются: отказы, вероятность безотказной работы и коэффициент готовности [1].

Отказы характеризуются плотностью повреждений, приходящихся на 100 км трассы в год, которые определяются по формуле (1):

$$n = \frac{100\ N}{KL}, \tag{1}$$

где N – число отказов на магистрали связи длиной L за K лет.

Отказы бывают двух основных видов: внезапные (ведут к обрыву ВОК) и постепенные (развивающиеся во времени). К постепенным отказам, например, относится трекинг-процесс, который вызывает разрушение (сгорание) кабеля. К постепенным – резкие перепады температуры окружающей среды, ураганные нагрузки на опоры и подвесные кабели.

С отказами на прямую связан такой критерий, как интенсивность отказов, определяющийся по формуле (2). Значение этой характеристики зависит от условий эксплуатации на отдельных участках магистрали и в общем случаи расчет ведется по формуле:

$$\lambda = \sum_{i=1}^{n} \Lambda_{CPi} * L_i , \quad (2)$$

где Λ_{CPi} – средняя плотность отказов на 1 км трассы в час.

Для линейного тракта интенсивность отказов может определяться по формуле (3), как сумма интенсивностей отказов НРП, ОРП и кабеля:

$$\Lambda_{сист} = \lambda_{нрп} \times N_{нрп} + \lambda_{орп} \times N_{орп} + \lambda_{каб} \times L , \quad (3)$$

где $\lambda_{нрп}$, $\lambda_{орп}$ – интенсивности отказов НРП и ОРП; $N_{нрп}$, $N_{орп}$ – количество НРП и ОРП; $\lambda_{каб}$ – интенсивность отказов одного километра кабеля; L – протяженность магистрали.

На основании формулы (3) получены некоторые значения интенсивности отказов на 1 км ОВ в зависимости от методов строительства ВОЛС:

$\lambda_К = 4{,}08 \times 10^{-7}$ час$^{-1}$ – для кабелей, прокладываемых непосредственно в грунт;

$\lambda_К = 4{,}92 \times 10^{-7}$ час$^{-1}$ – для кабелей типа 8-ки, подвешиваемых на опорах распределительных ЛЭП или воздушных линиях связи;

$\lambda_К = 4{,}32 \times 10^{-7}$ час$^{-1}$ – для ВОЛС выполненных по навивной технологии;

$\lambda_К = 2{,}78 \times 10^{-7}$ час$^{-1}$ – для ВОЛС проложенного в кабельную канализацию.

Вероятность безотказной работы за время t определяется показательной функцией (4):

$$P = e^{-\lambda t} . \quad (4)$$

Еще один из основных параметров надежности – коэффициент готовности, который должен оцениваться на стадии проектирования ВОЛС. Этот параметр учитывает все составляющие системы эксплуатации и может быть рассчитан для каждой подсистемы отдельно по формуле (5):

$$K_г = \frac{T_о}{(T_о + t_{в.п.})} = \frac{(T - t_{в.п.})}{T} , \quad (5)$$

где $T_о$ – время безотказной работы, T – время наблюдения, $t_{в.п.}$ – время повреждения.

На надежность ВОЛС оказывают воздействия многие факторы, основными из которых: эксплуатационные и конструктивно-производственные, то есть внутренние и внешние факторы. Наиболее частыми повреждениями ВОЛС являются механические повреждения в результате сотрясений, вибраций, растяжений под воздействием температуры, сдвиги почвы, работы, проводимые сторонними организациями и т. д. Таким образом, если рассматривать оптические кабели без металлических элементов и не учитывать повреждения из-за старения оптических волокон, для магистральных ВОЛС

63 % всех аварий, будут вызваны земляными работами сторонних организаций, для городских ВОЛС – 50 % всех аварий происходит из-за нарушения герметичности муфт и оболочек около муфт, для сельских ВОЛС – 55 % повреждений из-за земляных работ, производимых сторонними организациями.

В ВОЛС имеется особый внутренний источник отказов, который отличает эти линии от традиционных кабельных систем – обрывы ОВ, вызванные старением кварцевого стекла, т.е. необратимое изменение передаточных и механических характеристик оптического кабеля. Основной причиной старения является коррозия оптического волокна под воздействием влаги и механического напряжения. Важным параметром, при рассмотрении вопроса старения, является прочность материала оптического волокна. На этот параметр большое влияние оказывает наличие микротрещин или дефектов на поверхности ОВ. Получается, что любой обрыв при старении ОВ является результатом увеличения микротрещины.

Для повышения надежности работы системы одним из часто применяемых методов является – резервирование. При аварии происходит автоматическое переключение на резервный канал [2]. Однако резервирование имеет свои недостатки. Основной недостаток – значительные дополнительные расходы, поэтому его используют, если стоимость восстановления системы с резервным элементом меньше, чем для системы без резерва. Также ведут постоянный мониторинг линии на предмет неисправностей, а при проектировании ВОЛС проводят оценку надежности ВОЛС по критериям наработки на отказ.

Список используемых источников

1. Гроднев И. И., Мурадян А. Г., Шарафутдинов Р. М. Волоконно-оптические системы передачи и кабели. М. : Радио и связь, 1993. 264 с.

2. Пирмагомедов Р. Я. Исследование отказов физического канала пассивных оптических сетей и разработка методики их прогнозирования : дис. … канд. техн. наук : 05.12.13 / Пирмагомедов Рустам Ярахмедович. СПб., 2014. 193 с.

УДК 621.391

ОПТИЧЕСКИЕ МУЛЬТИПЛЕКСОРЫ ДЛЯ ТЕХНОЛОГИИ WDM

С. Ф. Глаголев, Г. В. Колотовкина, Е. А. Храпова

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

В настоящее время активно развивается технология спектрального мультиплексирования WDM, позволяющая эффективно и быстро наращивать пропускную способ-

ность сети. Основным устройством системы WDM, которое объединяет несколько оптических несущих в единый агрегатный поток на передающей стороне, является мультиплексор. На приемном конце обратную операцию выполняет демультиплексор. Это устройство обладает свойством обратимости, что позволяет рассматривать только технологии демультиплексирования.

технология спектрального уплотнения, демультиплексоры, технология AWG.

В общем виде все демультиплексоры можно разделить на два класса: построенные на микрооптических устройствах и на основе планарных интегральных устройств [1]. С помощью первой категории демультиплексоров реализуются две технологии, которые для разделения несущих используют интерференционные фильтры или угловую дисперсию.

Существует несколько видов интерференционных фильтров, например, на основе резонатора Фабри-Перо. Такое устройство состоит из двух плоскопараллельных зеркал с высокой отражающей способностью внутренних поверхностей и прозрачной непоглощающей диэлектрической среды между ними, как это показано на рисунке 1 [2]. Входной луч падает на плоскость левого зеркала, попадает внутрь полости резонатора, частично проходит через правое зеркало, а частично отражается от него. Отраженный луч затем отражается от левого зеркала, и процесс многократно повторяется. Если расстояние между зеркалами кратно λ/2, то все лучи, прошедшие через правое зеркало, оказываются в фазе и интерферируют между собой.

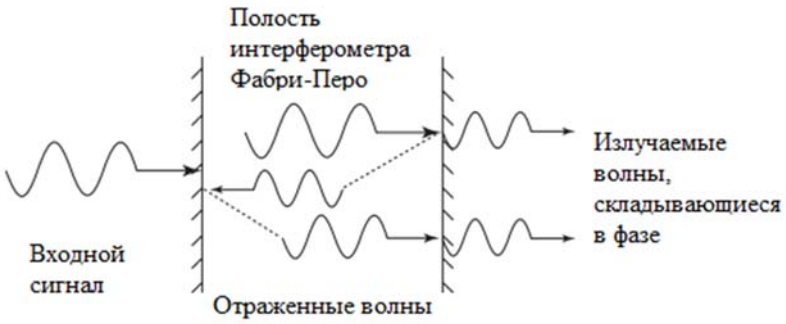


Рис. 1. Фильтрация света резонатором Фабри-Перо

Резонатор настраивается на выделение одной длины волны и для демультиплексирования *n* несущих необходимо поставить каскадно *n* фильтров. Достоинством таких фильтров является возможность их перестройки за счет изменения коэффициента преломления среды между зеркалами и расстояния между ними, однако, практически это достаточно сложно реализуется. Характеристика фильтра Фабри-Перо имеет вид гребенки, что накладывает определенные условия для его применения в системах WDM (*Wavelength Division Multiplexing*). Интерференционные фильтры

на основе резонатора Фабри-Перо редко используются в современных системах WDM, уступив место фильтрам на многослойных тонких пленках.

Тонкопленочный интерференционный оптический фильтр представляет собой оптическую подложку, на которую нанесли множество слоев диэлектрического материала с разными показателями преломления [3]. На каждом слое, в зависимости от его показателя преломления и толщины, происходит отражение определенной части падающего света. Таким образом, можно создать фильтр, пропускающий только определенный диапазон длин волн. Демультиплексор содержит набор фильтров, каждый из которых может выделить один канал. При этом формируется многоступенчатая система фильтров, изображенная на рисунке 2, в которой для демультиплексирования *n* несущих ставятся каскадно *n* фильтров.

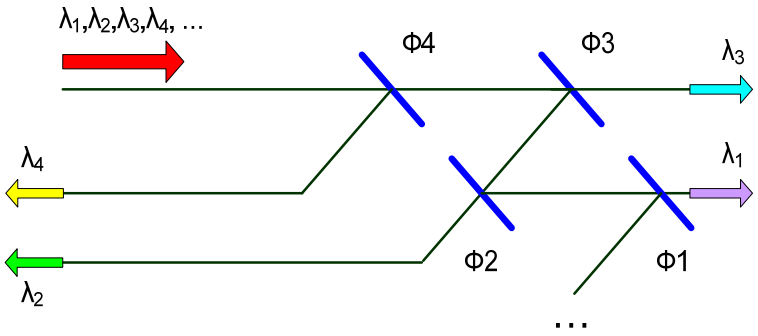


Рис. 2. Многоступенчатая система тонкопленочных фильтров

Фильтры расположены под наклоном, чтобы избежать попадания отраженного света обратно в систему. Однако такое положение влияет на эффективную толщину слоев, а, следовательно, и полосу пропускания, что необходимо заранее учитывать. Сами фильтры являются не перестраиваемыми. Достаточно сложным является подбор материала слоев с нужными оптическими и физическими свойствами. Число наносимых слоев зависит от предъявляемых к фильтру требований. С увеличением числа фильтров растут вносимые потери, поэтому мультиплексоры на тонкопленочных фильтрах используются только для систем CWDM с небольшим числом каналов. Данная технология является достаточно популярной, потому что позволяет создавать недорогие фильтры с различными спектральными свойствами.

Другой вид фильтров, которые так же часто применяются во всех современных системах WDM – это фильтры на решетке Брэгга. Для их получения сначала волокно легируется (например, германием), а затем для варьирования показателя преломления облучается ультрафиолетовым излучением с определенной пространственной периодической структурой [2]. Таким образом, в волокне создается дифракционная решетка, которая будет

отражать заданный интервал длин волн, как это показано на рисунке 3. Брэгговская длина волны фильтра и коэффициент отражения решётки могут быть заданы с большой точностью при производстве решётки. Эти параметры не должны изменяться на протяжении всего срока эксплуатации решётки. Необходимо отметить, что брегговская длина волны зависит от температуры и натяжения волокна. Для компенсации нестабильности фильтры располагают в приборах, контролирующих температуру. Возможно создание мультиплексоров на их основе с очень маленькими потерями. Решетка Брэгга рассчитана на фиксированную длину волны и для демультиплексирования *n* несущих формируют каскад из *n* решеток. При совместном использовании с двумя циркуляторами волоконная брэгговская решетка находит широкое применение в мультиплексорах ввода/вывода.

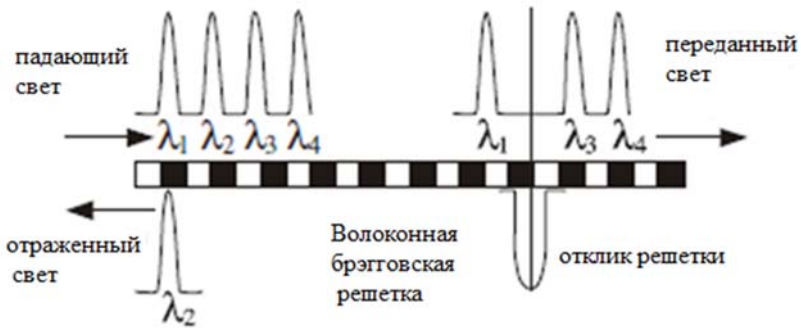


Рис. 3. Демультиплексор на основе волоконной брэгговской решетки

Следующий вид демультиплексирования использует явление угловой дисперсии. Данный метод основан на пространственном разложении оптического сигнала на несколько длин волн с помощью диспергирующего элемента [1]. Таким элементом может выступать призма или объемная дифракционная решетка. Потери, которые вносят такие устройства, практически не зависят от числа каналов, что является преимуществом системы. Демультиплексор, использующий отражательную призму по схеме Литтроу, имеет небольшие габариты и применяет всего одну систему фокусирующих элементов.

Широкое распространение получили объемные дифракционные решетки. Они могут в зависимости от угла падения отражать световой поток таким образом, что разность набега фаз, отраженных от соседних элементов решетки волн определенной длины будет равна 2π. При этом отраженные волны будут усиливать друг друга. Угол отражения зависит от длины волны. При работе необходимо контролировать поляризацию падающего оптического излучения. Демультиплексоры, основанные на дифракционной решетке, являются достаточно дорогими и сложными в изготовлении. Однако вносимые ими потери практически не зависят от числа каналов, за счет чего данная технология с успехом применяется для систем WDM с большим

числом каналов. На рисунке 5 представлен демультиплексор на дифракционной решетке, реализованный по схеме трехмерного оптического мультиплексирования 3DO (3-D Optics WDM). В его состав входят дифракционная решетка, вогнутое сферическое или параболическое зеркало и массив волокон, которые размещаются в пазах решетки с фиксированным шагом. После прохождения системы выделенная несущая фокусируется в точке B, где располагается выходное волокно.

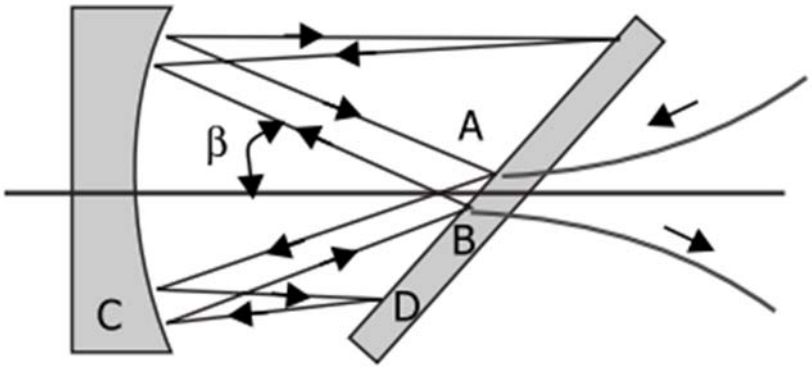


Рис. 5. Демультиплексор на основе трехмерного оптического мультиплексирования

Конструкция позволяет организовать до 131 канала с шагом 1 нм или до 262 каналов с шагом 0,5 нм.

В настоящее время особенное значение придается развитию технологий интегральной оптики, которые позволяют на маленькой подложке размещать большое количество оптических компонентов, взаимосвязанных друг с другом, тем самым создавая миниатюрные устройства.

Большое распространение получили интегрально-оптические мультиплексоры на основе фазосогласованных волноводных решеток AWG (*Arrayed Wave-guide Grating*). Они состоят из двух планарных оптических многопортовых разветвителей: входного $n \times m$ и выходного $m \times n$. Они соединяются между собой массивом из m волноводов, длины которых отличаются на фиксированную величину ΔL, то есть длина i-го волновода:

$$L_{i+1} = L_i + \Delta L. \quad (1)$$

Как следует из формулы (1), это вносит фазовый сдвиг между сигналами разных каналов, и в результате каждая длина волны света попадает в свой волновод. Демультиплексор AWG представлен на рисунке 6.

Для сравнения двух современных технологий в таблице указаны некоторые параметры мультиплексоров WDM. С учетом возможности использования современных планарных технологий и создания систем с большим числом каналов, мультиплексоры AWG являются наиболее перспективными.

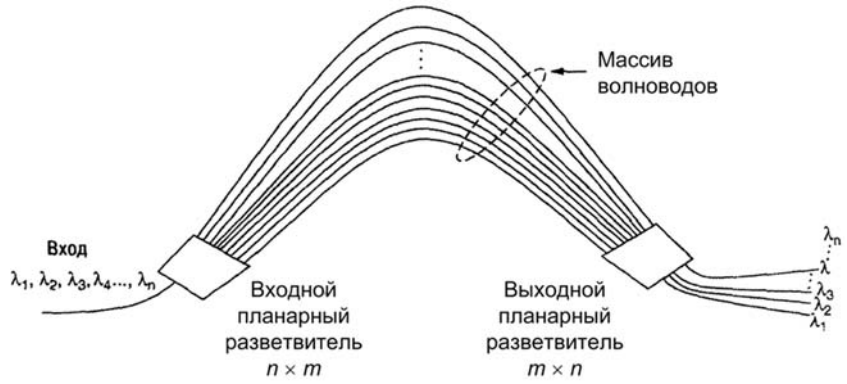


Рис. 6. Демультиплексор AWG

ТАБЛИЦА. Сравнение технологий оптического мультиплексирования AWG и 3DO

Технология	Максимальное число несущих	Шаг, нм	Вносимые потери, дБ	Переходное затухание, дБ	Чувствительность к поляризации, %
AWG	102–400	0,2–0,8	2,2–6,4	(–20)–33	0,3
3DO	262	0,4–250	2–6	(–30)–(–55)	0

Список используемых источников

1. Слепов Н. Н. Оптические мультиплексоры и демультиплексоры систем WDM [Электронный ресурс] // Электроника: НТБ. 2004. N 8. С. 42–47. URL: http://www.electronics.ru/files/article_pdf/1/article_1151_485.pdf (дата обращения 27.03.2016).

2. Слепов Н. Н. Оптические мультиплексоры ввода-вывода [Электронный ресурс] // Электроника: НТБ. 2001. N 1. С. 40–43. URL: http://www.electronics.ru/ files/article_pdf/1/article_1401_986.pdf (дата обращения 27.03.2016).

3. Слепов Н. Н. Современные технологии цифровых оптоволоконных сетей связи. 2-е изд., испр. М. : Радио и связь, 2003. 468 с.

УДК 004.056.55

СТЕГОСИСТЕМЫ ПОВЫШЕННОЙ СЕКРЕТНОСТИ ДЛЯ ВЛОЖЕНИЯ ИНФОРМАЦИИ В НЕПОДВИЖНЫЕ ИЗОБРАЖЕНИЯ

А. К. Годлевский, В. И. Коржик

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

В статье рассмотрена стегосистема с возможностью минимизации количества изменений яркости пикселей. Для решения этой проблемы были применены коды Хэмминга с изменяемыми параметрами. Представлена компьютерная программа с дружественным (удобным) интерфейсом.

стеганография, коды Хэмминга, матричное погружениеэ.

Стеганография – семейство методов, при помощи которых некоторое дополнительные сведения погружаются в основное покрывающее сообщение при сохранении хорошего качества покрывающего сообщения. Наиболее распространенный и, в то же время, простой в реализации метод вложения – вложение в наименее значащие биты (НЗБ) [1].

Для того чтобы минимизировать обнаруживаемость секретной информации, необходимо уменьшить количество изменений в покрывающем сообщении. Одним из методов, который позволяет добиться такого результата, является матричный метод погружения с использованием кодов Хэмминга. Основное преимущество этого подхода – при вложении требуется совершить меньше изменений, чем объем вкладываемой информации [2].

При использовании данного метода, p бит сообщения могут быть погружены в $2^p - 1$ пикселей.

Пусть x – вектор наименее значащих бит $2^p - 1$ пикселей исходного сообщения.

$$H = \begin{pmatrix} 00 & \dots & 1 \\ \dots & \dots & \dots \\ 10 & \dots & 1 \end{pmatrix}$$ – проверочная матрица кода Хэмминга.

Если $Hx \neq m$, отправитель вычитает $Hx - m$, находит результат в качестве столбца матрицы H и изменяет НЗБ соответствующего пикселя.

На рисунке 1 изображен график оценки эффективности матричных вложений с использованием кодов Хэмминга для неподвижных изображений размером 256 × 256 пикселей [3].

Рис. 1. Зависимость количества изменений НЗБ от количества вкладываемых бит для неподвижного изображения размером 256 × 256

В настоящей работе решалась задача по разработке программы с дружественным интерфейсом, которая позволяет вкладывать и извлекать секретные сообщения для неподвижных изображений, используя матричный

метод вложения с кодами Хэмминга, для минимизации количества изменений яркости пикселей.

При разработке программы применялись технологии в области Web-приложений. Для придания интерактивности интерфейсу, использовалась технология JavaScript. Поскольку программа подразумевает собой работу с неподвижным изображением, потребовалось использование специальной графической библиотеки ImageMagick.

При запуске программы, пользователь может выбрать функции вложения или извлечения секретного сообщения, как показано на рисунке 2. Кроме того, ниже представлена краткая информация о программе.

Программа поддерживает работу со всеми актуальными форматами изображения – bmp, png, jpeg, gif. При вложении информации, программа использует синий канал пикселя, т. к. этот цвет наименее восприимчив для человеческого глаза. Для изображений с режимом grayscale (градации серого) предусмотрено конвертирование в RGB-режим.

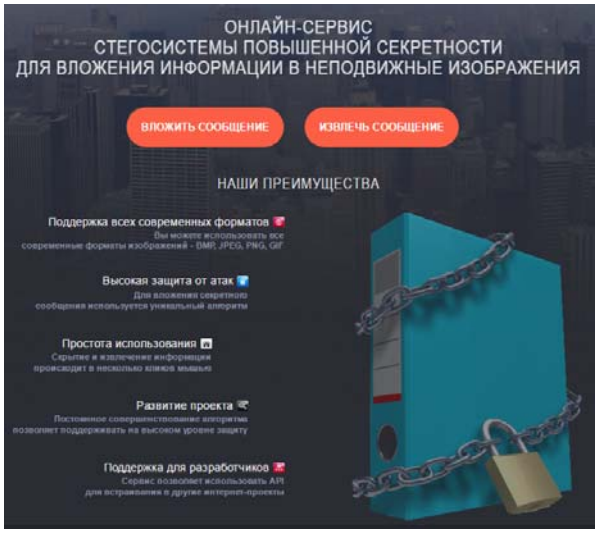


Рис. 2. Главное меню программы

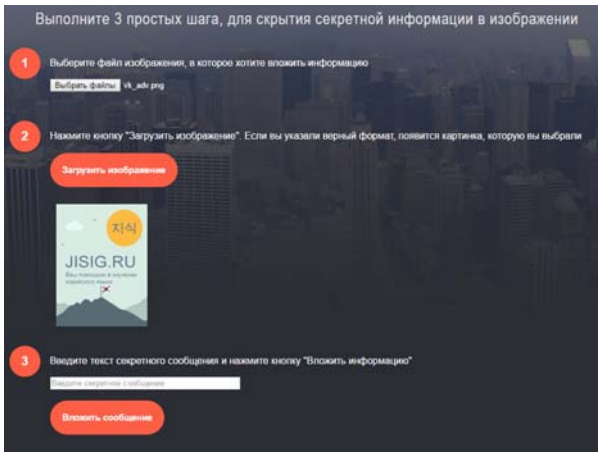


Рис. 3. Дружественный интерфейс онлайн-сервиса при вложении секретного сообщения

На рисунке 3 представлен дружественный интерфейс, с помощью которого пользователь может вложить или извлечь информацию, выполнив три простых шага.

Первый шаг подразумевает собой загрузку выбранного изображения, которое будет использоваться как покрывающее сообщение.

Вторым шагом пользователь загружает, выбранное ранее им изображение, в программу. Если файл с изображением не поврежден и формат файла выбран верно, миниатюрное представление изображения отобразится на экране.

Последним шагом необходимо будет указать текст секретного сообщения в специально поле. После чего, пользователь должен нажать кнопку «Вложить сообщение».

На рисунке 4 показан результат успешного выполнения программы. Пользователь имеет также возможность скачать файл на электронный носитель и передать его любым возможным способом передачи файлов (электронная почта, flash-накопитель и т. д.).

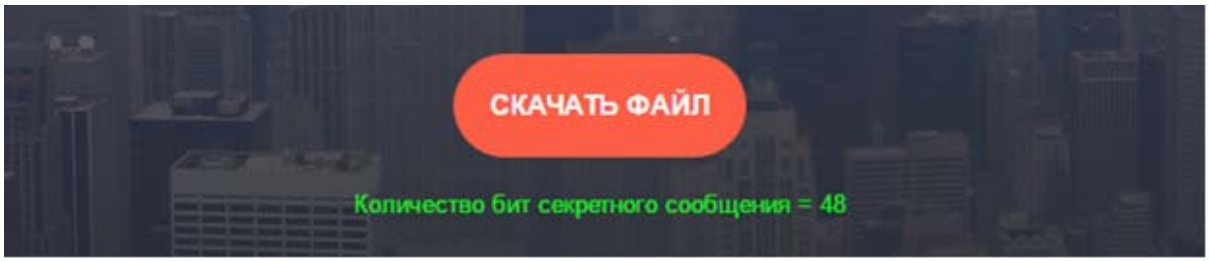


Рис. 4. Результат обработки, вложенной информации

Извлечение информации происходит по такому же алгоритму. Единственное различие между вложением и извлечением, это то, что при извлечении секретной информации, пользователь должен указать количество бит секретного сообщения.

На данный момент, для налаживания скрытого канала связи посредством данного сервиса, между корреспондентами должна быть предварительная договоренность об объеме передаваемой секретной информации. В дальнейшем, планируется доработать алгоритм таким образом, чтобы избавить пользователей от ограничения, связанного с объемом передаваемой информации.

В качестве дальнейших задач планируется внедрение в программу методов стегоанализа. Тогда после вложения секретного сообщения, пользователю будет представлена возможность проверить обнаруживаемость его стегосистемы. В качестве методов стегоанализа, предусматривается использование визуальной и статистической атак.

Список используемых источников

1. Fridrich J. Steganography in Digital Media: Principles, Algorithms and Applications. Cambridge University Press, Cambridge, England, 2009. 462 p. ISBN-13: 978-0521190190.

2. Коржик В. И., Небаева К. А. Основы стеганографии : учебно-методическое пособие. СПб. : СПбГУТ, 2015. 20 с.

3. Остроконский А. Д. Разработка стегосистемы, реализующей минимизацию количества изменений отсчетов покрывающего объекта при помощи матричного погружения / дипломная работа. СПб. : СПбГУТ, 2015. 92 с.

УДК 621.395

СТАТИСТИЧЕСКИЙ АНАЛИЗ ТРАФИКА ПРИ ЗАГРУЗКЕ ФОТОГРАФИИ В СОЦИАЛЬНЫЕ СЕТИ

В. Ю. Гойхман, А. Д. Дремина

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

Статья посвящена статистическому анализу трафика при загрузке фотографии в социальные сети. Исследования проводились для трех наиболее популярных сетей доступных для персонального компьютера: vk.com, facebook.com, twitter.com. Изображение загружалось по заданному расписанию, с использованием различных браузеров. В результате анализа получены значения величины сжатия изображения, зафиксированы значения скорости загрузки в разное время суток, получены соотношения объемов входящего и исходящего трафика.

Wireshark, Google Chrome, Firefox, Opera, Internet Explorer, vk.com, facebook.com, twitter.com, социальные сети, сетевой трафик.

Введение

На данный момент трафик социальных сетей составляет существенную часть глобального Интернет-трафика, обилие социальных сетей влечет за собой рост числа пользователей. В результате увеличивается и объем передаваемых данных, как следствие сеть становится более сложной и закрытой. Вопросам распознавания приложений на основе данных, собранных системой мониторинга трафика посвящен ряд работ, из которых можно выделить работы Andrew W. Moore, Konstantina Papagiannaki [1] и Wei Li [2]. С появлением социальных сетей перед операторами возникают новые задачи по организации телекоммуникационных сетей и выделению необходимых ресурсов. Исследованию количественных и качественных характеристик наиболее популярных социальных сетей посвящены статьи Главацкого С. П. [3], Воронкина А. С. [4], в которых описывается степень использования различных социальных сетей, а также исследование трафика с учетом эффекта самоподобия. Целью представленной статьи является анализ сетевого трафика, возникающего при загрузке фотографии в социальные сети: исследование зависимости скорости загрузки изображения от времени суток и дня недели, анализ объемов входящего и исходящего трафика и зависимость этих параметров от браузера. В процессе исследования загружалась одна и та же фотография в социальные сети vk.com, twitter.com и facebook.com с использованием четырех браузеров (*Chrome, Mozilla Firefox, Opera, Internet Explorer*) для каждой. Для захвата трафика использовалась системная утилита Wireshark, установленная на ноутбук с OCWindows 7. Подключение к сети интернет осуществлялось через wi-fi роутер.

Описание лабораторного стенда

Для проведения исследования использовалось следующее оборудование:

– роутер фирмы D-LINK;

– ноутбук (далее РМ – рабочее место) HP Pavilion dv6 с ОС Windows 7 и установленным ПО: Wireshark (Version 2.0.1); Chrome (48.0.2564.116 m); Mozilla Firefox (44.0.2); Opera (35.0.2066.92); Internet Explorer (11.0.9600.1780).

Описание проводимого эксперимента

При анализе статистических данных использовались 4 широко распространенных браузера по версии интернет-проекта статистики и веб-аналитики Openstat [5], доступных для РМ: Chrome, Mozilla Firefox, Opera и Internet Explorer. Испытаниям подвергались социальные сети vk.com, twitter.com и facebook.com, одни из наиболее популярных, по данным ресурса «SEO AUDITOR» [6] на январь–март 2016 г.

В ходе эксперимента в каждую из социальных сетей с помощью браузеров последовательно загружалась фотография размером 11,9 Мбайт расширения .jpeg и был захвачен трафик каждого испытания для дальнейшего анализа.

До начала проведения экспериментов, на РМ были отключены работающие службы, являющиеся источником сетевого трафика, после чего был повторно захвачен трафик для фильтрации в будущем IP-адресов, задействованых в фоновом режиме работы РМ.

Исследование представляет собой 18 экспериментов, 6 из которых проведены около 4:00 часов утра, 6 – около 9:00 и 6 – около 21:00. Одним экспериментом считаются испытания, проведенные для одной социальной сети с использованием всех 4-х браузеров, в результате которого фиксируются следующие события: открытие браузера; переход на главную страницу социальной сети; авторизация; переход во вкладку «фотографии»; начало загрузки изображения; окончание загрузки; выход из учетной записи; закрытие вкладки социальной сети; закрытие браузера; остановка Wireshark.

Алгоритм обработки полученных данных

На этапе анализа для каждого эксперимента имеем 4 файла с захваченными пакетами формата. pcapng. В результате обработки предполагается получить данные о скорости загрузки и объемах входящего/исходящего трафика.

Первым шагом в обработке полученных при помощи программы Wireshark данных является их преобразование в файлы формата .csv. Далее файлы проходят программную обработку скриптом, написанным

на PHP. В ходе сопоставления IP-адресов доменным именам, выполненного с помощью интернет-ресурса bgp.he.net, было выявлено, что передача данных социальных сетей производится через протокол TCP. Далее анализ ведется только для TCP пакетов. На первом этапе пакеты группируются по сессиям (*tcp.stream*), после чего сессии с адресами, попавшими в категорию «Фильтр» отбрасываются и в дальнейшей обработке не принимают участия. Следующим шагом проверяется наличие флага SYN в заголовке первого пакета сессии, если флаг не установлен, сессия отбрасывается, так как считается открытой до начала проведения эксперимента. Затем оставшиеся сессии группируются в соответствии с выполнявшимися действиями. На выходе получаем длительности всех сессий, участвующих в испытании, их количество и характеристики: отброшена сессия, завершена, не подтверждена или не завершена (по наличию флагов RST, FIN, ACK после SYN). Производится общий подсчет уникальных адресов, а также подсчет уникальных адресов социальной сети. Помимо этого, вычисляется объем входящего и исходящего трафика и строится график зависимости объема (байт) от времени (с). С использованием данных о начале загрузки фотографии и объёме переданных данных, проводится анализ участвующих в этой загрузке адресов, после чего вычисляется скорость загрузки.

Результаты исследования

1. Сжатие изображения. В ходе проведения экспериментов, было выявлено, что коэффициент сжатия варьируется в пределах от 10 до 85 и является величиной постоянной для каждой пары браузер – социальная сеть (табл.). При загрузке фотографии в facebook.com изображение подвергается наибольшему сжатию: величина коэффициента равна 85. Для twitter.com исследуемый коэффициент сжатия также является величиной постоянной равной 60. В социальной сети vk.com в браузере Chrome фотография подвергается наибольшему сжатию (35), в то время как для остальных браузеров (*Mozilla Firefox, Opera, IExplorer*) эта величина одинакова и равна 10.

ТАБЛИЦА. Коэффициенты сжатия изображения

Соц.сеть / браузер	Chrome	Mozilla Firefox	Opera	Internet Explorer
vk.com	35	10	10	10
twitter.com	60	60	60	60
facebook.com	85	85	85	85

2. Исследование зависимости скорости загрузки фотографии от дня недели и времени суток. В процессе анализа полученных данных (рис. 1–3) выявить зависимость скорости загрузки от времени суток и от дня недели не удалось, возможно, причиной того является загруженность сети. Однако

стоить отметить, что для соц.сетей vk.com, twitter.com, facebook.com значение скорости загрузки в браузере IExplorer наибольшее и в среднем равно 2,8 Мбайт/с, 2,0 Мбайт/с и 2,7 Мбайт/с соответственно. Для соц. сеть vk.com значение скорости во всех браузерах около 2,8 Мбайт/с, для платформы facebook во всех исследуемых браузерах, кроме IExplorer это значение находится в районе 0,7 Мбайт/с. И наконец для соц.сети twitter скорость загрузки колеблется около 0,1 Мбайт/с, для всех браузеров кроме IExplorer.

3. Исследования объема входящего и исходящего трафика. На основе полученных результатов (рис. 4–6: штрихпунктирная линия – исходящий трафик, сплошная – входящий) можно сделать вывод, что для vk.com (браузер *chrome*), twitter и facebook сжатие изображения происходит перед отправкой на сервер. Аналогично скорости загрузки, зависимость объема трафика от времени суток и дня недели не была найдена. Для социальной сети vk.com величина исходящего трафика (12,0 Мбайт) превышает входящий (от 0,5 до 3 Мбайт) во всех браузерах кроме Chrome, где соотношение объемов трафика в среднем является одинаковым (1 Мбайт). В соц. сети twitter.com объем исходящего (около 4,0 Мбайт) трафика превосходит входящий (от 0,1 до 2,0 Мбайт) во всех 4х браузерах. Для соц. сети facebook.com картина схожа с ситуацией vk.com для браузера Chrome: входящий и исходящий трафик порядка 1 Мбайт, за исключением браузера Mozilla, где объем входящих данных (≈ 3 Мбайт) превосходит объем исходящих (≈ 1 Мбайт).

Заключение

В ходе исследования было выявлено:

1) наибольшему сжатию изображение подвергается в социальной сети facebook.com в 85 раз, а наименьший коэффициент сжатия, равный 10 у сервиса vk.com. В twitter.com значение равно 60;

2) изображения в соц. сеть vk.com груязтся с наибольшей скоростью (около 2,8 Мбайт/с) в сравнении с остальными сетями; в социальную сеть tweeter.com с наименьшей(0,1 Мбайт/с).

Самая высокая скорость загрузки фотографий в браузере IExplorer для всех соц.сетей (около 2,5 Мбайт/с). В остальных браузерах результаты схожи (2,8 Мбайт/с – vk.com; 0,1 Мбайт/с – twitter.com; 0,7 Мбайт/с – facebook.com);

3) в социальной сети facebook.com объем входящего и исходящего трафика наименьший: 1 Мбайт и 0,8 Мбайт соответственно. В twitter.com объем входящего трафика 3,8 Мбайт, исходящего – от 0,1 до 2 Мбайт. В vk.com исходящий трафик – 12 Мбайт, входящий от 1 Мбайт до 2 Мбайт, кроме Chrome, где исходящий и входящий около 1 Мбайт.

В целом, для всех четырех браузеров в 90 % случаев объем переданных данных превосходит объем полученных.

Стоит также отметить, что на данном этапе обнаружить зависимость скорости передачи изображения, а также объема трафика от времени суток и дня недели не удалось.

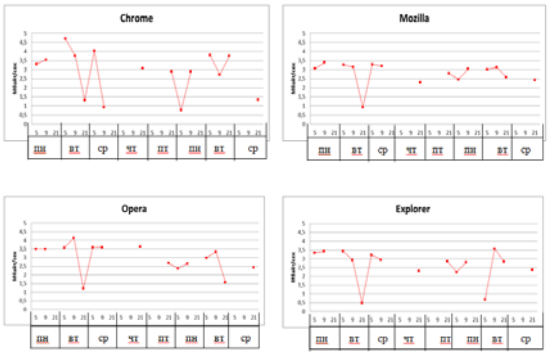


Рис. 1. Графики зависимости скорости от времени суток и дня недели. vk.com

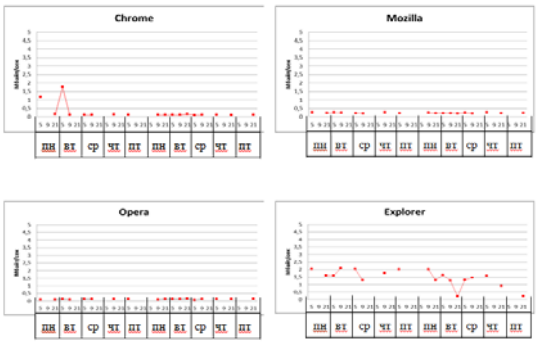


Рис. 2. Графики зависимости скорости от времени суток и дня недели. twitter.com

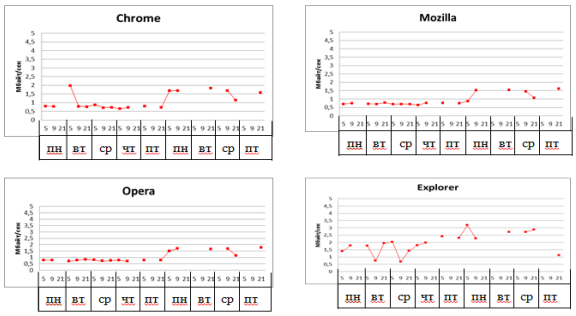


Рис. 3. Графики зависимости скорости от времени суток и дня недели. facebook.com

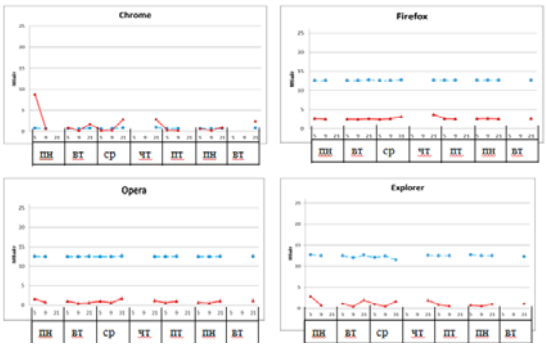


Рис. 4. Графики зависимостей входящего и исходящего трафика от времени суток и дня недели. vk.com

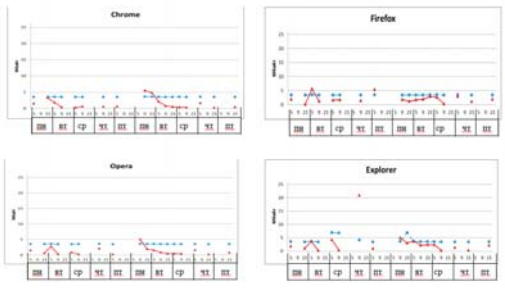


Рис. 5. Графики зависимостей входящего и исходящего трафика от времени суток и дня недели. twitter.com

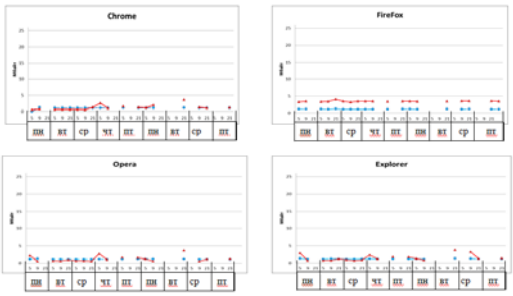


Рис. 6. Графики зависимостей входящего и исходящего трафика от времени суток и дня недели. facebook.com

Список используемых источников

1. Andrew W. Moore, K. Papagiannaki. Toward the Accurate Identification of Network Applications. University of Cambridge, 2005. – 14 p.
2. Wei Li. Toward the Accurate Efficient Online Traffic Classification. Cambridge University Computer Laboratory, 2007. – 18 p.
3. Главацкий С. П. Статистический анализ трафика социальных сетей // Наукові праці ОНАЗ ім. О. С. Попова. 2013. № 2. С. 94–99.
4. Воронкин А. С. Социальные сети: эволюция, структура, анализ // Образовательные технологии и общество. 2013. Т. 17. № 1. С. 650–675.
5. Интернет-проект статистики и веб-аналитики голландской компании «OpenStat B.V.» [Электронный ресурс] / URL: https://www.openstat.com (дата обращения 01.03.2016).
6. Сервис консальтинга и аналитики [Электронный ресурс] / URL: http://www.seo-auditor.ru/ (дата обращения 01.03.2016).

УДК 004.9

ПРОТОКОЛЫ ИНТЕРНЕТА ВЕЩЕЙ

В. Ю. Гойхман, А. А. Савельева

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

В статье рассматриваются протоколы Интернета вещей, их особенности, варианты применения. Приводится анализ и обосновывается выбор протокола в зависимости от планируемой сети Интернета вещей. Актуальность данной темы обусловлена многообразием существующих протоколов, стандартов Интернета вещей и отсутствием устоявшейся терминологии, описывающей концепцию в целом.

Интернет вещей, IoT, Протоколы IoT, M2M, XMPP, SOAP, COAP, STOMP, MQTT, DDS.

На сегодняшний день лавинное развитие Интернета вещей замедляется многообразием различных стандартов и протоколов. Вопросами стандартизации и практического внедрения Интернета вещей занимаются многие международные организации (ITU-T (Y.2060) [1], IEEE, ETSI (TR103 290) [2], OASIS), неправительственные ассоциации (oneM2M), альянсы производителей и операторов (IERC, IPSO), партнерские проекты (IoT-A). При этом существующие решения в данном направлении чаще носят разобщенный характер и направлены на достаточно локальные задачи. Отсюда и другое препятствие – многообразие протоколов. При интеграции Интернета вещей такая проблема приводит к вынужденному отвлечению на подбор подходящего протокола, часто имеющего определенные ограничения во взаимодействии с другими протоколами.

При исследовании было выявлено, что данной тематике в русскоязычном сегменте посвящено не так много литературы и публикаций [3, 4], а находящиеся в открытом доступе источники не раскрывают в полной мере интересующий вопрос применения протоколов Интернета вещей. В тоже время, в зарубежных источниках (количество которых существенно) данный вопрос поднимается все чаще, однако, информация также достаточно разобщена и носит ознакомительный характер [5, 6, 7]. Таким образом, очевидна необходимость в обобщении имеющихся материалов и их систематизации.

Цель настоящей статьи – анализ существующих протоколов и выработка рекомендаций по их использованию. В данных целях были выявлены особенности протоколов, протоколы распределены по задачам, решаемым с помощью их использования.

При реализации сети необходимо: Зарегистрировать устройство/узел; Сконфигурировать устройств/узел; Осуществить сбор и агрегацию данных.

Задача 1. Регистрация сенсора/узла

Понятие регистрации, как операции, неразрывно связано с адресацией. Представим некоторые примеры:

1) Server Name Indication (SNI) – часть протокола TLS, позволяющая клиенту сообщать имя хоста, с которым он желает соединиться.

2) Технологии автоматической идентификации Auto-ID (технологии штрих-кодов, RFID, различные коды и метки, магнитные полосы, смарт-карты и биометрические данные).

3) Уникальный серийный номер устройства.

4) Адресация XMPP.

Далее подробнее будет рассмотрена адресация протокола XMPP, поскольку именно с его помощью в относительно небольшой персональной сети можно назначить удобные адреса.

XMPP (*Extensible Messaging and Presence Protocol*) – расширяемый протокол обмена сообщениями и информацией о присутствии [8]. Применительно к Интернету вещей XMPP обеспечивает простой способ адресации устройств. Для идентификации пользователей используются запоминающиеся идентификаторы JID, по формату похожие на адреса электронной почты (например, *username@jabber.ru*). В протоколе XMPP используется текстовый формат XML. Протокол работает по TCP.

Адресация XMPP особенно удобна, когда данные передаются между отдалёнными, чаще всего независимыми точками, как в случае связи между двумя абонентами. Например, так возможно подключить домашний «умный» термостат к веб-серверу для получения к нему доступа с телефона.

Задача 2. Конфигурация устройств/узлов сети

Обычно переменные конфигурируются при заводской сборке. Иногда конфигурация устройства производится специальной утилитой. Для изменения изначальных настроек удаленно возможно использовать несколько протоколов (в зависимости от выбора «основного» протокола обмена сообщениями в сети). Наиболее часто используемый – SOAP, так как у этого протокола выделен механизм доступа RPC (*Remote Procedure Call*), который отвечает за удалённый вызов функций.

SOAP (*Simple Object Access Protocol*) – протокол обмена структурированными и произвольными сообщениями формата XML в распределённой вычислительной среде [9]. Также это базовая модель соединения, обеспечивающая согласованную передачу сообщения от отправителя к получателю, и допускающая наличие посредников.

Протокол SOAP базируется на сообщениях, которые разделяются на два типа: запросы и ответы. SOAP поддерживает два механизма доступа – SOAP RPC и SOAP Message [9].

SOAP RPC представляет собой простой протокол «запрос-ответ», который основывается на объекте Call. Этот объект используется для синхронного удаленного вызова процедур с помощью XML.

SOAP Message – это протокол для посылки и обработки сообщений, который может использоваться для асинхронных коммуникаций. Подразумевает немедленный или отложенный ответ на запрос.

Задача 3. Сбор и агрегация данных

Упомянутые выше протоколы также могут использоваться для решения этой задачи. В зависимости от условий, в которых реализуется сеть, подбирается наиболее подходящий протокол.

Для сети, в которой есть вероятность использования нескольких комбинаций разных протоколов, нуждающейся в простом протоколе передачи сообщений, можно использовать STOMP**.**

STOMP – Simple (*or Streaming*) Text Oriented Message Protocol – простой протокол обмена сообщениями, предполагающий широкое взаимодействие со многими языками, платформами и брокерами [10].

Протокол похож на HTTP, и работает над TCP. Обеспечивает совместимый формат передачи, что позволяет клиентам STOMP общаться с любым брокером сообщений, поддерживающим данный протокол. Таким образом, это способ взаимодействия, разработанный для обмена сообщениями между платформой и клиентом, описанных на разных языках программирования и разным ПО. Поддерживает большое количество совместимых клиентских библиотек, связанных языков.

Для сети с ограниченными ресурсами, низким энергопотреблением больше подойдет протокол COAP.

COAP (*Constrained Application Protocol*) – это специализированный протокол передачи, разработан рабочей группой IETF – CORE, учитывающий различные вопросы среды реализации в ограниченных сетях, узлах M2M приложений и т. д. [11]. COAP можно рассматривать как дополнение к HTTP. В стеке протоколов COAP лежит над UDP. Как в HTTP, некоторые из сообщений COAP подразумевают запросы/ответы. Позволяет серверам организовывать потоковую передачу изменений состояния клиентов.

Для загруженных сетей с большим количеством устройств рациональнее применять протокол, снижающий нагрузку на канал за счет организации очередей – протокол MQTT.

Протокол MQTT (*Message Queue Telemetry Transport*) – основное его назначение – телеметрия, дистанционный мониторинг. Реализуется по принципу «Издатель-подписчик», позволяет устройствам посылать и получать данные, когда возникает некоторое событие. MQTT – бинарный протокол обмена сообщениями с публикацией/подпиской, работающий поверх TCP [12]. Упрощенная схема, иллюстрирующая обмен сообщениями MQTT представлена ниже (рис. 1) [3]. Сообщения отправляются в очередь сообщений – контейнер или блок, в котором хранятся сообщения в процессе их пересылки. Приложение-брокер играет роль посредника. Сообщение хранится в очереди до тех пор, пока оно не будет доставлено.

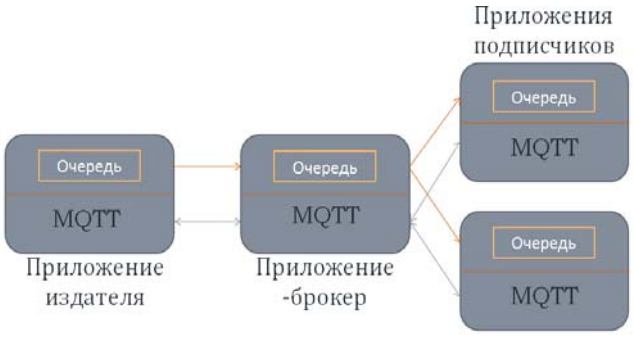


Рис. 1. Обмен сообщениями MQTT

Также для распределения нагрузки используется протокол DDS.

Протокол DDS (*Data Distribution Service*) распределяет данные по другим устройствам [13]. DDS реализует прямую шинную связь между устройствами на базе реляционной модели данных. Протокол DDS реализуется над UDP.

Операция чтения осуществляется на всех доступных устройствах. Данные не удаляются из локального кэша DDS в результате операции и могут быть прочтены снова при указании соответствующих параметров. Получение данных осуществляется тремя способами [13]:

1) Опрос (*polling*) – приложение периодически запрашивает DDS для получения новых данных или информирования о смене состояния.

2) Списки ожидания (*WaitSets*) – приложение регистрирует в DDS списки ожидания и ждет, пока одно из переданных событий не произойдет.

3) «Слушатели» (*listeners*) – приложения регистрирует в DDS классы-слушатели, которые будут информированы при наступлении событий.

В заключение описания сбора и агрегации данных, для наглядности приведем сравнительную таблицу, где главный критерий – назначение протокола (табл.).

ТАБЛИЦА. Сравнение протоколов сбора и агрегации

Прот.	Трансп.	Назначение	Особенность
STOMP	TCP	Для сети, в которой вероятно использование нескольких комбинаций разных протоколов, нуждающейся в простом протоколе обмена сообщениями	Взаимодействие со многими языками, платформами и брокерами
COAP	UDP	Для сети с ограниченными ресурсами, низким энергопотреблением	Учитывает различные вопросы среды реализации в ограниченных сетях
MQTT	TCP	Для загруженных сетей с большим количеством устройств	Использование механизма очередей сообщений
DDS	UDP	Для сетей, нуждающихся в распределении нагрузки	Реализует прямую шинную связь между устройствами на базе реляционной модели данных

Выводы

Подводя итог, можно составить следующую схему (рис. 2), иллюстрирующую оптимальное применение определенного протокола на различных отрезках сети, с учетом особенностей каждого из них. Примечание: Gateway – шлюз, приложение-брокер, либо сенсорный узел.

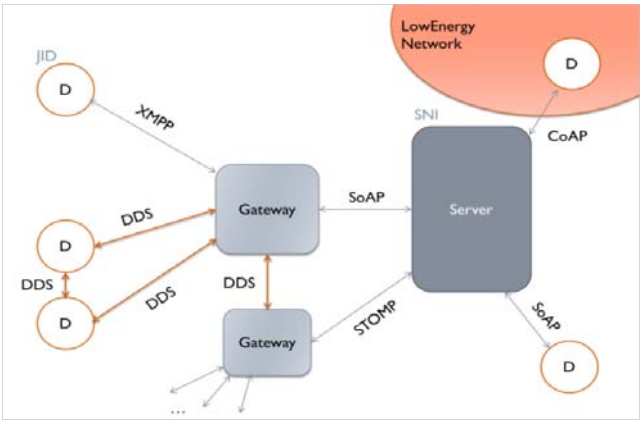


Рис. 2. Обобщающая схема

Интернет вещей и M2M предполагают большое количество вовлеченных устройств, некоторые могут иметь вычислительные мощности и ограничения, к которым не готовы традиционные протоколам связи. Вероятно, необходимо так же классифицировать их по нескольким ключевым параметрам: качеству сервиса, адресации и т. д.

Ключевые особенности протоколов зависят от их предполагаемого применения. Основные задачи протоколов различны, различны архитектуры и возможности. Поэтому к выбору оптимального протокола для своего приложения нужно подходить основательно, объективно взвешивать все положительные и отрицательные свойства каждого из них, исходя из конкретных потребностей.

Список используемых источников

1. ITU-T: Recommendations: Y Series: Y.2060 / Overview of the Internet of things // 2012. С. 3–9.

2. ETSI Recommendation TR 103 290 V1.1.1 / Machine-to-Machine communications (M2M) // 2015. 10 с.

3. Росляков А. В., Ваняшин С. В., Гребешков А. Ю. Интернет вещей / под ред. А. В. Рослякова. Самара : ПГУТИ, ООО «Издательство Ас Гард», 2014. 340 с.

4. Гольдштейн Б. С., Кучерявый А. Е. Сети связи пост-NGN. СПб. : БХВ-Петербург, 2014. 160 с.: ил. ISBN 978-5-9775-0900-8.

5. Vermesan O., Friess P. Internet of Things – From Research and Innovation to Market Deployment // River Publishers. 2014. PP. 106–112.

6. Schneider S. Understanding The Protocols Behind The Internet Of Things // Electronic Design. 2013. PP. 4–6.

7. Latvakoski J., Iivari A., Vitic P. A Survey on M2M Service Networks // Computers 2014. N 3(4). PP. 1.

8. Extensible Messaging and Presence Protocol (XMPP): Core // RFC-3920, 2004. PP. 2–4.

9. Box D., Ehnebuske D., Kakivaya G. Simple Object Access Protocol (SOAP) 1.1 // W3C. 2000. PP. 12–15.

10. The Constrained Application Protocol (CoAP). RFC 7252 – Proposed Standard. 2014. 5 p.

11. STOMP Protocol Specification, Version 1.2. Licensed under the Creative Commons Attribution v2.5 license. 2012. PP. 1–2.

12. MQTT V3.1 Protocol Specification. International Business Machines Corporation (IBM) Eurotech. 2015. PP. 1–2.

13. OMG (Object Management Group) DDS v1.4 – the DDS specification. 2015. PP. 8, 120.

УДК 621.39

АНАЛИЗ ПРОТОКОЛОВ ПЕРЕДАЧИ ДАННЫХ В МАГИСТРАЛЬНЫХ СЕТЯХ

Д. С. Гончарова, А. В. Ульянов

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

В статье рассматриваются протоколы, используемые для организации передачи пакетного трафика в оптических транспортных сетях OTN/xWDM. Производится анализ функций, реализуемых протоколами канального уровня, на основе заголовков кадров Ethernet, и GFP. Аргументируется наличие протокольной избыточности при инкапсуляции пакетного трафика в сети OTN. Предлагается использовать протокол GFP как базовый протокол канального уровня магистральных сетей с необходимостью расширения его функций посредством добавления полей заголовков. Производится расчет выигрыша пропускной способности магистральных сетей за счет отказа от Ethernet в сетях OTN на основе статистических данных о структуре трафика современных сетей и эксперимента, связанного с определением средних размеров пакетов мультисервисного трафика различного типа.

Optical Transport Network, OTN, Generic Framing Procedure, GFP, ethernet, коммутация, протокольная избыточность.

Технология спектрального уплотнения WDM и механизмы передачи данных, объединенные в стандарт OTN составляют базу современных магистральных сетей. Однако, OTN сети имеют серьезный недостаток – ручную коммутацию.

Сейчас такие крупные вендоры, как Infinera [1, 2], T8 [3] и др. задумываются о массовом производстве и внедрении интеллектуальных OTN сетей. В технологию OTN изначально закладывалась идея «прозрачной» передачи сетевого трафика, то есть эти сети служили по сути «удлинителем» между локальными сетями, однако концепция интеллектуального транспорта подразумевает согласованную работу между OTN и IP оборудованием [4].

В данной статье рассматривается структура канального уровня магистральных сетей и приводится анализ эффективности использования различных протоколов.

Ethernet и GFP

Рассмотрим процедуру инкапсуляции трафика различных услуг в кадры ODU. Так как ODU – это групповой кадр, то сравнивать его непосредственно с кадрами, например, Ethernet, не совсем корректно. Для размещения клиентских пакетов в групповом кадре ODU, используются индиви-

дуальные кадры GFP. Как уже было сказано ранее, идея «прозрачной» передачи подразумевала непосредственную инкапсуляцию кадров Ethernet в кадры GFP. Как видно из схемы (рис. 1), в этом случае возникает протокольная избыточность из-за использования нескольких протоколов канального уровня.

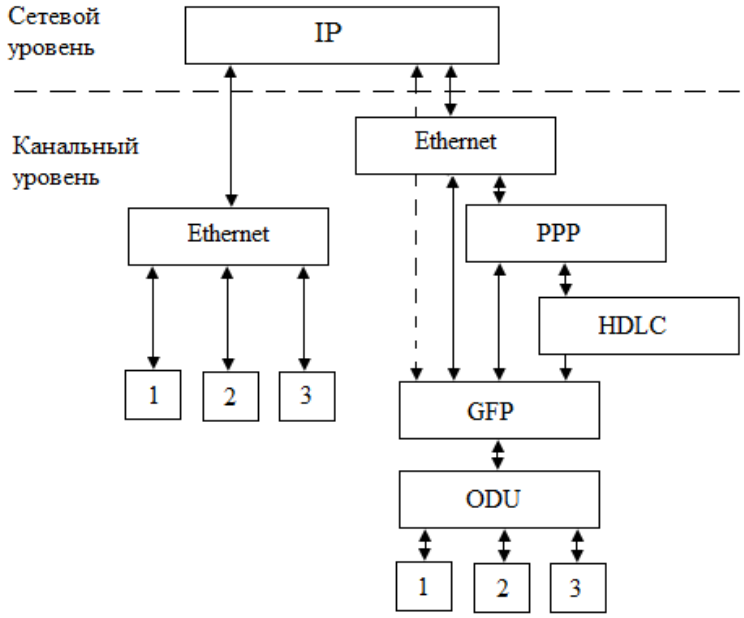


Рис. 1. Инкапсуляция мультисервисного трафика в кадры ODU

Преимуществом Ethernet является его широкое распространение в локальных сетях, а также хорошая взаимосвязь с протоколом сетевого уровня IP. Однако, Ethernet кадры в ODU упакованы быть не могут. Кроме того, MAC адресация, необходимая для коммутации в сетях Ethernet, здесь является избыточной, поскольку в сетях OTN коммутация осуществляется для групповых кадров ODU.

GFP, в свою очередь, поддерживает, согласно рекомендации G.7041, прямую инкапсуляцию IP пакетов, однако для него отсутствуют механизмы межуровневого взаимодействия, аналогичные Ethernet – IP.

Исходя из вышесказанного, можно использовать протокол GFP в качестве базового индивидуального канального уровня магистральных сетей. Тогда взаимодействие между оборудованием IP и OTN можно организовать с использованием протоколов GMPLS или SDN, для размещения сигнализации которых использовать заголовок расширения протокола GFP (рис. 2). Однако, немалую часть предоставляемых магистральным оператором услуг занимают низкоскоростные туннели второго уровня с разделением клиентских потоков по VLAN с тэгом согласно IEEE 802.1q. Такие потоки обрабатываются оборудованием сетевого уровня, хотя этого можно было бы избежать.

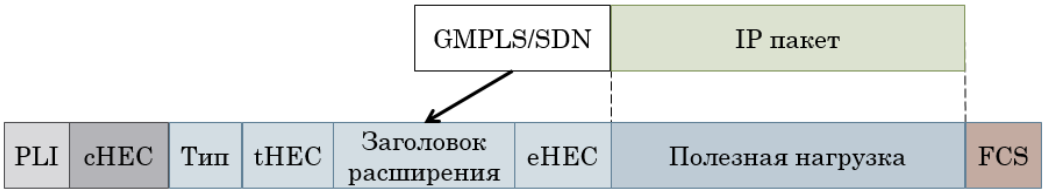


Рис. 2. Вариант размещения сигнализации в GFP-заголовке

Вариантом решения является совместимость протокола GFP с IEEE 802.1q. По аналогии с предыдущим решением, можно использовать заголовок расширения GFP, как показано на рисунке 3. В таком случае приходящий клиентский трафик будет поступать на коммутатор агрегации, trunk-порт которого будет включен непосредственно в OTN оборудование, минуя оборудование IP.

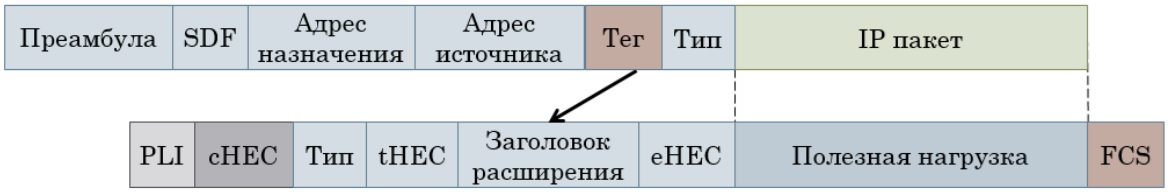


Рис. 3. Вариант размещения тэга 802.1q в GFP-заголовке

Расчет протокольной избыточности

Кроме того, избавление от некоторых протоколов и, как следствие, их заголовков, позволит дать некоторый выигрыш в пропускной способности магистральных каналов. Оценить эффективность предлагаемого метода можно, проанализировав статистику распределения трафика клиентских приложений [5].

Для расчета протокольной избыточности был проведен эксперимент, в котором было определено среднее значение длин кадров для трафика наиболее популярных приложений. В таблице приведены значения протокольной избыточности для каждого типа трафика.

ТАБЛИЦА. Статистические данные для различных типов трафика

Приложение	Доля объема трафика, %	Средний размер кадра, байты	Избыточность, %
Browsing	7	766	1,8
Chatting	5	232	5,7
Online Game	2	247	5,4
Downloading + BitTorrent (P2P)	27	1358	1,1

Приложение	Доля объема трафика, %	Средний размер кадра, байты	Избыточность, %
Online Video	55	1396	1

Средняя протокольная избыточность по всем приложениям составляет 1,4 %. Несмотря на то, что номинально это величина небольшая, выигрыш на магистральных каналах, например, с пропускными способностями 100 Гбит/с составляет до 1,5 Гбит/с.

Вывод

В статье показано наличие протокольной избыточности на канальном уровне магистральных сетей. Проведено сравнение и сделан вывод о преимуществе использования исключительно протокола GFP на индивидуальном канальном уровне, что позволит сделать шаг на пути согласования IP и OTN оборудования для дальнейшего развития интеллектуальных транспортных сетей. Были предложены варианты расширения протокола GFP для согласования с концепцией интеллектуального транспорта, требующие дальнейших исследований. На основе данных статистики трафика магистральной сети был рассчитан выигрыш от оптимизации протокольной структуры, составляющий в среднем 1,4 %.

Список используемых источников

1. Системный подход к многоуровневой автоматизации транспортной сети [Электронный ресурс] // Infinera corporation / USA. 2014. URL: https://www.infinera.com/russian/files/RU-Infinera-WP-Automate_Everything.pdf (дата обращения 13.04.2016).

2. Кляйн Р. Увеличение экономической эффективности сети при помощи IPoOTN [Электронный ресурс] // USA. 2013. URL: https://www.infinera.com/russian/files/RU-Infinera-WP-Improving_Economics.pdf (дата обращения 13.04.2016).

3. Цифровая кросс-коммутация OTN [Электронный ресурс] // Компания «Т8». URL: http://t8.ru/?page_id=6338 (дата обращения 13.04.2016).

4. Шмидт Э. Интегрированная OTN коммутация виртуализирует оптические сети [Электронный ресурс] // INFONETICS RESEARCH, INC, USA. 2012. URL: https://www.infinera.com/russian/files/RU-Infinera-WP-Infonetics-Integrated-OTN-Switching.pdf (дата обращения 13.04.2016).

5. Sandvine: Over 70% of North American Traffic is Now Streaming Video and Audio [Электронный ресурс] // Sandvine Incorporated. 2015. URL: https://www.sandvine.com/pr/2015/12/7/sandvine-over-70-of-north-american-traffic-is-now-streaming-video-and-audio.html (дата обращения 13.04.2016).

Статья предоставлена научным руководителем, кандидатом технических наук, доцентом О. А. Симониной.

УДК 004.021

ИССЛЕДОВАНИЕ МЕТОДОВ ПОСТРОЕНИЯ СТЕГОСИСТЕМ ДЛЯ ВИДЕОПОСЛЕДОВАТЕЛЬНОСТЕЙ

К. Н. Диканева, К. А. Небаева

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

В работе представлены результаты исследования методов построения стегосистем для видеофайлов, основанных на вложении в коэффициенты дискретно-косинусного преобразования. Рассмотрены методы построения MIDCAP и MIDVIS для вложения дополнительной информации в видеопоследовательности формата MPEG-4. Произведен анализ методов, выделены основные проблемы реализации методов вложения и возможности их решения.

стегосистема, видеопоследовательность, скрытая передача данных, MPEG-4.

Существует множество методов построения стегосистем для видеофайлов, основанных на вложении дополнительной информации в различные области видеопоследовательностей. В данной статье рассмотрен метод вложения информации в видеопоследовательность формата MPEG-4, основанный на вложении в коэффициенты дискретно-косинусного преобразования (*Discrete Cosine Transform* (DCT)).

Структура вложения в MPEG-4

Данные вкладываются в видео формата MPEG-4 во время процесса сжатия сырого видео YUV в формат MPEG-4 [1]. В широком смысле концепция вложения в MPEG-4 включает формирование intra- и inter- кадров с последующим кодированием. Оно включает такие составляющие, как DCT, квантование, вложение, предсказание, кодирование. Сжатие MPEG-4 включает формирование последовательности трех видов кадров – I-, P-, B-кадры [2]:

– I-кадры – intra-кадры, кодируются без ссылок на другие кадры, содержат неподвижное изображение и используются для построения других типов кадров;

– P-кадры – предсказуемые кадры, которые кодируются со ссылкой на предыдущий (с точки зрения приемника) принятый (I) или (P) кадр;

– B-кадры – двусторонне интерполируемые кадры, которые кодируются наиболее сложным образом. Такой кадр может строиться и на основе предыдущего кадра, и на основе последующего кадра, и как интерполяция между предыдущим и последующим кадрами.

Следовательно, в процессе сжатия MPEG-4 I-кадры – ключевые кадры, без которых реконструкция сжатого видео не возможна.

В [1] были предложены две схемы вложения данных, называемые MIDCAP (от англ. MIDdle CAPacity) и MIDVIS (от англ. MIDcap VISibilty). В схемах используются среднечастотные коэффициенты DCT для включения данных в процессе сжатия MPEG-4. MIDCAP предложена для улучшения емкости вложения. MIDVIS нацелена на улучшение визуального качества видео с вложением, уменьшения искажений путем включения данных в несглаженные (non-smoother) блоки.

Для вложения данных выбирается компонента яркости (*Y*) каждого I-кадра. Берется блок 8×8 компоненты яркости (*Y*) I-кадра, квантуются коэффициенты DCT и после данные включаются в этот блок. На рисунке 1 представлены основные шаги процедуры вложения данных в MPEG-4.

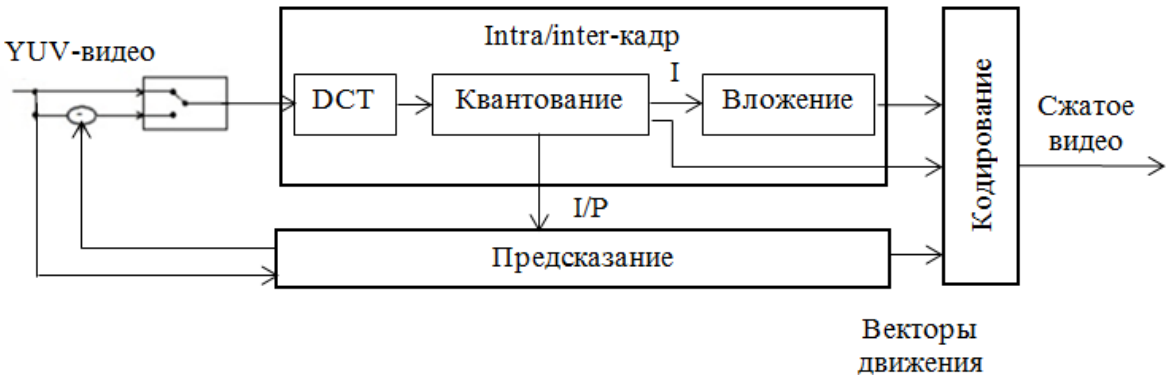


Рис. 1. Принцип вложения данных в MPEG-4

Сырое (необработанное) YUV-видео представляет собой последовательность кадров. Пусть $F = \{f_1, f_2, \dots, f_n\}$ – последовательность кадров сырого YUV-видео, где n – общее количество кадров. Каждый кадр $\overline{f_i} \epsilon F$ состоит из одной компоненты яркости (*Y*) и двух цветоразностных компонент (*U* и *V*).

Несмотря на то, что все типы кадров могут быть использованы для вложения информации, в рассматриваемых методах используются только I-кадры. Пусть $I = \{I_1, I_2, \dots, I_m\}$, где $m<n$. Соответственно, каждый кадр $I_i = \{Y^i, {C_b}^i, {C_r}^i\}$, где Y^i – компонента яркости кадра I_i и C_b C_r – цветоразностные компоненты кадра I_i. Данные будут вкладываться в компоненту Y^i. Каждая компонента размером $n_1 \times n_2$ разделена на блоки 8×8. Предполагается, что n_1 и n_2 кратны 8. Пусть $Y^i = \{{B_1}^i, {B_2}^i, \dots {B_l}^i\}$, где $B_j{}^i$ – j-ый блок 8×8 компоненты Y^i и $l = \frac{n_1 \times n_2}{64}$. Здесь $\widehat{m} = m \times l$ показывает общее число блоков в *I*-кадре. Эти непересекающиеся блоки 8×8 преобразуются при помощи дискретного косинусного преобразования следующим образом (1):

$$F_{u,v} = \frac{\alpha(u)\alpha(v)}{4} \sum_{x=0}^{7} \sum_{y=0}^{7} B_j^i(x,y)\hat{g}(x,y,u,v), \quad (1)$$

где $\hat{g}(x,y,u,v) = \cos\left(\frac{(2x+1)u\pi}{16}\right)\cos\left(\frac{(2y+1)v\pi}{16}\right)$,

$$\alpha(e) = \begin{cases} \frac{1}{\sqrt{2}}, & e = 0, \\ 1, & e \neq 0. \end{cases}$$

Итак, $0 \le u, v \le 7$ и $B_j^i(x,y)$ представляют значение интенсивности (пикселя) блока B_j^i в точке (x, y) в пространственной области и $F_{u,v}$ – это коэффициент в точке (u, v) в частотной области. Обратное дискретное косинусное преобразование определяется формулой (2), где $0 < x, y < 7$.

$$B_j^i(x,y) = \sum_{u=0}^{7}\sum_{v=0}^{7}\frac{\alpha(u)\alpha(v)}{4}F_{u,v}\hat{g}(x,y,u,v). \quad (2)$$

Пусть $\widehat{B^i} = \{\hat{B}_1, \hat{B}_2, \dots, \hat{B}_l\}$ – набор блоков 8×8 DCT-коэффициентов Y^i, $C^i = \{C_1, C_2, \dots, C_l\}$ – набор блоков 8×8 DCT-коэффициентов и $\bar{C}^i = \{\bar{C}_1, \bar{C}_2, \dots, \bar{C}_l\}$ – набор вложенных блоков в Y^i. $\boldsymbol{C} = \{C_i\}$ – это набор элементов в видеопоследовательности, в который предполагается вложение. $D_k(1 \le k \le 9)$ – набор квантованных DCT-коэффициентов от высокочастотной до низкочастотной области блока 8×8, как показано на рисунке 2. Эти наборы используются для вложения данных.

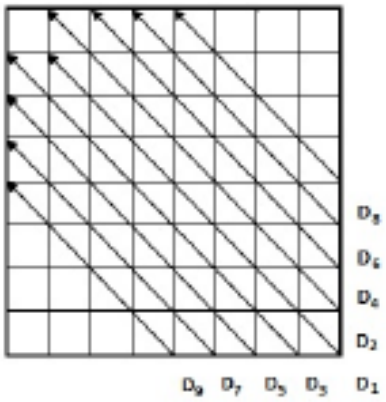


Рис. 2. Выбранные для вложения наборы

Процедура вложения данных

Для вложения данных используются компоненты среднечастотной области [3]. В каждый набор D_k вкладываются два последовательных бита $(s,t) \in I$, если это возможно. Решение о возможности вложения принимается на основе количества подряд идущих нулей (b_k) от высокой до низкой частоты. Если $b_k \ge 3$, то D_k подходит для вложения.

В процессе реализации схем вложения наиболее важными вопросами, которые необходимо решать являются конфликт данных (*data collision*) и избыточность данных [4]. Конфликт данных – это ситуация, при которой измененная информация (например, значение пикселей кадра, измененных

коэффициентов, т. д.), полученная в результате встраивания данных, смешивается с неизмененной во время восстановления исходного видео. Избыточность данных – это ситуация, при которой значение коэффициента (пикселя) превышает допустимый диапазон верхней или нижней границы.

В предложенных схемах проблема избыточности решается с помощью квантования DCT-коэффициентов, поскольку квантование ограничивает большие действительные числа блока до небольших целочисленных значений. Квантованные DCT-коэффициенты изменяются только на ±1 для достижения реверсивности схемы (чтобы можно было в полной мере восстановить оригинальное видео). Это очень небольшое изменение, поэтому оно не приведет к избыточности DCT-коэффициентов. Для исправления проблемы конфликта данных в предложенных схемах определяются определенные условия, которые описывают данную проблему и меры по ее устранению. Пусть $d_{k,j}$ первый ненулевой элемент D_k, который приводит к проблеме конфликта данных в следующих неоднозначных условиях для $1 \le k \le 9$ и $1 \le j \le K(k)$:

1) $b_k < 3;\ d_{k,j} \neq 0, d_{k,j+1} = d_{k,j+2} = 0;\ j = 0$ и $j + 2 \le K(k)$;
2) $b_k < 3;\ d_{k,j} \neq 0, d_{k,j+1} = \pm 1, d_{k,j+2} = 0;\ 1 \le j \le 3, j + 2 \le K(k)$;
3) $b_k < 3;\ d_{k,j} \neq 0, d_{k,j+1} = 0;\ 2 \le j \le 3, j + 1 \le K(k)$;
4) $3 \le b_k \le 5;\ d_{k,j} \neq 0, d_{k,j+1} = 0;\ j + 1 \le K(k); s = 0, t = 0$;
5) $3 \le b_k \le 4; d_{k,j} \neq 0, d_{k,j+1} = \pm 1, d_{k,j+2} = 0; j + 2 \le K(k); s = t = 0$.

Если какое-либо из условий присутствует в D_k, то значения $d_{k,j} \neq 0$ преобразовываются в $d'_{k,j}$, для устранения проблемы конфликта данных по формуле (3):

$$d'_{k,j} = \begin{cases} d_{k,j} + 1, & \text{если } d_{k,j} > 0, \\ d_{k,j} - 1, & \text{если } d_{k,j} < 0. \end{cases} \quad (3)$$

После устранения проблемы конфликта данных в подходящий для вложения D_k вкладываются два бита информации s и t.

Процедура извлечения данных

Данные извлекаются на основании наличия ненулевых значений в наборе D_k. Для каждого D_k в блоке с вложением $d_{k,j}$ – ненулевая компонента с наибольшей частотой. И далее данные извлекаются s и t, если они есть в D_k по следующим правилам:

1) $d_{k,j-1} = 0, d_{k,j} = \pm 1, d_{k,j+1} = 0; 3 < j + 2 \le K(k)$, то $s = 0, t = 1$;
2) $d_{k,j-2} = d_{k,j-1} = 0, d_{k,j} = \pm 1, d_{k,j+1} = 0; 3 < j + 1 = K(k)$,
то $s = 0,\ t = 1$;
3) $d_{k,j} = \pm 1, d_{k,j+1} = d_{k,j+2} = 0, d_{k,j+3} \neq 0; 3 < j + 3 \le K(k)$,
то $s = 1,\ t = 0$;

4) $d_{k,j-1} = 0, d_{k,j} = \pm 1, d_{k,j+1} = d_{k,j+2} = 0; 3 < j + 2 = K(k)$,
то $s = 1,\ t = 0$;
5) $d_{k,j} = d_{k,j+1} = \pm 1, d_{k,j+2} = 0, d_{k,j+3} \neq 0; 3 < j + 3 \leq K(k)$,
то $s = 1,\ t = 1$;
6) $d_{k,j-1} = 0, d_{k,j} = d_{k,j+1} = \pm 1, d_{k,j+2} = 0; 2 < j + 2 \leq K(k)$,
то $s = 1,\ t = 1$;
7) $d_{k,j-3} = d_{k,j-2} = d_{k,j-1} = 0, |d_{k,j}| > 1; 3 < j \leq K(k)$, то $s = \ t = 0$;
8) $d_{k,j-3} = d_{k,j-2} = d_{k,j-1} = 0, d_{k,j} = \pm 1; j = K(k); j > 3$, то $s = t = 0$
9) $d_{k,j-3} = d_{k,j-2} = d_{k,j-1} = 0, d_{k,j} = \pm 1, d_{k,j+1} \neq 0; 4 < j < K(k)$, то $s = 0,\ t = 0$;
10) $d_{k,j} \neq \pm 1, d_{k,j+1} = \pm 1, d_{k,j+2} = 0; 1 < j < 3$, то нет вложения;
11) $d_{k,j} \neq \pm 1, d_{k,j+1} = 0; 2 < j < 3$, то нет вложения;
12) $d_{k,j} \neq \pm 1, d_{k,j+1} = 0, d_{k,j+2} = 0; j = 1$, то нет вложения.
13) Если $D_k = \left(d_{k,1}, d_{k,2}, \dots, d_{K(k)}\right) = (0, 0, \dots, 0),$ то для $4 \leq j \leq K(k)$ $s = 0,\ t = 0$.

Суть использования предложенных схем состоит в том, что для улучшения визуального качества предлагается вкладывать данные в несглаженные блоки. Гладкие участки видео не будут затрагиваться при вложении, что приведет к меньшим искажениям.

В процессе исследования было выявлено, что при использовании предложенных схем можно увеличить емкость вложения почти в два раза по сравнению другими методами, при этом поддерживается приемлемое визуальное качество видео.

Список используемых источников

1. Gujjunoori S., Amberker B. B. Reversible data embedding for MPEG-4 video using middle frequency DCT coefficients // Journal of Informational Hiding and Multimedia Signal Proccessing. 2014. Vol. 5. N 3. PP. 408–419.

2. Грибунин В. Г., Оков И. Н., Туринцев И. В. Цифровая стеганография. М. : Солон-Пресс, 2002. 272 с.

3. Gujjunoori S., Amberker B B. DCT based reversible data embedding for MPEG-4 video using HVS characteristics // Journal of Information Security and Applications. 2013. Vol. 18. Issue 4. PP. 157–166.

4. Gujjunoori S., Amberker B. B. A DCT based reversible data hiding scheme for MPEG-4 video // Proc. of the Fourth International Conference on Signal and Image Processing. 2012. Vol. 1. PP. 69–81.

УДК 004.75

ИССЛЕДОВАНИЕ ИНСТАЛЛЯЦИИ БЕСПРОВОДНЫХ СЕНСОРНЫХ УЗЛОВ С БЕСПИЛОТНЫХ ЛЕТАТЕЛЬНЫХ АППАРАТОВ РАЗЛИЧНОГО ТИПА

Ч. З. Динь, Р. В. Киричек

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

В последние годы в исследованиях всепроникающих сенсорных сетях появился новый класс сетей – летающие сенсорные сети. В качестве летающих узлов используются общедоступные беспилотные летательные аппараты, которые собирают данные с удаленных сенсорных узлов. Одной из ключевых является задача инсталляции сенсорных узлов на большой территории, которая может быть решена с помощью БПЛА. В статье рассмотрены подходы инсталляции сенсорных узлов с БПЛА в зависимости от разных критериев. В частности, анализируются разные типы БПЛА и их возможности (время полета, скорость, грузоподъемность и др.) для доставки сенсорных узлов на заданную территорию и последующую инсталляцию.

всепроникающая сенсорная сеть, летающая сенсорная сеть, беспилотный летающий аппарат, БПЛА, беспроводный сенсорный узел, инсталляция, покрытие.

В последние годы в связи с популяризацией общедоступных беспилотных летательных аппаратов появился новый класс сетей – летающие сенсорные сети (ЛСС). Летающая сенсорная сеть предполагается два сегмента: наземный и летающий. В качестве летающих узлов используются общедоступные беспилотные летательные аппараты (БПЛА), которые собирают данные с удаленных сенсорных узлов. Первичной задачей при построении таких сетей является инсталляция сенсорных узлов на местности (наземный сегмент) для наилучшего покрытия территории и последующего оптимального сбора информации [1].

Задача инсталляции сенсорных узлов на большой территории может быть решена с помощью БПЛА. С этой целью необходимо обеспечить максимальное покрытие территории с минимальным числом узлов (минимизировав потребление энергии и, тем самым, продлив жизненный цикл сенсорных узлов).

На сегодняшний день возрастает интерес к использованию беспилотных летательных аппаратов (БПЛА) для военного и гражданского применения для задач дистанционного зондирования, картографирования, мониторинга дорожного движения, поиска и спасения [2, 3]. БПЛА стали общедоступными с учетом удешевления деталей для их изготовления (корпус, двигатель, радиоаппаратура, навигация и др. В зависимости от формы крыла и структуры фюзеляжа БПЛА могут быть классифицированы как:

– с жестким крылом (БПЛА самолетного типа: самолет, планер, дельтаплан);

– с вращающимся крылом (БПЛА вертолетного типа: вертолет, мультикоптер, автожир) [4, 5, 6]. В таблице 1 представлено сравнение параметров типового БПЛА общего пользования различного типа.

ТАБЛИЦА 1. Сравнения БПЛА различных типов [5, 6, 7]

	БПЛА самолетного типа	БПЛА вертолетного типа
Класс БПЛА	Микро- и мини-БПЛА ближнего радиуса действия (до 30 км)	Микро- и мини-БПЛА ближнего радиуса действия (до 10 км)
Скорость горизонтального полета, км/ч	40÷100	0÷60
Рабочая высота полёта над уровнем земли, м	60÷1000	5÷500
Продолжительность полета, мин.	до 60	до 30
Максимальный взлетный вес, кг	3,5	2,5
Максимальная масса полезной нагрузки, кг	1,2	0,8
Размер посадочной площадки, не менее, м×м	2x20	1x1
Режимы полета	Автоматический, полуавтоматический	Автоматический, полуавтоматический
Обслуживающий персонал, чел.	2–3	1–2
Типа взлёта/посадки	– При взлете: используется взлетно-посадочная полоса, стартовые катапульты или запускаемые «с руки». – При посадке: взлетно-посадочная полоса, парашют, или специальные уловители (тросы, сетки, растяжки).	Вертикальный взлет/посадка
Специальные способности	Большая длительность полета, большая максимальная высота полета и высокая скорость	Способность зависания в точке и высокая маневренность

Для того, чтобы определиться с выбором оптимального БПЛА для применения в задачах инсталляции сенсорных узлов проанализируем данные в таблице 1.

– БПЛА самолетного типа может использоваться в задачах случайной инсталляции беспроводных сенсорных узлов на средних и больших территориях, благодаря высокой длительности полета, максимальной высоте полета, высокой скорости, высокому показателю полезной нагрузки (возможность переносить большое количество сенсорных узлов) и возможности инсталляции с приблизительной точностью (рис. 1*а*). К отрицательным параметрам можно отнести то, что целевая область может быть не покрыта сенсорными узлами, что является недопустимым, например, в задачах охраны территории (рис. 1*б*).

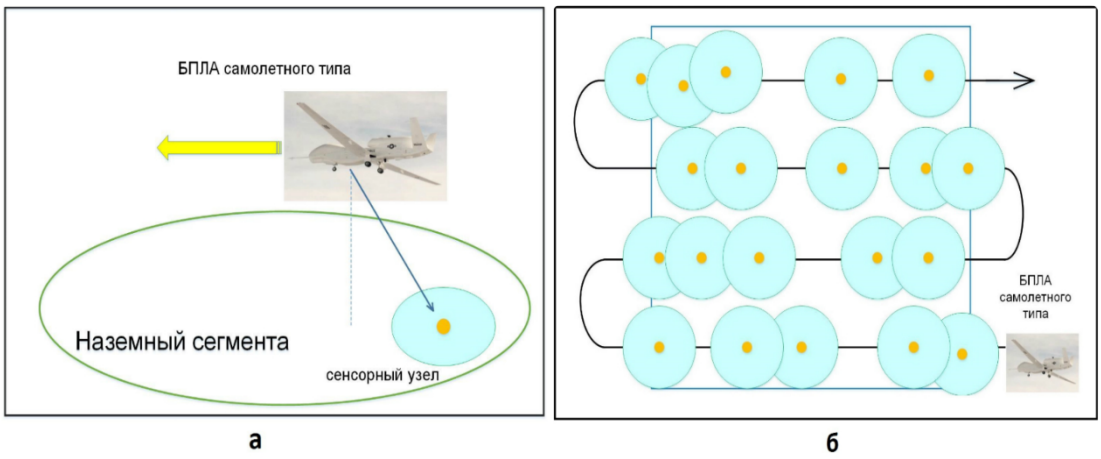


Рис. 1. БПЛА самолетного типа инсталлирует сенсорные узлы с приблизительной точностью (а); отдельные области не покрываются полностью (б)

Чтобы оценить вероятность покрытия целевой области, была разработана математическая модель, которая представлена в [8].

– БПЛА вертолетного типа (мультикоптер) может использоваться в детерминированной инсталляции беспроводных сенсорных узлов на узкой и средней областях, так как он имеет способность зависания в точке, а также высокую маневренность, что является полезным для более точной инсталляции сенсорных узлов в заданных целевых точках (рис. 2).

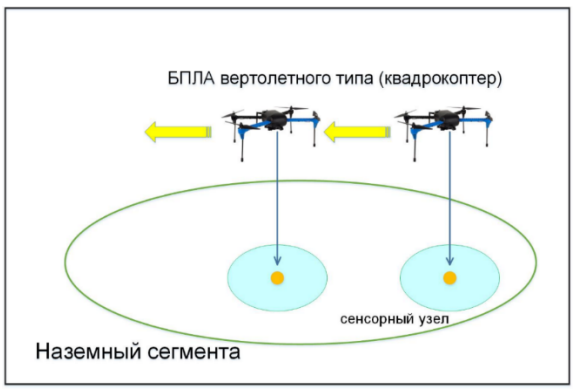


Рис. 2. БПЛА вертолетного типа устанавливает сенсорные узлы в точности

Для вычисления размеров целевой области, предполагаемой для инсталляции сенсорных узлов с использованием БПЛА, была разработана имитационная модель инсталляции сенсорных узлов [9]. На базе модели была проведена серия компьютерных экспериментов, в результате которых было установлено, что при скорости БПЛА приблизительно 10 м/с (36 км/ч) и радиусом действия сенсорного узла 50м БПЛА сможет полностью покрыть область в виде квадрата (500м х 500м) за 5800 сек.

Сравнив полученные результаты с работами [9, 10], а также с характеристиками приведенные в таблице 1, были получены результаты применения БПЛА для решения задачи инсталляции, которые представлены в таблице 2:

ТАБЛИЦА 2. Результаты применения БПЛА

	БПЛА самолетного типа	БПЛА вертолетного типа
Продолжительность полета, мин.	60	30
Скорость горизонтального полета, км/ч	40÷100	20÷60
Минимальная область покрытия (в виде квадрата)	555 м × 555 м	275 м × 275 м
Максимальная область покрытия (в виде квадрата)	880 м × 880 м	480 м × 480 м

Таким образом, в статье были рассмотрены беспилотные летательные аппараты различного типа, которые могут применяться в задачах инсталляции сенсорных узлов для обеспечения максимального покрытия. БПЛА вертолетного типа может инсталлировать сенсорные узлы с высокой точностью, а БПЛА самолетного типа может инсталлировать сенсорные узлы с приблизительной точности так как не способен зависать на месте и постоянно движется вперед. Была разработана имитационная модель инсталляции сенсорных узлов с БПЛА вертолетного типа, а также проанализированы характеристики каждого из типов БПЛА, что позволило установить минимальные и максимальные размеры области покрытия.

Список используемых источников

1. Кучерявый А. Е., Владыко А. Г., Киричек Р. В., Парамонов А. И., Прокопьев А. В., Богданов А. И., Дорг-Гольц А. А. Летающие сенсорные сети // Электросвязь. 2014. № 9. С. 2–5.

2. Haiyang C., Yongcan C., Yangquan C. Autopilots for Small Fixed-Wing Unmanned Air Vehicles: A Survey // Mechatronics and Automation ICMA. Aug. 2007. PP. 3144–3149.

3. Shweta Gupte, Paul I. T. M., James M. C. A Survey of Quad rotor Unmanned Aerial Vehicles // South east con, Proceedings of IEEE. Mar. 2012. PP. 1–6.

4. Фетисов В. С., Неугодникова Л. М., Адамовский В. В., Красноперов Р. А. Беспилотная авиация терминология классификация современное состояние: монография. Уфа: ФОТОН. 2014. 217 с.: ил. ISBN 978-5-9903144-3-6.

5. Boudjit K. and Larbes C. Detection and Implementation Autonomous Target Tracking with a Quadrotor AR. Drone // Informatics in Control, Automation and Robotics (ICINCO). Jul. 2015. Vol. 2. PP. 223–230.

6. Зинченко О. Н. Беспилотные летательные аппараты: применение в целях аэрофотосъемки для картографирования (часть 1) [Электронный ресурс] // Ракурс. 2011. URL: http://www.racurs.ru/?page=681 (дата обращения 03.03.2016).

7. Кучерявый А. Е., Владыко А. Г., Киричек Р. В. Летающие сенсорные сети - новое приложение Интернета Вещей // Актуальные проблемы инфотелекоммуникаций в науке и образовании. IV Международная научно-техническая и научно-методическая конференция: сборник научных статей в 2 томах. СПб. : СПбГУТ, 2015. Т. 1. С. 17–22.

8. Динь Ч. З., Киричек Р. В., Парамонов А. И., Кучерявый А. Е. Методы инсталляции сенсорных узлов с квадрокоптера общего пользования // Информационные технологии и телекоммуникации. 2015. № 4 (12). С. 57–66.

9. Динь Ч. З., Киричек Р. В., Кучерявый А. Е. Обзор методов инсталляции сенсорных узлов с квадрокоптера // Информационные технологии и телекоммуникации. 2015. № 1 (9). С. 50–61.

10. Динь Ч. З., Киричек Р. В., Парамонов А. И., Кучерявый А. Е. Имитационная модель инсталляции сенсоров с квадрокоптера на заданной территории // Информационные технологии и телекоммуникации. 2015. № 2 (10). С. 93–100.

УДК 004.056.5

ПРИМЕНЕНИЕ ТЕХНОЛОГИИ БОЛЬШИХ ДАННЫХ В СИСТЕМАХ УПРАВЛЕНИЯ ИНФОРМАЦИЕЙ И СОБЫТИЯМИ БЕЗОПАСНОСТИ

Н. Д. Дубровин, И. А. Ушаков, А. А. Чечулин

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

В современных условиях постоянного увеличения количества и многообразия данных, поступающих в системы защиты информации, возможностей традиционных систем хранения и обработки все чаще оказывается недостаточно для оперативного анализа и формирования решений. Для решения этой проблемы предлагается применять технологию Больших данных. В статье рассмотрены основные методы и понятия технологии Больших данных, а также архитектура разработанного программного прототипа для проведения экспериментов.

Большие данные, Hadoop, обработка данных, вычислительный кластер, SIEM-система.

В последнее время, в сфере информационных технологий, проявляется значительный интерес к технологиям Big Data (рус. «Большие данные»).

Этот интерес связан с постоянным увеличением количества данных, которые необходимо оперативно обрабатывать. Эта проблема актуальна как для государственных структур, так и для крупных компаний, такие как Google, IBM, Microsoft, Yahoo, Hewlett-Packard, Oracle. Для этих компаний собранная информация является очень важным активом, который может принести прибыль. Однако достаточно быстро обработать такое количество информации и извлечь из нее полезные данные с каждым днем становится труднее и дороже.

Вместе с количеством данных растет также и их многообразие. Крупные предприятия собирают терабайты данных, таких как сетевые события, события программных приложений и действий сотрудников. Например, в компании Hewlett-Packard генерируется около одного триллиона событий в день или примерно 12 миллионов событий в секунду [1]. И эти объемы постоянно растут, поскольку увеличивается количество источников информации, предприятия нанимают новых сотрудников, подключают к сети больше устройств с разнообразным программным обеспечением. В связи с этим, традиционные аналитические методы и системы хранения данных [2] становятся менее эффективными и неспособны оперативно обрабатывать огромные объемы многообразных и неструктурированных данных и сразу получать результаты, пригодные для восприятия человеком, как это можно сделать, применив технологии Больших данных.

Для задачи обеспечения защиты информации характерны те же тенденции. В наши дни для защиты сети передачи данных становится недостаточно таких устройств, как межсетевой экран или система обнаружения вторжений. Для полного контроля, управления и анализа обстановки требуется сочетание различных инструментов и устройств. Но по-настоящему полную картину обо всех событиях, которые происходят в сети, можно получить, собрав и проанализировав одновременно все источники информации. Для этого используют системы управления информацией и событиями безопасности – SIEM *(Security Information and Event Management)* системы [3]. Эти системы осуществляют сбор данных из разных источников, их унификацию, корреляцию и визуализацию результатов анализа. Обычно, подобные системы не предназначены для предотвращения нарушения политики безопасности, их цель оповестить специалиста по информационной безопасности об отклонениях от нормального поведения и возможного нарушения безопасности. Но, в условиях непрерывного роста количества и многообразия данных, такие системы становятся малоэффективными. Поэтому, в настоящее время развивается направление применения технологии Больших данных для обработки событий безопасности в SIEM-системах.

Основные принципы Больших данных

У термина Большие данные нет строгого определения, однако принято считать, что это совокупность технологий, методов и инструментов, с помощью которых можно хранить и обрабатывать структурированные и неструктурированные огромные объемы данных, поступающие непрерывным потоком. Понятие Большие данные основывается на четырех *V*: *Volume* – объем обрабатываемых данных; *Velocity* – скорость обработки; *Variety* – разнообразие форматов данных; *Value* – ценность информации, извлеченной из обработанных данных [1].

Основываясь на данном определении, можно выделить три основных принципа работы с Большими данными:

1. Локальное хранение. Хранить блок данных на том узле, на котором выполняется обработка.

2. Масштабируемость. Возможность беспрепятственно увеличивать количество узлов вычислительного кластера, при увеличении объема обрабатываемых данных.

3. Отказоустойчивость. Система работает устойчиво и без ошибок, даже при выходе из строя одного или нескольких вычислительных узлов кластера.

Hadoop – набор свободно распространяемых программных средств с открытым исходным кодом, предназначенный для разработки и реализации программ, которые запускаются на кластерах из десятков, сотен или тысяч вычислительных узлов [4]. В его состав входят три основных элемента:

1) HDFS *(Hadoop Distributed File System)* – распределенная файловая система [4]. Отвечает за распределенное, по нескольким узлам, хранение данных в вычислительном кластере. HDFS может обеспечить высокую надежность от потери данных, организуя их хранение таким образом, что один и тот же блок может храниться и обрабатываться на нескольких узлах. Узлы в HDFS бывают трех типов:

– NameNode – является мозгом всей системы. Отвечает за обработку таких операций, как действия над каталогами, открытие или закрытие файлов, хранение метаданных файловой системы, а также метаинформацию о расположении блоков данных и узлах DataNode. В одном кластере может быть только один NameNode, поэтому он является единой точкой отказа системы.

– DataNode – является узлом хранения данных. В одном кластере может быть очень большое количество таких узлов. Отвечают за непосредственное хранение блоков файлов, а также выполнение операций чтения и записи файлов и данных.

– SecondaryNameNode – является вспомогательным модулем для NameNode. Предназначен для быстрого восстановления работоспособности NameNode при выходе его из строя или перезагрузки. Для этого он

периодически копирует файлы состояния и последних изменений файловой системы.

2) MapReduce – модель распределенных вычислений, разработанная компанией Google. Вычисления производятся на кластере, состоящем из главного узла *(master node)*, который осуществляет управление ресурсами и распределение задач между рабочими узлами *(worker node)*, которые в свою очередь выполняют поблочную обработку данных. Алгоритм работы модели показан на рисунке 1.

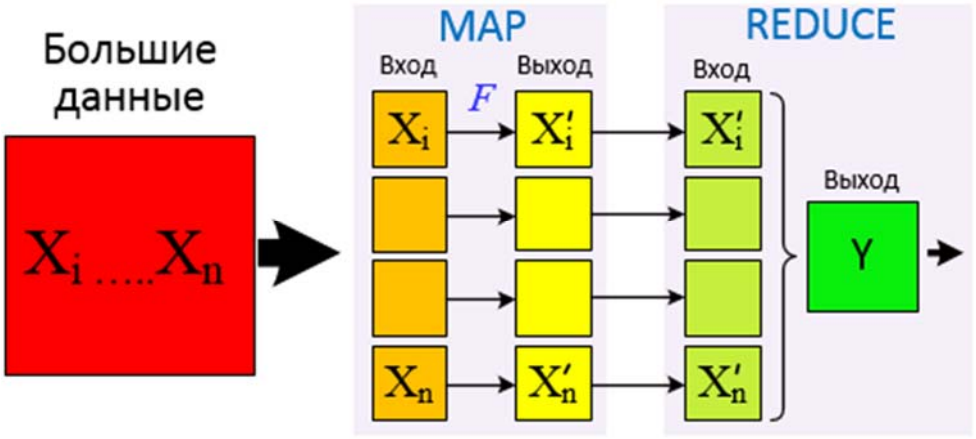


Рис. 1. MapReduce

Алгоритм работы MapReduce состоит из двух основных шагов – Map и Reduce. На первом шаге выполняется предварительная обработка большого объема «сырых» данных разбитого на блоки посредством применения заданной функции *F*. Операции запускаются независимо на каждом рабочем узле и выполняются параллельно. На втором шаге выполняется функция Reduce – объединение результатов предварительной обработки [5].

3) YARN – модуль, управляющий ресурсами кластера [6]. Он состоит из трех основных программ-агентов *(daemons)*:

– ResourceManager – управляет вычислительным кластером. Распределяет физические ресурсы – процессорную мощность и память.

– ApplicationMaster – управляет каждым приложением, запускаемым в YARN. Выполняет мониторинг потребления ресурсов рабочими узлами.

– NodeManager – управляет каждым узлом в кластере.

Архитектура прототипа

Архитектура прототипа представлена на рисунке 2. В ее состав входят вычислительный кластер, состоящий из одного главного и шести рабочих узлов, а также SIEM-система OSSIM. OSSIM *(Open Source Security Information Management)* – это система управления информацией и событиями безопасности с открытым исходным кодом, разрабатываемая компанией AlienVault.

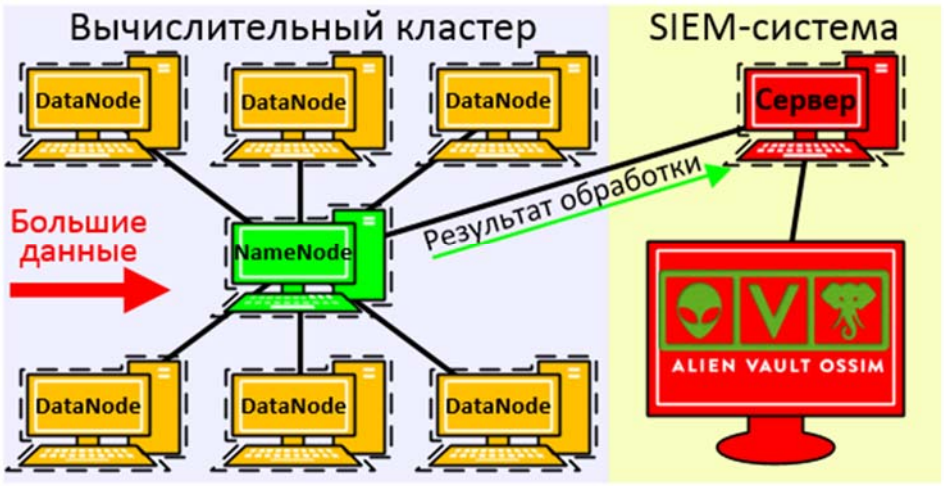


Рис. 2. Схема прототипа

Для обработки Больших данных используется Apache Hadoop версии 2.6.0. Принцип работы прототипа основан на обработке, загружаемых в HDFS, больших объемов данных, которая выполняется рабочими узлами на основе заранее выбранной функции. Главный узел объединяет результаты обработки блоков данных, и в заданном формате передает информацию SIEM-системе, которая анализирует ее, собирая статистику и применяя заданные правила безопасности. После анализа и корреляции, эта информация предоставляется оператору SIEM-системы в виде подробного отчета о событиях безопасности и выводах, полученных на основе их анализа.

Заключение

В данной статье рассмотрены основные принципы технологии Больших данных и пример реализации прототипа для обработки Больших данных для повышения эффективности работы системы управления информацией и событиями безопасности. Для реализации представленного прототипа использовались Apache Hadoop и SIEM-система OSSIM. На текущий момент проект находится на стадии разработки, проводятся тесты производительности вычислительного кластера, написание функций, на основе которых будет выполняться обработка Больших данных, настройка и тестирование работы SIEM-системы с воспроизведением различных сетевых атак и нарушений информационной безопасности.

Представленный прототип может использоваться в компаниях, оперирующих с большим количеством информации, касающихся безопасности.

Список используемых источников

1. Alvaro A. Cárdenas, Pratyusa K. Manadhata, Sree Rajan. Big Data Analytics for Security Intelligence. Cloud Security Alliance, 2013. – URL: https://downloads.cloudsecurityalliance.org/initiatives/bdwg/Big_Data_Analytics_for_Security_Intelligence.pdf (дата обращения 07.03.2016).

2. Полубелова О. В., Котенко И. В., Саенко И. Б., Чечулин А. А. Применение онтологий и логического вывода для управления информацией и событиями безопасности // Системы высокой доступности. 2012. № 2. С. 100–108.

3. Котенко И. В., Саенко И. Б., Полубелова О. В., Чечулин А. А. Применение технологии управления информацией и событиями безопасности для защиты информации в критически важных инфраструктурах // Труды СПИИРАН. 2012. Вып. 1 (20). С. 27–56.

4. Tom White. Hadoop: The Definitive Guide, 2th Edition. O'Reilly Media, Yahoo Press, 2011. – 625 с.

5. Dean J., Ghemawat S. MapReduce: Simplified Data Processing on Large Clusters / OSDI'04: Sixth Symposium on Operating System Design and Implementation, San Francisco, CA, December, 2004. – URL: https://static.googleusercontent.com/media/research.google.com/ru//archive/mapreduce-osdi04.pdf (дата обращения 07.03.2016).

6. M. Tim Jones, Micah Nelson. Moving ahead with Hadoop YARN. IBM developerWorks, 2013. URL: https://www.ibm.com/developerworks /library/bd-hadoopyarn/ (дата обращения 07.03.2016).

УДК 004.7 (004.942)

ПОДХОДЫ К МОДЕЛИРОВАНИЮ СИСТЕМ ЗАКОННОГО ПЕРЕХВАТА ТРАФИКА В SDN

В. С. Елагин

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

В статье исследуются модели и варианты реализации оперативного перехвата трафика в сетях SDN.

моделирование систем массового обслуживания, СОРМ, SDN, сервисная платформа, программно-конфигурируемые сети, пост-NGN.

Моделирование систем законного перехвата трафика – это процесс, который на сегодняшний день исключен из цикла создания и внедрения мероприятий СОРМ на сетях связи.

С учетом исполнения приказа Минкомсвязи России от 16.04.2014 N 83 «Об утверждении Правил применения оборудования систем коммутации, включая программное обеспечение, обеспечивающего выполнение установленных действий при проведении оперативно-розыскных мероприятий. Часть III. Правила применения оборудования коммутации и маршрутизации пакетов информации сетей передачи данных, включая программное обеспечение, обеспечивающего выполнение установленных действий при проведении оперативно-розыскных мероприятий» [1] становятся более осязаемыми черты технической стороны СОРМ. При этом стоит констатировать, что сегодня силами международных организаций в области связи находятся

в разработке, и внедряются огромное число протоколов и технологий, которые, естественно не учтены в приказе.

Одним из наиболее перспективных направлений развития сетей связи является SDN (Программно-конфигурируемые сети), концепция построения которых значительно отличается от традиционных сетей с коммутацией пакетов.

Поэтому важным вопросом на сегодняшний день становится создание опережающего задела в направлении анализа и моделирования систем оперативно-розыскных мероприятий в парадигме SDN. Это позволит создать адекватные модели и сформулировать необходимые требования (технические, организационные и т. д.) к системам законного перехвата, часть из которых уже была рассмотрена в рамках СОРМ в сетях пост-NGN [2], в рамка к моменту их повсеместного развертывания у операторов связи.

Особенности управления передачей трафика в SDN сетях

Существует две независимые модели архитектуры SDN. Одна из них развивается консорциумом ONF, другая – IETF. Кроме этого, некоторые открытые комьюнити пытаются разработать протоколы взаимодействия между NFV и SDN.

Например, группой ETSI NFV ISG представлена модель MANO (*Management And Orchestration*), а консорциумом MEF (*Metro Ethernet Forum*) была разработана концепция LSO (*Lifecycle Service Orchestration*), которая является неким связующим звеном между двумя вышеописанными архитектурами. Наибольшую популярность и экономические показатели имеет модель ONF на базе протокола OpenFlow. Консорциум продвигает трехуровневую модель, состоящую из уровней приложений, управления и инфраструктуры, если подробно рассмотреть информационные потоки в архитектуре SDN (рис. 1), то можно увидеть два направления обмена информацией. Первый поток получил название «северный интерфейс» (*northbound* API), а второй «южный интерфейс» (*southbound* API). В качестве первого выступает протокол на основе REST API (REST – общие принципы организации взаимодействия приложения с сервером, API – application programminginterface, интерфейс программирования приложений, состоящий из набора готовых кодов, предоставляемых приложением для использования во внешних программных продуктах), а в качестве «южного интерфейса» протокол OpenFlow.

Изолирование управления от функций форвардинга данных называется «disaggregation», в связи с этим, каждый из уровней может быть рассмотрен по отдельности, а не в качестве единой интегрированной системы.

Рис. 1. Трехуровневая модель SDN

Подходы к законному перехвату в SDN

Для разбора возможных моделей законного перехвата в SDN стоит рассмотреть принципы установления соединения и организации пользовательских сессий.

Из логики работы SDN известно, что в штатном режиме на контроллер отправляются идентификаторы сеанса связи (в том числе абонента) не выше 4-го уровня модели OSI.

Поэтому можно сделать предварительные выводы о возможности реализации СОРМ в сетях SDN:

1. Поскольку суть концепции программно-конфигурируемых сетей направлена на разделение уровней инфраструктуры и управления, то есть «упрощения» логики работы коммутатора и вынос сложных сетевых функций в обязанности контроллера/оркестратора, то логично будет внедрять функции СОРМ на уровне управления или приложений и реализовать все функции в виде сетевого приложения. Такие выводы напрашиваются исходя еще из одного свойства ПКС-сетей – централизации, которое может позволить системе законного перехвата трафика следить и собирать необходимую информацию в одном узле сети (контроллер/оркестратор) одновременно от нескольких других узлов (OpenFlow-коммутаторы).

2. Приказом Министерства связи и массовых коммуникаций утверждены параметры, согласно которым необходимо осуществлять отбор и передачу поступающих пакетов данных на OpenFlow-коммутаторы. Искать и отправлять пакеты по указанным параметрам на вышележащие уровни в программно-конфигурируемых сетях возможно, используя классификаторы (Match).

Список MatchField в протоколе OpenFlow составляет более 40 значений.

Таким образом, чтобы рассмотреть возможность реализации системы ОРМ как сетевого приложение [3], для начала необходимо провести сравнительный анализ параметров, установленных 83 приказом Министерства связи и массовых коммуникаций, с возможными классификаторами, определенными в потоковых таблицах OpenFlow-коммутаторов.

Эксперимент был направлен на анализ информации передаваемой по протоколу OpenFlow при организации сессий различных протоколов: ICMP, ARP, HTTP.

Схема эксперимента представлена на рисунке 2.

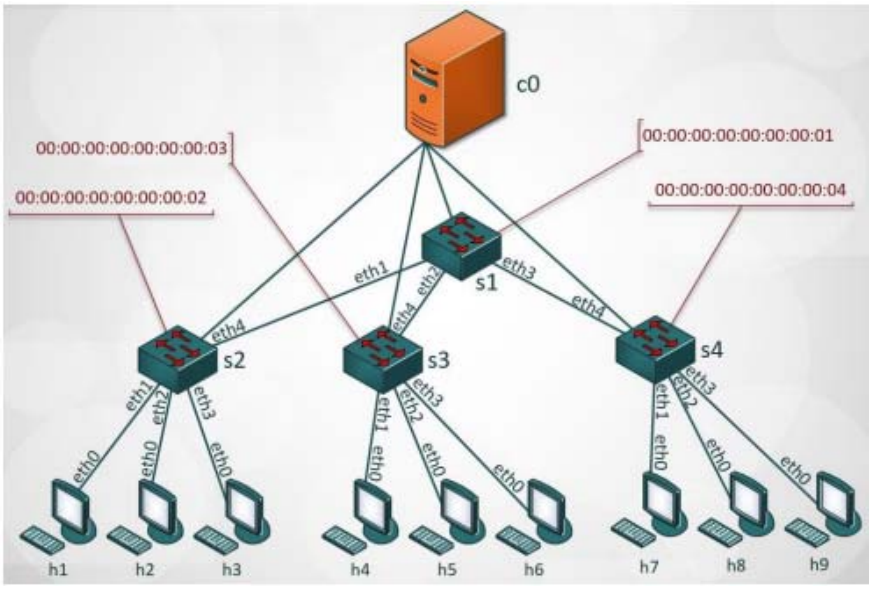


Рис. 2. Схема эксперимента

Принятые условные обозначения:

› h1..h9 – хосты подключенные к OpenFlow-коммутаторам;

› eth0..eth4 – интерфейсы подключения (Ethernet);

› s1..s4 – OpenFlow-коммутаторы;

› c0 – контроллер Floodlight;

› выноски обозначают DPID каждого OpenFlow-коммутатора.

Напомним, что в рамках эксперимента необходимо показать какую информацию получает контроллер о потоках в OpenFlow-коммутаторах и достаточно ли этой информации для интеграции системы ОРМ в уровень управления SDN сети, а именно в контроллер/оркестратор. Ход работы эксперимента был разбит на несколько этапов в зависимости от используемых протоколов для передачи трафика в виртуальной сети SDN между OpenFlow-коммутаторами:

Первый этап

На данном этапе в качестве трафика, генерируемого хостами, использовались сообщения проверки возможности доступа (*Echo Request и Echo Reply*), генерируемые утилитой ping по протоколу ICMP.

Второй этап

На втором этапе в качестве трафика, генерируемого хостами, использовались сообщения протокола ARP (*Address Resolution Protocol* – протокол определения адреса).

Третий этап

По результатам предыдущих этапов эксперимента видно, что протокол OpenFlow позволяет переносить данные протоколов до транспортного уровня модели OSI, но параметры контроля, установленные приказом Министерства связи и массовых коммуникаций, содержат данные (напр. электронные почтовые адреса), которые переносятся пакетами более высокоуровневых протоколов, выше, чем транспортный уровень модели OSI.

По результатам всех трех экспериментов подтвердились предположения о передаче на контроллер, только данных из заголовков 1–4 уровня модели OSI, что не устраивает требованиям 83 Приказа Минкомсвязи.

Перспективные подходы к СОРМ в SDN

Теоретические выводы и эксперимент показал, невозможность использования существующих технических средств концепции SDN на уровне управления сетью для проведения СОРМ.

Поэтому важным вопросом становится предложение моделей реализации СОРМ в сетях SDN. На сегодняшний день свои очертания приобретают две модели реализации:

1. «Пассивный» съем трафика на уровне коммутаторов SDN с последующим анализом на отдельных серверах.

2. Специальное приложение «LIaaS», которое позволит анализировать доступные на уровне контроллера данные (тип протокола, MAC адреса, IP адреса и т. д.), и на основании специализированных алгоритмов запрашивать Действие (Action) на передачу инкапсулированных пакетов целиком.

Оба варианта реализации имеют свои преимущества и недостатки, однако, об их окончательной реализации пока говорить рано, ввиду продолжающегося становления и развития самой концепции SDN.

Однако темпы развития этой концепции достаточно высоки, чтобы предположить их практическое внедрение в ближайшее время, поэтому вопрос организации СОРМ на этих сетях является своевременным и важным вопросом.

Список используемых источников

1. Приказ Минкомсвязи РФ от 16 апреля 2014 года № 83 «Об утверждении Правил применения оборудования систем коммутации, включая программное обеспечение, обеспечивающего выполнение установленных действий при проведении оперативно-розыскных мероприятий. Часть III. Правила применения оборудования коммутации и маршрутизации пакетов информации сетей передачи данных, включая программное

обеспечение, обеспечивающего выполнение установленных действий при проведении оперативно-розыскных мероприятий» // Рос. газ. 2014. – 18 июля.

2. Гольдштейн Б. С., Крюков Ю. А., Хегай И. П., Шляпоберский В. Э. Интерфейсы СОРМ. Справочник по телекоммуникационным протоколам. СПб. : BHV, 2006 – 157 с.

3. Гольдштейн Б. С., Елагин В. С., Крюков Ю. А., Семенов Ю. Н. Новая парадигма законного перехвата сообщений в NGN/IMS // Вестник связи. 2010. № 4. С. 38–46.

УДК 681.3.81

ТЕХНИКИ СОЦИАЛЬНОЙ ИНЖЕНЕРИИ В ИНФОРМАЦИОННЫХ СРЕДАХ И МЕТОДЫ ЗАЩИТЫ ОТ НИХ

К. Э. Есалов, М. Е. Павленко

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

Обеспечение безопасности названо первой из пяти главных проблем Интернета. В данный момент информационные сети представляют собой эффективную, но полную угроз и опасностей, среду. И не смотря на многообразие различных средств защиты, существуют угрозы, от которых не просто защититься программными или аппаратными средствами. Одной из таких угроз является социальная инженерия. Данный доклад посвящён рассмотрению технологии применения социальной инженерии в компьютерных сетях связи. В нём проанализированы различные виды атак, связанных с использованием социальной инженерии и описаны существующие и возможные методы их предотвращения.

информационная безопасность, социальная инженерия, предотвращение угроз, сетевая атака, фишинг.

Как показывает мировая практика успешно проведенных взломов, большая часть проблем связана именно с проблемами с людьми. Дело в том, что при определенных условиях и при правильном подходе злоумышленника люди способны выдать любую информацию.

Социальная инженерия – это метод несанкционированного доступа к информации или системам хранения информации с использованием слабостей человеческого фактора. Основной целью социальных инженеров, как и других хакеров и взломщиков, является получение доступа к защищенным системам с целью кражи информации, паролей, данных о кредитных картах и т. п. Основным отличием от простого взлома является то, что в данном случае в роли объекта атаки выбирается не машина, а ее оператор. Именно поэтому все методы и техники социальных инженеров основываются на использовании слабостей человеческого фактора, что считается крайне разрушительным, так как злоумышленник получает информацию,

например, с помощью обычного телефонного разговора или электронной переписки с сотрудниками, выдавая себя за начальника или другого служащего. Для защиты от атак данного вида следует знать о наиболее распространенных видах мошенничества, понимать, что на самом деле хотят взломщики и своевременно организовывать подходящую политику безопасности [1].

Существует несколько распространенных техник и видов атак, которыми пользуются социальные инженеры. Все эти техники основаны на особенностях принятия людьми решений, известных как когнитивные предубеждения. Эти предрассудки используются в различных комбинациях, с целью создания наиболее подходящей стратегии обмана в каждом конкретном случае. Но общей чертой всех этих методов является введение в заблуждение, с целью заставить человека совершить какое-либо действие, которое не выгодно ему и необходимо социальному инженеру. Для достижения поставленного результата, злоумышленник использует целый ряд всевозможных тактик.

Сегодня одним из самых распространенных методов получения конфиденциальной информации является фишинг (термин образован от игры слов *password harvesting fishing* – «ловля паролей»). Фишинг можно охарактеризовать как тип интернет-мошенничества, который использует принципы социальной инженерии с целью получения доступа к конфиденциальным данным пользователя – логинам, паролям, номерам банковских карт и т. д. Наиболее ярким примером фишинговой атаки может служить сообщение, отправленное жертве по электронной почте, и подделанное под официальное письмо – от банка или платёжной системы – требующее проверки определённой информации или совершения определённых действий. Причины могут называться самые различные. Это может быть утеря данных, поломка в системе и прочее. Такие письма обычно содержат ссылку на фальшивую веб-страницу, в точности похожую на официальную, и содержащую форму, требующую ввести конфиденциальную информацию.

Практически каждый день появляются новые схемы мошенничества. Большинство людей может самостоятельно научиться распознавать мошеннические сообщения, познакомившись с их некоторыми отличительными признаками. Чаще всего фишинговые сообщения содержат:

– сведения, вызывающие беспокойство, или угрозы, например, закрытия пользовательских банковских счетов;

– обещания огромного денежного приза с минимальными усилиями или вовсе без них;

– запросы о добровольных пожертвованиях от лица благотворительных организаций;

– грамматические, пунктуационные и орфографические ошибки.

Телефонный фишинг – Вишинг (англ. *vishing – voice fishing*) назван так по аналогии с фишингом. Данная техника основана на использовании системы предварительно записанных голосовых сообщений, с целью воссоздать «официальные звонки» банковских и других IVR систем. Обычно, жертва получает запрос (чаще всего через фишинг электронной почты) связаться с банком и подтвердить или обновить какую-либо информацию. Система требует аутентификации пользователя, посредством ввода PIN-кода или пароля. Поэтому, предварительно записав ключевую фразу, можно выведать всю нужную информацию.

Квид про кво (от лат. *Quid pro quo* – «то за это») – в английском языке это выражение обычно используется в значении «услуга за услугу». Данный вид атаки подразумевает обращение злоумышленника в компанию по корпоративному телефону или электронной почте. Зачастую злоумышленник представляется сотрудником технической поддержки, который сообщает о возникновении технических проблем на рабочем месте сотрудника и предлагает помощь в их устранении. В процессе «решения» технических проблем, злоумышленник вынуждает цель атаки совершать действия, позволяющие атакующему запускать команды или устанавливать различное программное обеспечение на компьютере «жертвы».

Троянская программа – это вредоносная программа, используемая злоумышленником для сбора, разрушения или модификации информации, нарушения работоспособности компьютера или использования ресурсов пользователя в своих целях. Чаще всего злоумышленник отправляет жертве электронное сообщение, содержащее «интересный» контент, обновление антивируса, или другую информацию, способную заинтересовать пользователя. Открывая прикрепленный к письму файл, пользователь устанавливает себе на компьютер вредоносное программное обеспечение, позволяющее мошеннику получить доступ к конфиденциальной информации.

Сбор информации из открытых источников. Применение техник социальной инженерии требует не только знания психологии, но и умения собирать о человеке необходимую информацию. Относительно новым способом получения такой информации стал её сбор из открытых источников, главным образом из социальных сетей. К примеру, такие сайты как livejournal, «Одноклассники», «ВКонтакте», содержат огромное количество данных, которые люди и не пытаются скрыть. Как правило, пользователи не уделяют должного внимания вопросам безопасности, оставляя в свободном доступе данные и сведения, которые могут быть использованы злоумышленником.

«Дорожное яблоко». Этот метод атаки представляет собой адаптацию троянского коня, и состоит в использовании физических носителей. Злоумышленник подбрасывает «инфицированные» носители информации в местах общего доступа, где эти носители могут быть легко найдены, такими как туалеты, парковки, столовые, или на рабочем месте атакуемого сотрудника.

Обратная социальная инженерия. Об обратной социальной инженерии упоминают тогда, когда жертва сама предлагает злоумышленнику нужную ему информацию. Это может показаться абсурдным, но на самом деле лица, обладающие авторитетом в технической или социальной сфере, часто получают идентификаторы и пароли пользователей и другую важную личную информацию просто потому, что никто не сомневается в их порядочности. Например, сотрудники службы поддержки никогда не спрашивают у пользователей идентификатор или пароль; им не нужна эта информация для решения проблем. Однако, многие пользователи ради скорейшего устранения проблем добровольно сообщают эти конфиденциальные сведения. Получается, что злоумышленнику даже не нужно спрашивать об этом.

Методы защиты от социальной инженерии

Для защиты от социальной инженерии можно применять как *технические*, так и *антропогенные* средства.

Простейшими методами *антропогенной* защиты можно назвать:

1) Привлечение внимания людей к вопросам безопасности.

2) Осознание пользователями всей серьезности проблемы и принятие политики безопасности системы.

3) Изучение и внедрение необходимых методов и действий для повышения защиты информационного обеспечения.

Поскольку информационная безопасность – непрерывный процесс, то для обеспечения максимальной защиты фирмы базируется на обученности и ответственности персонала.

К *технической* защите можно отнести средства, мешающие заполучить информацию и средства, мешающие воспользоваться полученной информацией.

Для защиты от спама и других атак, связанных с рассылкой по электронной почте можно использовать эти средства как вместе, так и по отдельности. Помешать злоумышленнику получить запрашиваемую информацию можно, анализируя как текст входящих писем (предположительно, злоумышленника), так и исходящих (предположительно, цели атаки) по ключевым словам. К недостаткам данного метода можно отнести очень большую нагрузку на сервер и невозможность предусмотреть все варианты написания слов. К примеру, если взломщику становится известно, что программа реагирует на слово «пароль» и слово «указать», злоумышленник может заменить их на «пассворд» и, соответственно, «ввести». Так же стоит принимать во внимание возможность написания слов с заменой кириллических букв латиницей для совпадающих символов.

Средства, мешающие воспользоваться полученной информацией, можно разделить на те, которые полностью блокируют использование дан-

ных, где бы то ни было, кроме рабочего места пользователя (привязка аутентификационных данных к серийным номерам и электронным подписям комплектующих компьютера, IP и физическому адресам), так и те, которые делают невозможным (или труднореализуемым) автоматическое использование полученных ресурсов (например, авторизация по системе *Captcha*, когда в качестве пароля нужно выбрать указанное ранее изображение или часть изображения, но в сильно искаженном виде). Как в первом, так и во втором случае известный баланс между ценностью требуемой информации и работой, требуемой для ее получения, смещается, вообще говоря, в сторону работы, так как частично или полностью блокируется возможность автоматизации. Таким образом, даже имея все данные, выданные ничего не подозревающим пользователем, например, с целью массово разослать рекламное сообщение (спам), злоумышленнику придется на этапе каждой итерации самостоятельно вводить полученные реквизиты.

Так же к средствам, мешающим воспользоваться полученной информацией, относится система защиты от самой распространенной техники социальной инженерии – фишинга. Защита от фишинга давно существует и используется в новых версиях веб-браузеров и антивирусов. В качестве защиты используется фишинговый фильтр или так называемая система антифишинга. Идея защиты от фишинга заключается в том, что система должна перед загрузкой данных по определенному URL вначале проверить его репутацию в базе данных. Для этого традиционно используется очень компактный запрос к базе, содержащей URL ресурса, на который пользователь собирается попасть. А в ответ система сообщает уровень опасности запрашиваемого URL. Такие базы данных регулярно пополняются данными о новых фишинговых сайтах и помогают защититься от масштабных атак, но защитить пользователя от индивидуальной атаки такая система не способна.

В ближайшее время планируется разработать модуль защиты от фишинга и других веб-атак для стенда по изучению сетевой безопасности Nester. Этот модуль будет представлять из себя Web Application Firewall с базой данных для антифишингового фильтра. Такой модуль поможет хорошо изучить веб-безопасность и ознакомиться с существующими методами защиты для веб-приложений.

Из рассмотренных выше техник социальной инженерии видно, что далеко не от всех видов атак есть возможность защититься техническими средствами. От некоторых техник может защитить только осведомленность атакуемого, например, от телефонного фишинга или обратной социальной инженерии. А существующие технические средства защищают в основном от массовых атак, поэтому любой пользователь или определенная группа пользователей может быть подвергнута специально подготовленной индивидуальной атаке, обходящей существующие методы защиты. Именно поэтому в будущем планируется создание системы, которая включала бы

в себя как технические, так и антропогенные средства защиты. Такой системы, которая бы не только останавливала уже выявленные и занесённые в базу атаки, но и предупреждала пользователя об опасности при переходе на незнакомую страницу, похожую по определённым критериям на опасную. Так же в связи с развитием систем DPI возможно будут созданы системы, основанные на анализе поведения пользователей в сети. Такие системы будут блокировать пользователей в случае отклонения от «привычного» поведения.

Список используемых источников

1. Кузнецов М. В., Симдянов И. В. Социальная инженерия и социальные хакеры. СПб. : БХВ-Петербург, 2007. 358 с.: ил. – ISBN 5-94157-929-2.

УДК 004.056

СРАВНЕНИЕ НОВОГО РОССИЙСКОГО СТАНДАРТА ШИФРОВАНИЯ С РАНЕЕ ИЗВЕСТНЫМИ АЛГОРИТМАМИ БЛОКОВОГО ШИФРОВАНИЯ И ОЦЕНКА ВОЗМОЖНОСТИ ЕГО ВЗЛОМА ПО ЦЕПЯМ ЭЛЕКТРОПИТАНИЯ

К. Н. Жернова, В. И. Коржик

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

Рассматриваются алгоритмы шифрования и дешифрования нового российского стандарта ГОСТ Р 34.12-2015. Производится сравнение данного шифра с известными ранее блоковыми шифрами DES, AES, ГОСТ-28147-89 как по внешним параметрам, так и по стойкости. Делается вывод, что, хотя новый стандарт не в точности соответствует оптимальным методам построения блоковых шифров, он значительно ближе к ним, чем ранее известные шифры. В качестве недостатка отмечается слабая стойкость аппаратной реализации нового стандарта к атаке по цепям электропитания.

блоковый шифр, линейное и нелинейное преобразование, алгоритм ГОСТ Р 34.12-2015, атака на блоковые шифры, атака по цепям электропитания, побочная атака.

Настоящий стандарт содержит описание алгоритмов блочного шифрования и дешифрования и предложен для замены стандарта ГОСТ-28147-89. Необходимость разработки нового стандарта вызвана потребностью в создании блочных шифров с различными длинами блока, соответствующих современным требованиям к криптографической стойкости и эксплуатационным свойствам.

Стандартом определены два алгоритма шифрования для блоков длиной 64 бита и 128 битов. Алгоритм шифрования длиной 64 бита подобен алгоритму шифрования согласно ГОСТ-28147-89, который был рассмотрен ранее, но содержит точные задания всех параметров алгоритма [1].

Схема одного раунда шифрования (рис. 1) реализуется при помощи следующих шагов:

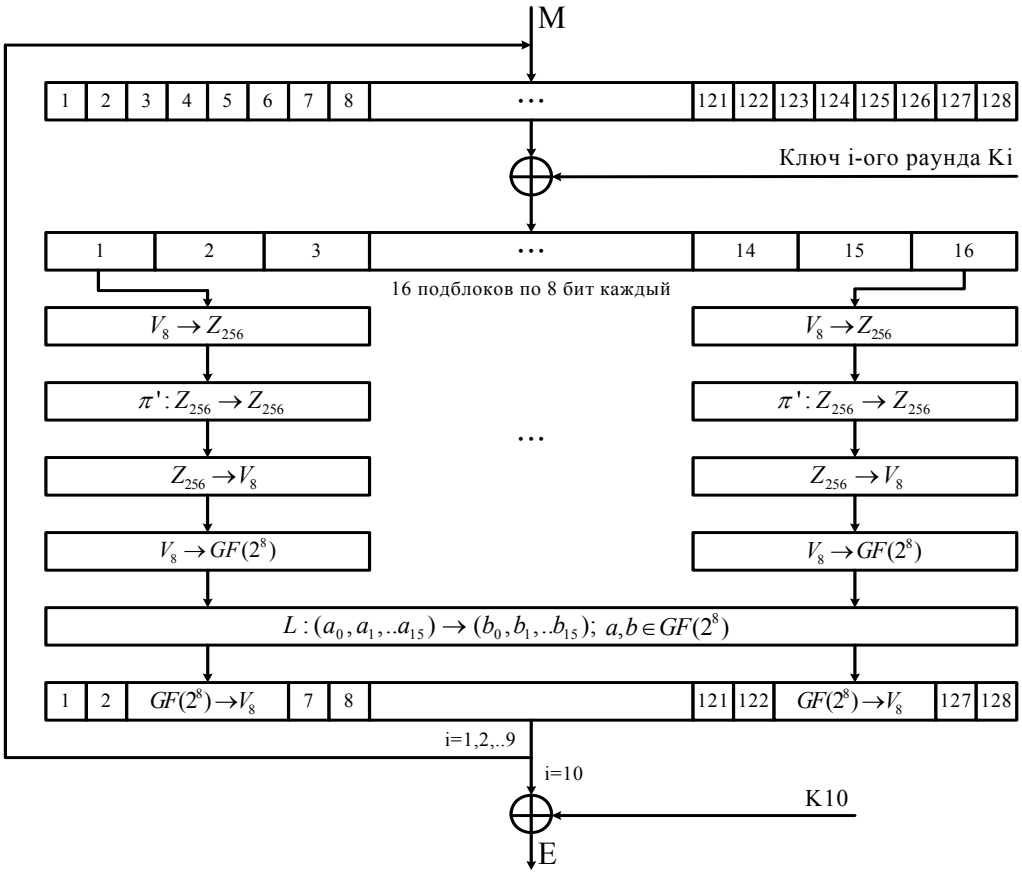


Рис. 1. Схема одного раунда алгоритма шифрования ГОСТ Р 34.12-2015

1. 128 бит информации M складываются по mod2 со 128 битами раундового ключа K_i, $i = 1, 2 .. 9$.

2. Получившийся блок из 128 бит разбивается на 16 подблоков по 8 бит каждый.

3. Над каждым подблоком производится нелинейное преобразование в соответствии с заранее известной таблицей.

4. 16 подблоков объединяются в один блок, состоящий из шестнадцати 8-битных подблоков. Над ним производится линейное преобразование L, которое будет описано позднее.

5. Блок, состоящий из шестнадцати элементов конечного поля $GF(2^8)$, преобразуется в двоичную последовательность и отправляется в начало алгоритма для всех раундов, кроме $i = 10$.

6. Для 10-го раунда на выход поступает блок, полученный в пункте 5 после выполнения 9-го раунда, который складывается по mod2 с 10-ым раундовым ключом и образует криптограмму *E* для исходного сообщения *M*.

Алгоритм выработки раундовых ключей описывается одной формулой:

$$(K_{2i}+1, K_{2i}+2) = F[C_{8(i-1)+8}]\cdots F\left[C_{8(i-1)+1}\right](K_{2i-1}, K_{2i}),$$

где K_i – раундовый ключ, C_j – раундовая константа, $i = 1, \ldots 4, j = 1, \ldots 32$. $F[C](.\,,.)$ означает один цикл схемы Фейстеля, а именно:

$$F[C](a_1, a_0) = (LSX[C](a_1) \oplus a_0, a_1),$$

где *LSX* – полный цикл преобразований алгоритма шифрования ГОСТ Р 34.12-2015, a_0, a_1 – две половины ключа для выполнения схемы Фейстеля.

Сравнение основных параметров и особенностей алгоритмов (табл. 1 и табл. 2) показало, что новый ГОСТ более всего похож на AES, но в качестве нелинейного преобразования в новом ГОСТ используется таблица.

ТАБЛИЦА 1. Сравнение основных параметров некоторых алгоритмов шифрования

Параметр	ГОСТ-28147-89	DES	AES	ГОСТ Р-34-2015
Длина базового ключа, бит	256	56	128/192/256	256
Длина шифрующих блоков, бит	64	64	128	128
Количество раундов	32	16	14	10
Длина раундовых ключей, бит	64	56	128	128

Данные расчёты показывают, что вычисление нелинейного преобразования при помощи обратного элемента в конечном поле в новом ГОСТ не используется.

Действительно, пусть

$$S(x) = Ax^{-1} \oplus b.$$

Выберем элементы x_1 и x_2, принадлежащие полю $GF(2^8)$, $x_1 \neq x_2$; $x_1, x_2 \neq 0$. Пусть x_1=10 и x_2=30. В двоичном представлении x_1=00001010, x_2=00011110.

Обратными элементами к ним в поле $GF(2^8)$, построенном на неприводимом полиноме $x^8+x^6+x^3+x+1$, будут: x_1^{-1}=00100001, x_2^{-1}=00011111.

Согласно таблице, используемой при нелинейном преобразовании в новом ГОСТ, $S(x_1) = S(10) = 250$, $S(x_2) = S(30) = 95$. При переводе обоих чисел в двоичный вектор V_8 получаем 250→11111010, 95→01011111. Тогда вычислим $Ax^{-1} \oplus b$: $Ax_1^{-1} \oplus b$ = 00001001 ≠ $S(x_1)$, $Ax_2^{-1} \oplus b$ = 10000011 ≠ $S(x_2)$.

ТАБЛИЦА 2. Сравнение особенностей алгоритмов

Особенность	ГОСТ-28147-89	DES	AES	ГОСТ Р-34-2015
Использование схемы Фейстеля	Есть	Есть	Нет	Нет
Нелинейное преобразование	Одна неизвестная таблица, 8 *S*-блоков	8 различных *S*-блоков, заданных разными таблицами	Обращение элементов в конечном поле $GF(2^8)$	Известная таблица, 16 *S*-блоков
Линейное преобразование	Циклическая перестановка и чередование блоков в схеме Фейстеля	Перестановки бит в промежуточных блоках раундов	Циклический сдвиг и «перемешивание столбцов»	Близко к укороченному РС-коду
Выработка раундовых ключей	Разделение базового ключа и использование ключей, взятых в обратном порядке	Используются только линейные преобразования	Циклические сдвиги и расширения	Используются как линейные, так и нелинейные преобразования

Их сумма может быть представлена следующей формулой:

$$S(x_1) \oplus S(x_2) = A(x_1^{-1} + x_2^{-1}),$$

что также не совпадает с расчётами, где $S(x_1) \oplus S(x_2) = 10100101$, а $A(x_1^{-1} + x_2^{-1}) = 01111100$.

Линейное преобразование в ГОСТ Р 34.12-2015 (рис. 2) не является кодом Рида-Соломона, но в то же время оно более близко к оптимальному, чем в ранее известных стандартах. Так, в AES линейное преобразование не соответствует оптимальному.

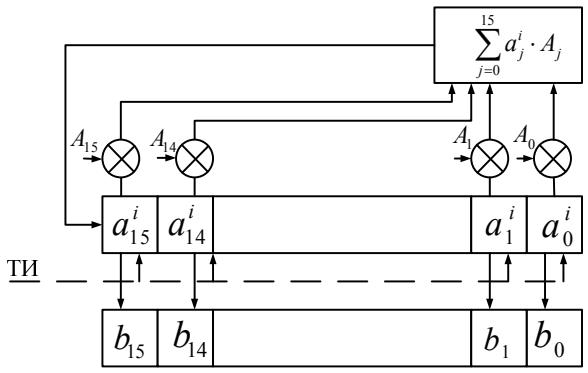


Рис. 2. Схема линейного преобразования в алгоритме шифрования ГОСТ Р 34.12-2015

В сравнении с AES, линейное преобразование нового ГОСТ ближе к порождающей матрице укороченного кода Рида-Соломона. Однако, для

того, чтобы преобразование было оптимальным, нужно сделать следующие преобразования:

1) найти порождающий многочлен полного РС-кода с параметрами (255, 239) над полем $GF(2^8)$ по следующей формуле:

$$g(x) = (x-\propto)(x-\propto^2)\cdots(x-\propto^{15});$$

2) рассчитать порождающий многочлен полного РС-кода:

$$h(x) = \frac{(x^{255}+1)}{g(x)};$$

3) построить схему, показанную на рисунке ниже (рис. 3), где $k = 239$;

4) ввести информацию из 223 нулей и 16 проверочных символов в блоки памяти;

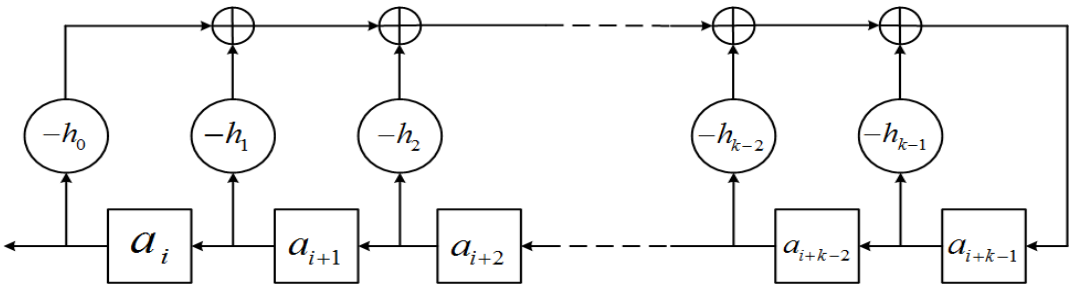


Рис. 3. Генератор циклического кода, реализованный на регистре сдвига

5) выполнить 255 сдвигов и получить последние 16 символов, которые и используются как результат оптимального линейного преобразования [2]. Это, конечно, не совсем не схема, которая представлена в ГОСТ Р 34.12-2015.

Алгоритмы современных блочных шифров, в том числе старый и новый ГОСТ, на сегодняшний день лишены математических уязвимостей. Однако при аппаратной реализации криптографические операции выполняются при помощи интегральных схем.

Физические параметры этих устройств, снимаемые в процессе шифрования, в частности энергопотребление, выдают дополнительную информацию о шифре (так называемую утечку), которая может быть использована для извлечения секретного ключа шифра.

Данный класс атак называют побочными атаками по цепям питания. Наиболее известная из них – это разностный анализ мощности (DPA).

Атака DPA основывается на той гипотезе, что энергопотребление чипа зависит от обрабатываемых им данных. Другими словами, на обработку 1 чипу требуется больше энергии, чем на обработку 0. Подключив осциллограф к цепи питания чипа и сняв потребляемую им мощность при шифровании нескольких сотен сообщений, можно определить секретный ключ используемого шифра [3].

При помощи DPA за последние 15 лет было взломано множество существующих аппаратных реализаций шифров, в том числе DES и AES. Предварительный анализ шифра ГОСТ Р 34.12-2015 показал, что реализация DPA в отношении него не сложнее, чем в отношении шифров DES или ГОСТ-28147-89.

В заключение можно заметить, что ГОСТ Р 34.12-2015 больше всего похож на AES, но линейное преобразование в AES далеко от оптимального. В новом ГОСТ линейное преобразование близко к оптимальному, но не является PC-кодом по неизвестным нам причинам.

Список используемых источников

1. Коржик В. И., Просихин В.П., Яковлев В.А. Основы криптографии: учебное пособие. СПб. : СПбГУТ, 2014. 276 с. ISBN 978-5-89160-097-3.

2. Питерсон У., Уэлдон Э. Коды, исправляющие ошибки. М. : Мир, 1976. 593 с.

3. Коржик В. И., Тихонов С. В. О возможности взлома аппаратной реализации шифра ГОСТ // Проблемы информационной безопасности. Компьютерные системы. 2012. N 3. С. 53–62.

УДК 004.725.7

КОНЦЕНТРАТОР УСТРОЙСТВ ИНТЕНЕТА ВЕЩЕЙ

М. В. Захаров, Р. В. Киричек

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

В связи с тем, что концепция Интернета Вещей получила повсеместное распространение, в ближайшее время стоит ожидать лавинообразного роста устройств, подключённых к сети Интернет, как в промышленном, так и в квартирном секторе. Для обеспечения удобного взаимодействия пользователей с оборудованием различных производителей требуется реализовать возможность централизованного управления Интернет Вещами в рамках одного предприятия, офиса, квартиры и т. д. Решением этой задачи является разработка и создание концентратора устройств Интернет Вещей.

Интернет Вещей, концентратор, беспроводной доступ.

Интернет Вещей, признанный в настоящее время мировым научным сообществом как новая парадигма развития отрасли телекоммуникаций, стал предвестником [1, 2], и, впоследствии, одним из столпов новой научно-технической революции. Робототехника и киберфизические системы, несущие в себе зачатки, или даже полнофункциональный искусственный интел-

лект с помощью технологий и устройств Интернета Вещей смогут самостоятельно исследовать окружающий мир, взаимодействовать с его объектами, чем выведут человечество на принципиально новый уровень развития.

Важной особенностью Интернета Вещей является лёгкость для проникновения в эту концепцию новых идей. Новая область знаний захватила умы не только большинства сотрудников научно-исследовательских отделов крупных производственных компаний, но и огромное число свободных исследователей и разработчиков. Разнообразие подходов к реализации новой концепции придаёт Интернету Вещей небывалую гибкость, однако, возникают и проблемы, связанные с отсутствием стандартов и единообразного подхода при разработке новых устройств. Постоянно ширится число технологий беспроводного доступа, которые предполагается использовать при реализации концепции Интернете Вещей. Это не только новые версии хорошо известных ранее протоколов WiFi и Bluetooth, но и совершенно новые протоколы – ZigBee и т. д. Их главная задача – обеспечивать взаимодействие различных Интернет Вещей между собой и с человеком [3, 4].

В условиях научно-исследовательской лаборатории, опытно-конструкторского отдела предприятия, оснащённых по последнему слову техники, обычно не возникает проблем, связанных с сопряжением оборудования, использующего различные технологии доступа. Свободные разработчики имеют меньшую по объёму материально-техническую базу, но этот недостаток легко компенсируется выбором одной из существующих технологий доступа как приоритетной для исследователей. Однако при дальнейшем распространении устройств Интернета Вещей и выходе их на широкий потребительский рынок могут возникнуть ситуации, когда в квартире простого обывателя, офисном здании или производственном цеху промышленного предприятия окажется множество различных умных устройств широкого круга производителей, снабжённых разнообразными модулями беспроводного доступа, взаимодействовать с которыми по отдельности будет просто неудобно. Одно из возможных решений – создание концентратора устройств Интернета Вещей (рис. 1).

При создании такого устройства потребуется решить несколько задач. Первая задача связана с обеспечением безопасности концентратора устройств Интернета Вещей, с сохранением возможности удалённого мониторинга состояния тех или иных показателей, контролируемых датчиками и умными устройствами [5, 6]. Концентратор является уязвимым местом сети, т. к. он контролирует работу всех узлов и обеспечивает взаимодействие с пользователем. Вторая задача – разработка удобного Web-интерфейса, который позволил бы пользователю управлять своими Интернет Вещами с помощью смартфона, ноутбука, планшета и т. д. Разработчикам следует приложить все усилия, чтобы упростить процесс добавления новых устройств, сделать интуитивно понятный интерфейс. Третья задача – агре-

гировать в концентраторе как можно больше интерфейсов, обеспечивающих подключение умных устройств по различным технологиям беспроводного доступа. Стоит учесть, что в настоящее время эти технологии развиваются довольно динамично, появляется всё больше протоколов [7]. Исходя из этого, концентратор устройств Интернета Вещей должен будет иметь модульную структуру (рис. 2), позволяющую конечному пользователю по мере необходимости приобретать дополнительные модули и самостоятельно устанавливать их в концентратор. Такой подход не только позволит в значительной степени увеличить гибкость устройства, максимально точно подстраивая его под предпочтения владельца, но и сохранять актуальность его использования на протяжении всего срока службы.

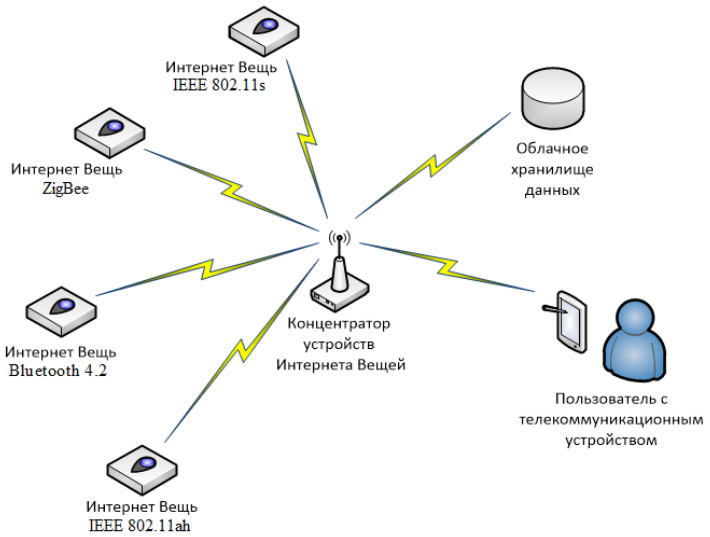


Рис. 1. Концентратор устройств Интернета Вещей.

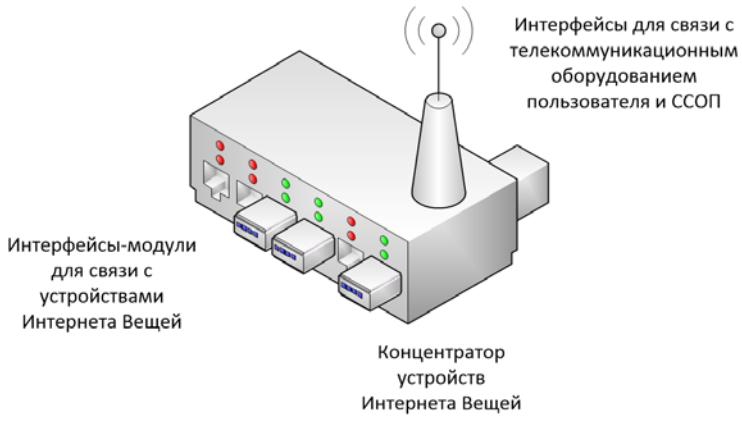


Рис. 2. Модульная структура концентратора устройств Интернета Вещей

В ближайшее время согласно прогнозам крупнейших лидеров рынка телекоммуникационного оборудования, произойдёт повсеместное распространение персональных и промышленных устройств Интернета Вещей.

Создание концентратора для объединения устройств Интернета Вещей позволит легко управлять подобными устройствами, а также кардинально пересмотреть концепцию персональных (PAN) и локальных (LAN) сетей, качественно повысить уровень жизни человека, в значительной степени расширить спектр предоставляемых пользователю услуг. Подобное устройство найдёт широкое применение, как в народно-хозяйственном, так и в квартирном секторе.

Список используемых источников

1. Гольдштейн Б. С., Кучерявый А. Е. Сети связи пост-NGN. СПб. : БХВ-Петербург, 2013. 160 с.: ил. ISBN 978-5-9775-0900-8.

2. Кучерявый А. Е., Прокопьев А. Е., Кучерявый Е. А. Самоорганизующиеся сети. СПб. : Любавич, 2011. 311 с. ISBN

3. Кучерявый А. Е., Кучерявый Е. А. От e-России к u-России: тенденции развития электросвязи // Электросвязь. 2005. № 5. С. 10–11.

4. Киричек Р. В., Кучерявый А. Е., Парамонов А. И., Прокопьев А. В. Эволюция исследований в области беспроводных сенсорных сетей // Информационные технологии и телекоммуникации. 2014. № 4. С. 29–41.

5. Kirichek R., Vladyko A., Zakharov M., Koucheryavy A. Model networks for Internet of Things and SDN // 18th International Conference on Advanced Communication Technology (ICACT) 2016. С. 76–79.

6. Киричек Р. В., Владыко А. Г., Захаров М. В., Кучерявый А. Е. Модельные сети для Интернета Вещей и Программируемых Сетей // Информационные технологии и телекоммуникации. 2015. № 3 (11). С. 17–26.

7. Kirichek R., Koucheryavy A. Internet of Things laboratory test bed // Lecture Notes in Electrical Engineering. 2016. Т. 348. PP. 485–494.

УДК621.391.1

ИССЛЕДОВАНИЕ ВОПРОСОВ ОЦЕНКИ ПРОПУСКНОЙ СПОСОБНОСТИ ТРАНСПОРТНОЙ СЕТИ СВЯЗИ СПЕЦИАЛЬНОГО НАЗНАЧЕНИЯ

В. Г. Иванов, Р. Н. Панков, А. В. Удальцов

Военная академия связи им. Маршала Советского Союза С. М. Буденного

В статье рассматриваются вопросы оценки пропускной способности транспортной сети связи специального назначения, при этом подробно описаны основные свойства и требования к транспортным сетям различного назначения.

транспортная сеть, пропускная способность, сети связи специального назначения.

В настоящее время понятие «транспортная сеть» достаточно широко применяется в сетях связи различного назначения, и в первую очередь, для определения функций сети – переноса (транспортирования) и распределения потоков разнородного трафика между различными сетями доступа.

В соответствии с рекомендациями G.803 международного союза электросвязи (МСЭ-Т) (ранее МККТТ) понятие «транспортирование» определяется как функциональный процесс переноса информации между разнесенными пунктами, а понятие «передача» – как физический процесс распространения информационных сигналов в физической среде. Транспортная сеть – это совокупность всех ресурсов, выполняющих функции транспортирования. Она включает не только системы передачи, но и относящиеся к ним средства контроля, оперативного переключения, резервирования, управления [1].

Таким образом, транспортная сеть связи – это совокупность всех ресурсов, выполняющих функции транспортирования в телекоммуникационных сетях, которая включает не только системы передачи, но и относящиеся к ним средства контроля, оперативного переключения, резервирования, управления. Но существует более тривиальное определение: транспортная сеть – это сеть, основной задачей которой является осуществление транспортной функции. Транспортная функция в свою очередь заключается в доставке информации по назначению, а именно: от одного порта данной сети к другому.

В цифровой системе связи специального назначения на базе первичной сети могут создаваться транспортная сеть связи, сеть связи доступа и объектовые сети связи [2].

Главным требованием, предъявляемым к транспортным сетям, является выполнение сетью основной функции – обеспечения пользователям возможности доступа ко всем разделяемым ресурсам сети, все остальные требования связаны с качеством обслуживания конечных пользователей сети (табл.).

Основным функциональным предназначением систем специального назначения является обеспечение передачи (доставка) потоков сообщений, необходимых для управления различными объектами. Важность обеспечения своевременной передачи потоков сообщений в объемах, заданных потребностями системы управления, заключается в том, что от этого непосредственно зависит качество управления, а, следовательно, и эффективность выполняемых объектами управления действий.

Для обеспечения своевременной передачи потоков сообщений, необходимых для управления войсками, система связи должна иметь определенный уровень пропускной способности.

ТАБЛИЦА. Требования, предъявляемые к транспортной сети связи специального назначения

Требования	Показатель
Готовность сети	$T_{гот}$
Расширяемость, масштабируемость	$N_{эс}$, $N_{ус}$
Управляемость	$T_{цу}$
Пропускная способность	λ
Устойчивость	$K_{и}$
Мобильность	$T_{мб}$
Разведзащищенность	$P_{вскр}$
Доступность	C_{s}

Пропускная способность – способность системы связи передавать потоки сообщений в единицу времени с требуемым качеством.

Особая важность такого свойства систем связи, как пропускная способность, состоит в том, что оно определяет основное функциональное предназначение системы и выдвигает в качестве главной и первоочередной задачи – обеспечение необходимой пропускной способности.

В теории различают *шенноновскую* (теоретическую), *техническую* и *эксплуатационную* пропускную способность.

Шенноновская пропускная способность (R) характеризует максимально достижимую скорость передачи в канале связи. Она безотносительна к оконечной аппаратуре и определяется теоретически достижимой скоростью (бит/с) передачи в заданном спектре частот.

Пропускной способностью канала связи называют наибольшее теоретически достижимое количество информации, которое может быть передано по каналу за единицу времени. Пропускная способность канала определяется физическими свойствами канала связи и сигнала. От пропускной способности канала зависит максимально возможная скорость передачи данных по этому каналу. Для определения максимально возможной скорости надо знать три основных параметра канала связи и три основных параметра сигнала, по нему передаваемого.

Параметры канала:

F_k – пропускная способность канала связи, или, иначе, полоса частот, которую канал может пропустить, не внося заметного нормированного затухания сигнала;

H_k – динамический диапазон, равный отношению максимально допустимого уровня сигнала в канале к уровню помех, нормированного для этого типа каналов;

T_k – время, в течение которого канал используется для передачи данных.

Параметры сигнала:

F_c – ширина спектра частот сигнала, под которой понимается интервал по шкале частотного спектра, занимаемый сигналом;

H_c – динамический диапазон, представляющий собой отношение средней мощности сигнала к мощности помехи в канале;

T_c – длительность сигнала, то есть время его существования.

Произведение трех названных параметров определяют, соответственно:

объем канала связи:

$$V_k = F_k H_k T_k,$$

объем сигнала:

$$V_c = F_c H_c T_c.$$

От пропускной способности канала связи зависит максимально возможная скорость передач данных по этому каналу, которая определяется формулой Шеннона.

Максимально возможная пропускная способность не зависит от способа физического кодирования, так как определяет возможности линии при гипотетическом наилучшем способе кодирования [2].

Пропускная способность сети зависит как от характеристик физической среды, так и от принятого способа передачи данных. Пропускная способность часто используется в качестве характеристики не только сети, сколько собственно технологии, на которой построена сеть.

Техническая пропускная способность ($R_т$) характеризует достигнутую при разработке и производстве средств связи скорость передачи сообщений. Она определяется техническими возможностями аппаратуры (терминалов) по передаче сообщений (того или иного вида) и образованию каналов передачи.

Техническая пропускная способность транспортной сети связи не зависит от загруженности сети и имеет постоянное значение, определяемое используемыми в сети технологиями.

На разных участках сети, где используется несколько разных технологий, пропускная способность может быть различной. Для анализа и настройки сети необходимо знать данные о пропускной способности ее элементов [3].

Эксплуатационная (или реальная) пропускная способность ($R_э$) характеризует пропускную способность системы связи (направления связи, линии, канала и средства передачи), которая обеспечивается или может быть обеспечена с учетом всех дестабилизирующих факторов, снижающих возможности по передаче потоков сообщений.

Между шенноновской, технической и реальной пропускной способностью существует прямая зависимость:

$$R_{\text{Т}} = k_{\text{Т}}R, k_{\text{Т}} < 1;\ R_{\text{э}} = k_{\text{э}}R_T, k_{\text{э}} < 1,$$

где $k_{\text{т}}$ – коэффициент, учитывающий снижение шенноновской пропускной способности за счет несовершенства технических решений; $k_{\text{э}}$ – коэффициент, учитывающий снижение технической пропускной способности за счет эксплуатационных потерь.

Эксплуатационная (реальная) пропускная способность может выражаться реальной скоростью передачи данных ($R_{\text{пд}}$) или количеством сообщений данных (пакетов), передаваемых в единицу времени ($\lambda_{\text{пд}}$).

Требования к пропускной способности задаются количеством сообщений (λ) определенного объема (V) для различных видов связи, которые необходимо передать с заданной своевременностью, т. е. критерием пропускной способности является соотношение:

$$\lambda_i \geq \lambda_{i\text{тр}} \text{ при } Q_i \geq Q_{i\text{тр}},$$

где λ_i – возможности по передаче сообщений i-го вида; $\lambda_{i\text{тр}}$ – требуемая пропускная способность по передаче сообщений i-го вида; Q_i – обеспечиваемая вероятность своевременной передачи поступающих сообщений i-го вида; $Q_{i\text{тр}}$ – требуемая вероятность своевременной передачи сообщений i-го вида.

При оценке пропускной способности системы связи и задании требований к ней по данному свойству обычно применяются показатели, имеющие однозначную оценку для всех видов связи. Такими показателями являются входящий поток сообщений Z_{ij} (поток сообщений данного вида связи, поступающий на j-е направление системы связи) и исполненный поток сообщений Y_{ij} (переданный системой связи), характеризующие соответственно поступающую в систему связи и исполненную ею нагрузку. Величина Y_{ij} характеризует пропускную способность системы (направления, канала) связи, а требования к пропускной способности задаются соотношением $Y \geq Z$.

Соотношения между показателями λ_{ij}, $\lambda_{ij\text{тр}}$ и Z_{ij}, Y_{ij} выражаются в виде:

$$Z_{ij} = \lambda_{ij\text{тр}}t_{\text{с}}, \text{Y}_{ij} = \lambda_{ij}t_c.$$

В качестве единицы измерения входящего и исполненного потока сообщений принят эрланг, показывающий время занятия канала связи для передачи сообщений. Один эрланг соответствует одному часу занятия канала в течение часа. При необходимости от пропускной способности, выраженной в эрлангах (Эрл), можно перейти к пропускной способности, выраженной количеством сообщений в час:

$$\lambda = \frac{Y}{t_c},$$

где $t_{\text{с}}$ – среднее время передачи сообщения (ч).

Приведенные оценки пропускной способности характеризуют функционирование транспортной сети связи в интересах вторичных сетей связи. Задача планирования транспортной сети связи системы связи заключается в том, чтобы создать такую ее структуру, которая обеспечивала бы передачу в полном объеме потоков сообщений, создаваемых вторичными сетями.

В первую очередь при планировании транспортной сети связи специального назначения будет учитываться пропускная способность и достоверность передачи данных, поскольку эти характеристики прямо влияют на производительность и надежность создаваемой сети. Пропускная способность и достоверность – это характеристики, как линии связи, так и способа передачи данных. Поэтому если способ передачи (протокол) уже определен, то известны и эти характеристики.

Однако нельзя говорить о пропускной способности линии связи, до того как для нее определен протокол физического уровня. Именно в таких случаях, когда только предстоит определить, какой из множества существующих протоколов можно использовать на данной линии, очень важными являются остальные характеристики линии, такие как полоса пропускания, перекрестные наводки, помехоустойчивость и другие характеристики.

Конкретные количественные значения требований к пропускной способности по каждому виду связи определяются на основе обработки статистических данных, а также научного прогнозирования потребностей системы управления в информационном обмене в операции.

Существующие и рассмотренные выше вопросы оценки пропускной способности транспортных сетей на сегодняшний день не могут в полной мере применяться для определения основной функции сети –транспортировки различных потоков информации (сообщений), а чаще используется при анализе производительности вторичных сетей связи.

С одной стороны (технической), пропускная способность транспортной сети связи специального назначения зависит как от характеристик физической среды, так и от принятого способа передачи данных, она не зависит от загруженности сети и имеет постоянное значение, определяемое используемыми в сети технологиями. Пропускная способность используется в качестве характеристики не только сети, но и собственно технологии, на которой построена сеть. С этой точки зрения, оценка пропускной способности транспортной сети связи определяется технологией аппаратуры, физическими свойствами канала связи и сигнала.

С другой стороны, для обеспечения своевременной передачи потоков сообщений, необходимых для управления войсками, транспортная сеть связи должна иметь определенный уровень пропускной способности, то есть обладать способностью передавать потоки сообщений в единицу времени с требуемым качеством. В данном случае на пропускную способность транспортной сети связи будут оказывать множество факторов:

устойчивость системы и линий связи, топологическая структура построения сети, объем информации постигаемый в систему в единицу времени и т. п.

Список используемых источников

1. О связи: федер. закон Рос. Федерации от 7 июля 2003 г. N 126-ФЗ (действ. редакция 2006 г.): принят Гос. Думой Федер. Собр. Рос. Федерации 18 июня 2003 г.; одобр. Советом Федерации Федер. Собр. Рос. Федерации 25 июня 2003 г. // Рос. газ. – 2003. – 10 июля.

2. Карташев А. В. Основные направления развития перспективных услуг связи для ВС РФ / Связь в Вооружённых Силах Российской Федерации. 2011. С. 52–53.

3. Попов Г. Н., Кулеша О. П. Расчёт и измерения качественных показателей транспортной сети: учебное пособие. – Новосибирск : СибГУТИ, 2002. 103 с.

4. Фокин В. Г. Управление телекоммуникационными сетями: учебное пособие. Новосибирск : СибГУТИ, 2001. 112 с.

УДК 621.315

ЭВОЛЮЦИЯ СТАНДАРТОВ СКС

В. С. Иванов, О. Г. Патрик

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

В статье рассматриваются причины появления и последующего развития стандартов СКС. Приводятся изменения основных, нормируемых международным стандартом ISO/IEC 11801, электрических характеристик кабелей СКС.

структурированная кабельная система, стандарты СКС, нормирование характеристик.

Необходимость в разработке стандарта на локальные вычислительные сети (ЛВС) появилась в связи с тем, что в 80-х годах прошлого столетия разработчики ЛВС различных фирм использовали различные типы кабелей, способы их прокладки и различные способы их терминирования и измерений.

История стандартизации структурированных кабельных систем (СКС) началась с выпуска в июне 1991 г. первого в США национального стандарта TIA/EIA-568-A «Commercial Building Telecommunications Cabling Stanadard» («Стандарт на телекоммуникационную кабельную систему коммерческого здания»).

Международная организация по стандартизации (ISO) и Международная электротехническая компания (IEC) также выпускают в 1995 г. международный стандарт на СКС: ISO/IEC 11801 «Information technology-Generic

cabling for customer premises» («Информационная технология – универсальная кабельная система для зданий и территории заказчика»).

В странах Европейского Экономического Союза также в 1995 г. Европейский комитет по стандартизации в области электротехники и электроники – CENELEC (фр. *Comite Europeen de Normalisation Electrotechnique*) выпустил основополагающий европейский стандарт: EN 50173 «Information technology – Generic cabling systems» («Информационная технология – Структурированные кабельные системы»).

В течение 2002–2011 г.г. выходили последующие редакции американских, европейских и международных стандартов. В 2008 г. появился отечественный стандарт ГОСТ Р 53246-2008, а затем в 2012 г. – ГОСТ Р 54429-2011 [1, 2].

Динамика развития стандартов хорошо видна на рисунке.

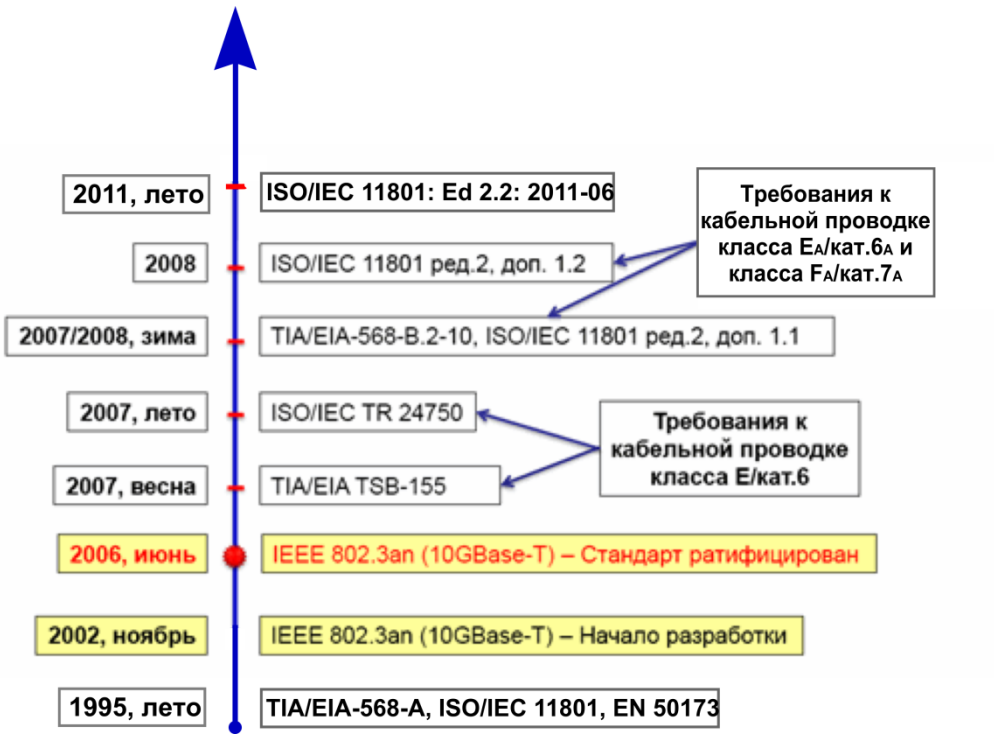


Рисунок. Динамика развития стандартов СКС

На ранних этапах развития СКС электрические характеристики кабелей намного превышали требования активного оборудования. Но по мере увеличения скорости передачи данных (10 Мбит/с в 1995 г., 10 Гбит/с в 2006 г.) требования разработчиков активного оборудования становились все более жесткими. Если в 1995 г. достаточно было контролировать всего лишь 5 параметров, то в 1999 г. – вдвое больше, что хорошо видно из таблицы 1. Данные, приведенные в таблице 1, заимствованы из [3].

Помимо учета помех, возникающих при взаимном влиянии пар друг на друга на ближнем конце кабеля при встречном направлении передачи, потребовалось учитывать взаимное влияние на дальнем конце кабеля

при совпадающем направлении передачи, а также влияние от соседних пар в кабельном сердечнике (PSNEXT и PSILFEXT).

В дальнейшем были введены новые параметры тестирования кабельных пар, характеризующие влияние от соседних кабелей:

– ANEXT – Alien Near End Crosstalk;
– PSANEXT – Power Sum Alien Near End Crosstalk;
– AFEXT – Alien Far End Crosstalk;
– PSAFEXT – Power Sum Alien Far End Crosstalk.

Изменилось название защищенности на дальнем конце – ELFEXT (*Equal Level Far End Crosstalk*). Согласно Международному стандарту ISO/IEC 11801 с 2008 г. этот параметр стали обозначать как ACR-F. Был изъят из употребления параметр ACR, так как он легко определяется в результате вычитания из переходного затухания на ближнем конце вносимых потерь.

Таблица 1. Нормирование характеристик кабелей СКС на f = 100 МГц (Класс D/Кат. кабеля 5)

Наименование параметра	1995 г.	1999 г.	2002 г.
1. Insertion loss (вносимые потери), дБ/100 м	23,2	20,6	20,4
2. Return loss (возвратные потери), дБ/100 м	10,0	12,1	12,0
3. NEXT (переходное затухание на ближнем конце), дБ не менее	24,0	29,3	32,3
4. ACR, дБ	4,0	8,7	11,9
5. Propogation delay, мкс	1,0	0,85	0,49
6. Delay skew, мкс	–	0,043	0,044
7. PSNEXT (суммарное переходное затухание на ближнем конце), дБ не менее	–	26,3	29,3
8. PSACR, дБ	–	5,7	8,9
9. ELFEXT (защищенность на дальнем конце), дБ не менее	–	19,6	18,6
10. PSELFEXT (суммарная защищенность на дальнем конце), дБ не менее	–	17,0	15,6

Увеличение скорости передачи данных сначала до 40 Гбит/с, а затем до 100 Гбит/с потребовало применения экранирования как отдельных пар, так и кабельного сердечника в целом. Появились новые категории кабелей: категория 7 (диапазон частот до 600 МГц) и категория 7_A (диапазон частот до 1000 МГц). Ожидается появление стандартов, регламентирующих работу

СКС в диапазоне частот до 2000 МГц, Класс I (Категория 8.1) и Класс II (Категория 8.2) (табл. 2) [1].

Таблица 2. Основные характеристики кабелей СКС (ГОСТ Р 54429-2011)

Наименование параметра	*F*, МГц	Катег. 5 Класс D	Катег. 6 Класс E	Катег. 6_A Класс E_A	Катег. 7 Класс F	Катег.7_A Класс F_A
1. Коэффициент затухания при температуре 20^0 С, дБ/100 м, не более	100	22,0	19,9	19,1	19,0	18,5
	250	–	33,0	31,3	31,0	29,7
	500	–	–	45,3	45,3	42,8
	600	–	–	–	50,1	47,1
	1000	–	–	–	–	61,9
2. Затухание отражения (возвратные потери), дБ, не менее	100	20,1	20,1	20,1	20,1	20,1
	250	–	17,3	17,1	17,1	17,1
	500	–	–	15,6	15,6	15,6
	600	–	–	–	15,6	15,6
	1000	–	–	–	–	15,1
3. Переходное затухание на ближнем конце (NEXT), дБ/100 м, не менее	100	35,3	45,3	45,3	72,4	75,4
	250	–	39,3	39,3	66,4	69,4
	500	–	–	34,8	61,9	64,9
	600	–	–	–	60,7	63,7
	1000	–	–	–	–	60,4
4. Переходное затухание суммарной мощности влияния на ближнем конце (PSNEXT), дБ не менее	100	32,3	42,3	42,3	69,4	72,4
	250	–	36,3	36,3	63,4	66,4
	500	–	–	31,8	58,9	61,9
	600	–	–	–	57,7	60,7
	1000	–	–	–	–	57,4
5. Защищенность на дальнем конце (ILFEXT), дБ/100 м, не менее	100	24,0	28,0	28,0	55,3	55,3
	250	–	20,0	20,0	47,3	47,3
	500	–	–	14,0	41,3	41,3
	600	–	–	–	39,7	39,7
	1000	–	–	–	–	35,3
6. Защищенность от суммарной мощности влияния на дальнем конце (PSACR-F), дБ/100 м, не менее	100	21,0	25,0	25,0	52,3	52,3
	250	–	17,0	17,0	44,3	44,3
	500	–	–	11,0	38,3	38,3
	600	–	–	–	36,7	36,7
	1000	–	–	–	–	32,3

Список используемых источников

1. Семенов А. Б. СКС категории 8 // Журнал сетевых решений (LAN). 2014. № 5. – С. 52–57.

2. ГОСТ Р 54429 – 2011 Кабели связи симметричные для цифровых систем передачи. Общие технические условия. М. : Стандартинформ. 2012. 43 с.

3. Самарский П. А. Основы структурированных кабельных систем. М. : Компания АйТи; ДМК Пресс, 2005. 216 с.

УДК 621.315

АНАЛИЗ ИНФОРМАЦИИ ПО ВОСП-СР ОТЕЧЕСТВЕННОГО И ЗАРУБЕЖНОГО ПРОИЗВОДСТВА

С. А. Иванов, Ю. А. Сафронов

Военная академия связи им. Маршала Советского Союза С. М. Буденного

В этой статье представлен анализ информации по системам с разреженным спектральным мультиплексированием – CWDM и системам с плотным спектральным мультиплексированием – DWDM, которые на сегодняшний день являются основными системами, решающими проблему и обеспечивающие практически неограниченные возможности роста полосы пропускания. Так же не стоит забывать о такой системе как перестраиваемые оптические мультиплексоры ввода-вывода – ROADM, которые позволяют легко и быстро увеличить пропускную способность линии связи там, где это нужно, не прибегая к дорогим методам перепроектировки сети и не останавливая предоставление услуг связи.

DWDM, CWDM, ROADM.

Сегодня среди ведущих компаний телекоммуникационной техники идет серьезная конкуренция за рынок сбыта. Самые крупные компании задают общий темп рынку и занимают большие его сегменты, более мелкие компании занимают определенные ниши и становятся лидерами только в них. При этом между ними нет единых стандартов и зафиксированных предложений по вопросам каналообразования на канальном уровне. Это, во-первых, усложняет коммутацию оптических каналов внутри сегмента одного бренда и требует применения ROADM. Во-вторых, делает практически невозможным коммутацию каналов на оборудовании различных брендов.

Данная разница в стандартах является существенным препятствием для создания единого международного телекоммуникационного пространства с коммутацией оптических каналов.

Настоящая статья дает краткий анализ современного состояния рынка многоканальных волоконно-оптических средств связи ведущих мировых производителей, с целью определения возможных направлений построения волоконно-оптических средств связи как основы перспективной телекоммуникационной системы связи с коммутацией оптических каналов.

Основными производителями ВОСС на сегодняшний день являются: США (*Cisco, Juniper Networks*), Российская Федерация (Т8, ОАО СУПЕРТЕЛ, НТО ИРЭ-Полюс), КНР (*Huawei Technologies Co*), Республика Франция (*Alcatel-Lucent*).

ТАБЛИЦА 1. Сводная таблица оборудования и характеристик

На обор	Производитель и страна производитель	Страна Бренда	Общий стандарт	Оптические усилители	ROADM	Свои стандарты для канало-образования
Мульт пла «В	Т8, Российская Федерация	Российская Федерация	МСЭ-Т G.694.1	EDFA, RAMAN и гибридные EDFA+RAMAN	WSS 1×1, 1×2, 1×4, 1×9	Нет
«СП	ОАО СУПЕРТЕЛ, Российская Федерация	Российская Федерация	МСЭ-Т G.694.1	EDFA, RAMAN	Нет	Нет
«П	НТО ИРЭ-Полюс, Российская Федерация	Российская Федерация	МСЭ-Т G.694.1	EAU, ROP-EAU, RAU	Нет	Нет
Cisco Serie Sys	Cisco	США	МСЭ-Т G.694.1	EDFA, RAMAN	Есть	Есть
Hua BWS	Huawei Technologies Co, КНР	КНР	МСЭ-Т G.694.1 G.692, G.691, G.681, G.otn	EDFA\Raman	Есть	Патентованная технология Su-perWDM
EX-4	Juniper Networks	США	МСЭ-Т G.694.1	Нет	Нет	Есть
Alca 183	Alcatel-Lucent	Республика Франция	МСЭ-Т G.694.1	RAMAN	Tunable ROADM	Есть

Из таблицы 1 видно, что компании придерживаются только стандартов, устанавливающих положение оптических каналов в линейном спектре – G.694.1 (DWDM) и G.694.2 (CWDM)

DWDM-плотные WDM (англ. dense WDM, сокр. DWDM) – системы с разносом каналов около 100 ГГц, позволяющие мультиплексировать до 40 каналов.

CWDM-грубые WDM (англ. coarse WDM, сокр. CWDM) – системы с частотным разносом каналов более 2500ГГц, позволяющие мультиплексировать не более 18 каналов. Используемые в настоящее время CWDM работают в полосе от 1271 нм до 1611 нм, промежуток между каналами 20 нм (2500 ГГц) (рис. 1).

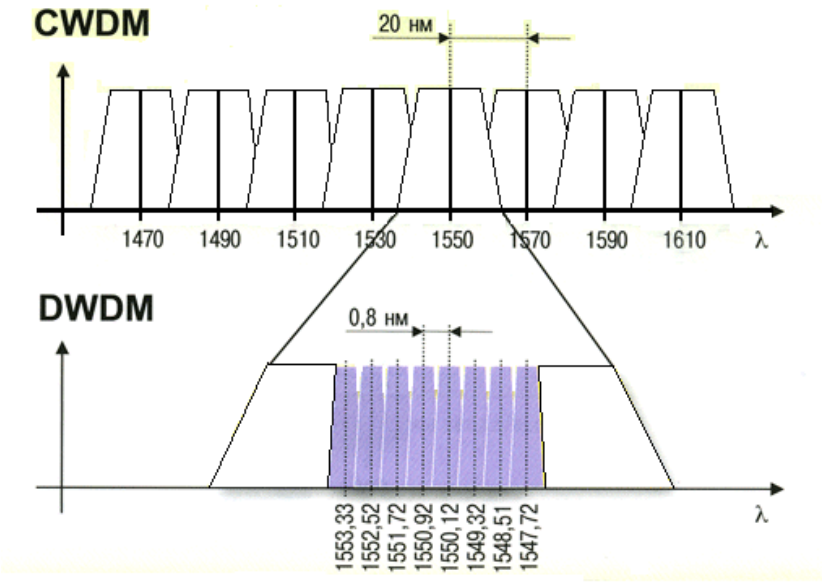


Рис. 1. Частотное разделение каналов CWDM и DWDM

Стандартов на режимы работы лазеров (линейного оборудования) и канального оборудования – нет. Между компаниями постоянно возникают трения [8, 9].

Коммутация разноволновых каналов осуществляется с помощью перестраиваемых оптических мультиплексоров ввода-вывода (ROADM), которые составляют до 70 % стоимости станционного оборудования.

Применение различных по конструкциям ROADM имеет ряд ограничений, обусловленных, прежде всего, возможностями по доступу к оптическим каналам средствами оптических коммутаторов на основе различных технологий (WB, MEMS, PLC, WSS), величинами потерь мощности в оптических соединениях коммутаторов, уменьшением полосы пропускания оптического канала при каскадировании ROADM с пространственными оптическими фильтрами технологии AWG (*Arrayed Waveguide Grating*), требуемым временем реконфигурации и перестройки источников излучения в транспондерах.

Плюсы и минусы ROADM разных поколений показаны в таблице 2. Схемы ROADM (рис. 2–5).

ТАБЛИЦА 2. Поколения ROADM их плюсы и минусы

Тип	Достоинства	Недостатки
WB (wavelength block) (рис. 2)	Первые представители ROADM количество портов ввода/вывода равно количеству волн	Большие размеры, высокая цена, закрепление длины волны за портом, невозможность увеличения порядка узла
PLC (planar lightwave circuit) (рис. 3)	Низкая цена, малые размеры, простое программное обеспечение и техническое исполнение	Закреплённость длины волны за определённым портом, невозможность масштабирования узла
WSS (wavelength selective switch) (рис. 4)	Возможность коммутации любого количества волн на любой порт, масштабируемость	Высокая цена, большие размеры, сложное обслуживание
OXC (PXC) (Optical Cross-Connect) (рис. 5)	Возможность коммутации любого числа волн на выходные порты, масштабируемость	Сложность реализации функций широкого вещания, зависимость сложности от технологии исполнения коммутатора

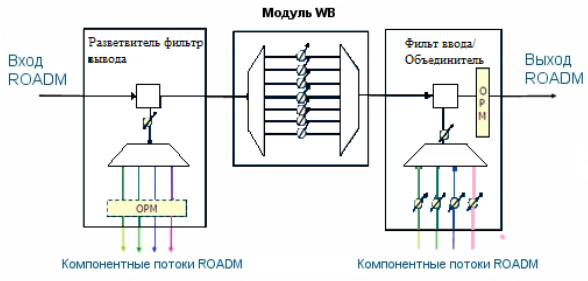


Рис. 2. Схема WB

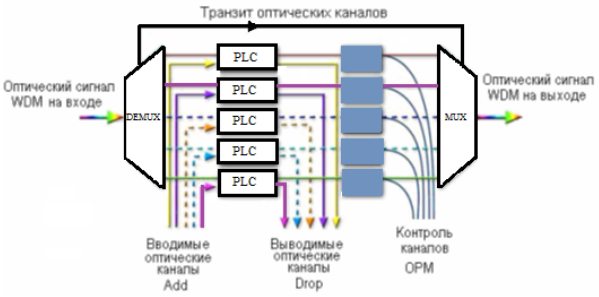


Рис. 3. Схема PLC

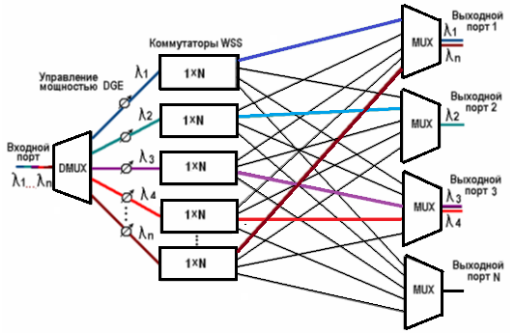


Рис. 4. Схема WSS

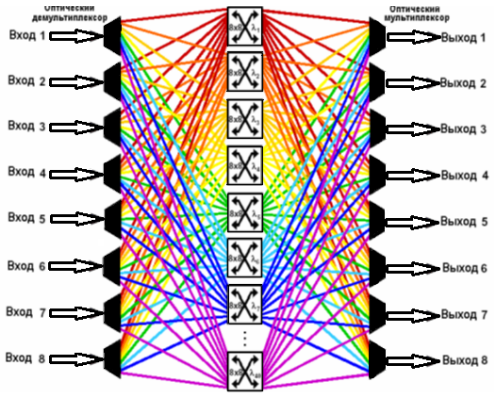


Рис. 5. Схема OXC (PXC)

При выходе из строя ROADM остается ограниченный объем коммутации, и основная часть действующих каналов по направлению связи теряется.

Так как сегодня на сетях связи функционирует большая номенклатура не стандартизированного оборудования волоконно-оптического оборудования связи то возникает проблема обучения обслуживающего его персонала и связанна с необходимостью обучения эксплуатации на каждом типовом образце средств связи. Подготовка таких специалистов долгое и дорогое удовольствие

Приведенные выше аспекты позволяют сделать следующие выводы:

1. Сложная многоуровневая коммутация разноволновых оптических каналов, в сегменте одного бренда, и практическое отсутствие такой коммутации между оборудованием разных брендов, требует разработки следующего поколения многоканальной оптической системы передачи с типовыми каналами.

2. Для унификации и обеспечения возможности встречного рабочего оборудования различных брендов на линейном и канальном уровне необходима стандартизация режимов работы линейного и канального оборудования многоканальных ВОСП.

Список используемых источников

1. Сайт компании Т8. URL: http://t8.ru/?page_id=3600 (дата обращения 11.03.2016).

2. Сайт компании ОАО СУПЕРТЕЛ. URL: http://www.supertel.info/spektr.html (дата обращения 13.03.2016).

3. Сайт компании НТО ИРЭ-Полюс. URL: http://www.ntoire-polus.ru/products_pusk.html (дата обращения 13.03.2016).

4. Сайт компании Cisco. URL: http://www.cisco.com/c/en/us/products/optical-networking/ons-15200-series-dwdm-systems/index.html (дата обращения 13.03.2016).

5. Сайт компании Huawei Technologies Co. URL: http://huawei.com/ru/products/transport-network/wdm-otn/bws1600G/index.htm (дата обращения 14.03.2016).

6. Сайт компании Juniper Networks. URL: http://www.juniper.net/us/en/products-services/switching/ex-series/ex4200/ (дата обращения 14.03.2016).

7. Сайт компании Newbridge Systems Integration. URL: http://www.nsi-com.ru/hardware/20 (дата обращения 14.03.2016).

8. Сайт Издательства «Открытые системы». URL: http://www.osp.ru/nets/2003/03/148445/ (дата обращения 10.03.2016).

9. Попсулин С. Китай ответил на обвинения США в шпионаже с помощью оборудования Huawei и ZTE [Электронный ресурс]. URL: http://www.cnews.ru/news/top/kitaj_otvetil_na_obvineniya_ssha_v_shpionazhe_1 (дата обращения 10.03.2016).

УДК 004.728.8

МЕТОДИКА ЗАЩИТЫ СЕТИ СВЯЗИ ОТ DDOS АТАК С ПОМОЩЬЮ BGP FLOWSPEC

Д. Б. Казаков, А. В. Красов, Н. О. Лоханько, Р. С. Подоляк

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

Данная статья посвящена BGP Flow Specification, описанного в RFC 5575, и чаще сокращенно называемому BGP FlowSpec. Это расширение протокола BGP, основная задача которого динамически отражать DDoS атаки. Целью статьи ставиться рассказ о самом протоколе, о его функционировании, рассматриваются и анализируются сценарии противодействия для различных DDoS атак при различных топологиях сетей связи, описываются особенности BGP FlowSpec, а также другие варианты его использования помимо предотвращения DDoS атак.

безопасность сети, BGP FlowSpec, DDoS.

Технология BGP FlowSpec использует довольно популярный подход, заключающийся в разделении data plane и control Plane. Control plane – это формирование некой топологии на базе существующий сети для управления самой сетью. Data plane – использует результат работы Control plane и служит для передачи полезного трафика.

Подразумевается, что есть некоторое центральное устройство или элемент, который обеспечивает формирование различных правил. Точка принятия решения не обязана находится на пути следования трафика и появляется возможность разделить обработку полезного трафика и формирование распространение правил BGP (рис. 1).

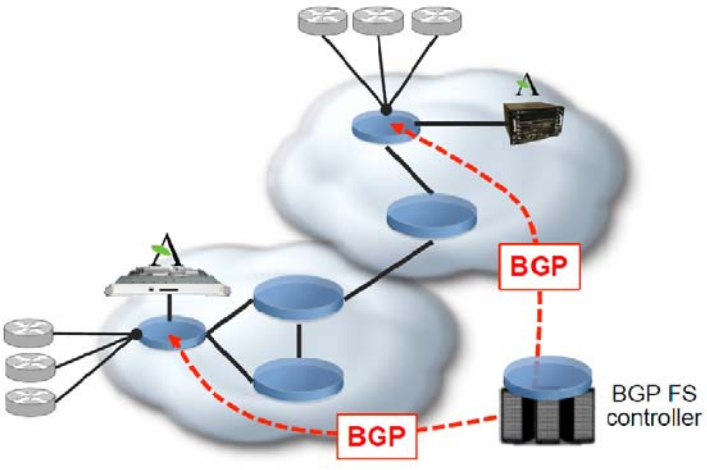


Рис. 1. Архитектура сети с использованием BGP FS

В рамках концепции BGP FlowSpec существуют 3 элемента – контроллер, клиент и route reflector, из которых первые два обязательны. Контроллер представляет собой устройство или программное обеспечение, задача которого сводится к тому, чтобы сформировать и распространить правила для клиента. Правила говорят, что и с каким трафиком нужно сделать. Контроллер может быть совмещен с клиентом (например, это может быть маршрутизатор). Контроллер осуществляет выбор нужной политики и сигнализация с помощью BGP на клиентов (*Control plane*). Функциональность контроллера поддерживается либо специализированным программным обеспечением, либо маршрутизаторами под управлением IOS XR. Задача контроллера обнаружить нелегитимные действия или нелегитимный трафик, а также выработать и распространить правила BGP FlowSpec. Разделение Data Plane и Control Plane подразумевает что контроллер работает с Data Plane, а клиент работает и с Data Plane и с Control Plane.

Протокол BGP FlowSpec описывается в RFC 5575. В качестве сигнального протокола был выбран BGP, так как он является наиболее универсальным, из-за возможности расширения этого протокола (поддерживает добавление новых address family) а также поддерживается большинством маршрутизаторов. Также протокол BGP является основой для функционирования сети Интернет, поэтому выбор его как транспорта логичен, если не сказать безальтернативен. Для того чтобы реализовать необходимую функциональность используется новый тип NLRI с новой комбинацией address family [1]. Этим NLRI будет гранулярно описываться тот трафик, к которому впоследствии будет применяться нужное действие.

BGP FlowSpec правила применяются на входящем направлении интерфейса и используют TCAM. Следует учесть, что BGP FlowSpec использует технологии PBR, что приводит к различным последствиям с точки зрения производительности.

Рассмотрим применение технологии BGP FlowSpec при противодействии DDoS. DDoS атаки направлены на то, чтобы в течении какого-то времени жертва атаки, фактически, перестала функционировать. Поэтому, как правило, DDoS атаки призваны дискредитировать, остановить или повредить бизнес компаний. Атака может генерироваться любым узлом или группой узлов в интернете, но можно постараться эту атаку определенным образом подавить. Эффективность противодействия DDoS во многом осуществляется тем, где применяются средства защиты. Необходимо реализовать функции защиты как можно ближе к источнику DDoS атаки. Также следует понимать, что природа атак тоже различна. Некоторые атаки очень легко отфильтровать, но их мощь может заключаться в огромном объеме трафика. Более сложными атаками являются атаки, реализуемые на уровне приложений, и для противодействия им нужна система, которая сможет проанализировать трафик и определить легитимный он или нет.

Существует 3 типа DDOS атак:

1) Stateless Amplifications атаки. Это атаки, которые не используют процедуру установления соединения перед отправкой нелегитимного трафика. Узел посылает очень маленькие по размеру запросы, но с подделанным IP-адресом источника. Запросы направлены на определённые протоколы и сервисы в сторону реально существующих узлов сети. Получая такие запросы, эти легитимные узлы сети отвечают вполне легитимным трафиком. Но вследствие природы протокола, используемого для атаки, ответ будет по размеру превосходить исходный запрос. Причём ответ будет высылаться не в сторону узла с которого получен запрос, а в сторону подделанного IP адреса (рис. 2).

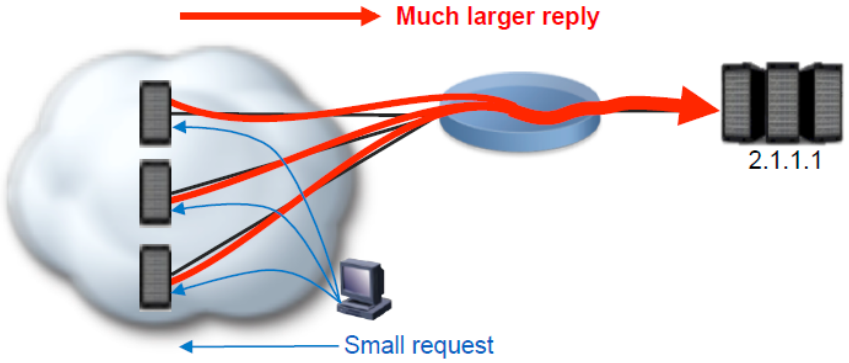


Рис. 2. Схема Stateless Amplification DDoS атаки

BGP FlowSpec может использоваться для фильтрации 1-го и 2-го типов атаки. При атаке 3-го типа атаки BGP можно просигнализировать правило, которое перенаправит этот трафик на систему, которая сможет провести более глубокий анализ.

2) L3/L4 атаки. Это атаки такие как UDP flood или ICMP flood. UDP-флуд – это атака, использующая бессеансовый режим протокола UDP. Она заключается в отправке множества UDP-пакетов на определённые или случайные номера портов удалённого хоста, который для каждого полученного пакета должен определить соответствующее приложение, убедиться в отсутствии его активности и отправить ответное ICMP-сообщение «адресат недоступен». В итоге атакуемая система окажется перегруженной, так как в протоколе UDP механизм предотвращения перегрузок отсутствует, поэтому после начала атаки паразитный трафик быстро захватит всю доступную полосу пропускания, и полезному трафику останется лишь малая её часть. Подменив IP-адреса источников в UDP-пакетах, злоумышленник может перенаправить поток ICMP-ответов и тем самым сохранить работоспособность атакующих хостов, а также обеспечить их анонимность [2].

С помощью BGP FlowSpec можно просигнализировать правило сообщающее о том, что трафик направляющийся в сторону определенного узла

и с соответствующем флагом фрагментации нужно выделить соответствующую полосу пропускания (рис. 3) [3]. Подобным образом BGP FlowSpec позволяет противодействовать атакам первого типа.

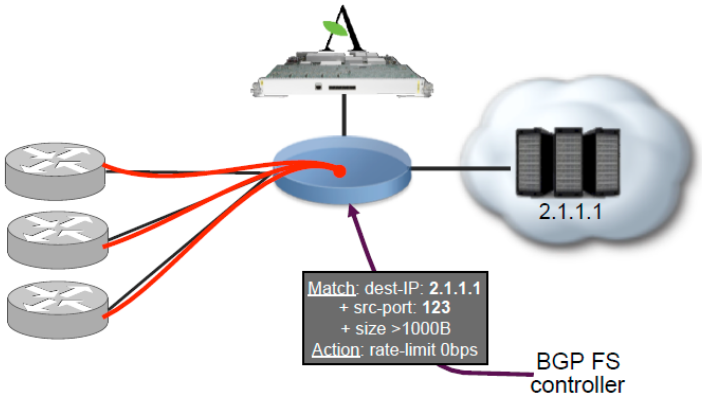


Рис. 3. Схема противодействия DDoS атаки 2-го типа

3) Атаки уровня приложений. Это наиболее сложный для обнаружения тип атаки, так как со стороны сетевых устройств, трафик будет казаться абсолютно легитимным. В качестве противодействия таким атакам BGP FlowSpec контроллер, при обнаружении подозрительной активности может просигнализировать правило, сообщающее что трафик, предназначающийся атакуемому узлу, нужно направить на подключенный узел по очистке трафика. Поэтому контроллер должен получать телеметрию сети и на основе этой информации принять решение о действии и сигнализировать о нём с помощью BGP FlowSpec ().

Действие, применяемое к трафику, может быть смена next-hop адреса. Альтернативой этому может быть перенаправление в сторону другого VRF (рис. 4).

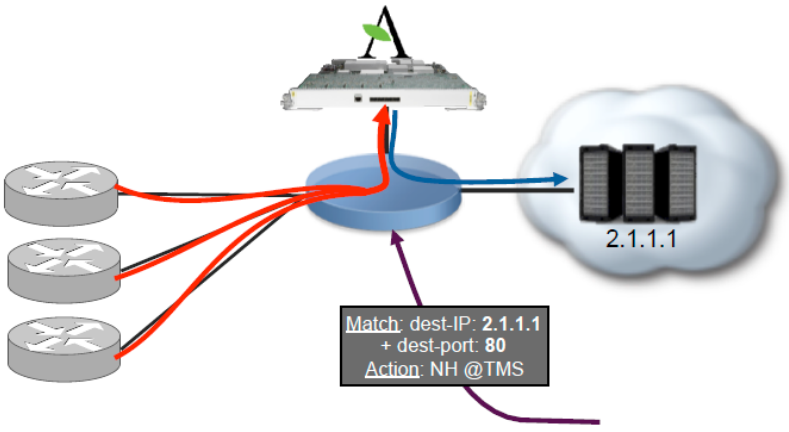


Рис. 4. Схема противодействия DDoS атакам уровня приложений

Рассмотрим основные достоинства технологии BGP FlowSpec:

1) Возможность реализации централизованной точки управления. (можно разместить контроллер вне пути прохождения трафика).

2) В различие от механизмов ACL возможно гораздо более гранулярно определить тот трафик, к которому в последствии будет применяться какое-либо действие – перенаправление, фильтрация, блокирование и т. д. Нет необходимости обрабатывать весь трафик.

3) Возможность подавлять DDoS атаку если она достаточно простая либо перенаправлять эту атаку в сторону специализированных центров очистки (если это необходимо) с помощью BGP FlowSpec.

4) Нет необходимости в статических маршрутах.

5) Не нужно в случае атаки создавать маршрут в сторону VRF для фильтрации. Для определенного вида трафика указывается правило о том, что он перенаправляется в сторону определенного VRF.

BGP FlowSpec можно использовать не только для подавления DDoS атак. Например, в случае если необходимо обеспечить трансляцию IP адресов, а в наличии имеются устройства с разной производительностью масштабируемостью. Это приведёт к тому, что очень сложно распределить трафик по устройствам так чтобы он соответствовал возможностям той или иной платформы. BGP FlowSpec позволяет на границе сети, направленной на абонентов, применять BGP FlowSpec правила, которые будут распределять трафик по доступным ресурсов для трансляции IP адресов. Зная заранее, что один из модулей у может обработать 30 Гбит/с можно сформировать правило с помощью централизованного контроллера в котором укажется, для какого сегмента сети нужно сформировать правило перенаправления на 30 гигабитный модуль. Для других префиксов также можно гранулярно выбрать трафик и направить его на соответствующую платформу.

Также в зависимости от ситуации появляется возможности динамически перераспределять трафик, например, для URL фильтрации. В этом случае весь HTTP трафик направляется в центр фильтрации, в котором, впоследствии, выполняется фильтрация по URL.

BGP FlowSpec представляет из себя гибкое и универсальное решение, позволяющее эффективно бороться с DDoS атаками в масштабах сети, а также динамично управлять потоками трафика в сети.

Список используемых источников

1. Бабайцев А. Расширенные возможности протокола BGP [Электронный ресурс]. 24.11.2014. URL: http://pt.slideshare.net/CiscoRu/rasshirennye-vozmozhnosti-protokolabgp (дата обращения 29.03.2016).

2. UDP Flood (англ.) // DDoS Attack Glossary (Incapsula, Inc.) URL: http://incapsula.com›ddos/attack-glossary/udp-flood.html (дата обращения 29.03.2016).

3. Коденцев Д. Обеспечение безопасности сети оператора связи с помощью BGP FlowSpec [Электронный ресурс]. 17.06.2015. URL: http://ciscoclub.ru/vebinar-po-tehnologiyam-i-resheniyam-dlya-operatorov-svyazi-2 (дата обращения 29.03.2016).

УДК 004.716

ПРОБЛЕМЫ СЕТЕВОЙ БЕЗОПАСНОСТИ В ИНТЕРНЕТЕ ВЕЩЕЙ

Р. В. Киричек, А. В. Петриков

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

В настоящее время Интернет Вещей является наиболее значимой концепцией в сфере телекоммуникаций и в тоже время одной из потенциально опасных технологий. Статья посвящена обзору и исследованию актуальных проблем сетевой безопасности в рамках концепции Интернета Вещей. Рассматриваются характерные особенности IoT-устройств с точки зрения сетевой безопасности, анализируются причины возникновения основных уязвимостей, а также основные виды атак. Показана невозможность применения классических методов защиты информации для большинства IoT-устройств, а также формулируются задачи по обеспечению конфиденциальности, целостности и доступности информации в зависимости от функций, выполняемых Интернет Вещью.

Интернет Вещей, сетевая безопасность, конфиденциальность, целостность, шифрование.

Интернет вещей (англ. *Internet of Things*, IoT) – сеть физических объектов, оснащенных встроенной электроникой, программным обеспечением, интерфейсами взаимодействия, позволяющими организовать сбор, хранение и передачу информации. Данная концепция подразумевает плотную интеграцию компьютерных систем с окружающей средой, при этом обеспечивается освобождение человека от необходимости непосредственного участия во многих общественно-экономических процессах [1, 2, 3].

Поскольку основными объектами данной концепции являются «вещи», подключенные к сети, количество которых в последние годы стремительно растет (от 500 млн в 2003 г. до 25 миллиардов в 2015 г.), то днем появления Интернета Вещей принято считать дату, когда количество таких устройств сравнялось с населением Земли (2008–2009 гг.) [4]. Уже сегодня 98,8 % изготовленных микропроцессоров используется в встраиваемых системах, и только 1,2 % – в традиционных компьютерах.

К таким системам можно отнести радиочастотные метки, бесконтактные смарт-карты, SIM-карты, средства системы глобальной мобильной связи, средства автоматизированных систем управления технологическими процессами (SCADA), беспроводные сенсоры, имплантированные медицинские сенсоры: стимуляторы мозга, электронные кардиостимуляторы; электронные паспорта и прочие электронные средства идентификации личности, средства автоматизации поставок, системы проведения банковских операций через Интернет, автоматическая оплата пошлин, услуг, дорожных

и прочих сборов, общественный транспорт, средства борьбы с контрафактной продукцией, противоугонные автомобильные системы, средства контроля и отслеживания багажа, и т. д. [5, 6].

Очевидно, что уже в настоящее время Интернет Вещей охватывает широкий спектр сфер жизнедеятельности общества, что в очередной раз подчеркивает значимость данной концепции в современном мире. Однако, не стоит забывать, что при всех своих преимуществах, концепция Интернета Вещей несет в себе огромное количество потенциальных проблем [7], в первую очередь связанных с сетевой безопасностью [8, 9]. Так, например, в отчете национального разведывательного совета США Интернет Вещей указывается как одна из наиболее потенциально опасных технологий относительно ближайшего будущего [10].

В рамках концепции Интернета Вещей, как и в любой информационной системе, задача по обеспечению безопасности сводится к реализации следующий трех требований:

1. Конфиденциальности данных (доступность только для субъектов, имеющих на неё право).

2. Целостности данных (невозможность несанкционированной модификации).

3. Доступности данных (невозможность временного или постоянного сокрытия информации от авторизованных пользователей).

При этом стоит отметь, что, поскольку Интернет Вещей является следующей ступенью развития существующей сегодня глобальной сети Интернет и построен в т. ч. и на уже широко используемых сетевых протоколах (в частности протоколах стека TCP/IP), ему присущи все классические проблемы, связанные с сетевой безопасностью данных протоколов, однако атаки на IoT-системы имеют свою специфику. В данной статье внимание уделяется проблемам безопасности, связанными с особенностями Интернета Вещей, т. е. с теми новыми аспектами, которые Интернет Вещей привносит в глобальную сеть.

Для выявления таких особенностей необходимо выделить основные факторы, являющиеся предпосылками развития концепции Интернета Вещей [1, 2]:

– непрерывный процесс миниатюризации электронных устройств;

– снижение энергопотребления за счет совершенствования процесса производства электронных компонентов;

– снижение стоимости электронных устройств;

– разработка новых беспроводных протоколов передачи данных с низким энергопотреблением.

Вместе с тем, большинство из вышеперечисленных факторов являются и ограничениями с точки зрения сетевой безопасности, поскольку требова-

ния к низкой стоимости, низкому уровню энергопотребления, и к компактности устройств затрудняют реализацию классических методов защиты в виде привычных криптографических алгоритмов шифрования данных и аутентификации сообщений и устройств (DES, AES, RSA, ГОСТ 28147-89 и т. д.).

Так же стоит отметить, что преимущественно беспроводной характер соединений IoT-устройств и потенциальная возможность физического доступа повышают вероятность проведения атак, связанных с пассивным прослушиванием, атак по побочным каналам (электромагнитное излучение), атак, связанных с фальсификацией узлов, а также атак, связанных с физическим разрушением устройств [11, 12].

На основе вышеперечисленных фактов можно заключить, что концепция Интернета Вещей требует применения новых подходов и методов в области сетевой безопасности, среди которых авторами были выделены три основных потенциально эффективных направления исследований:

– малоресурсная криптография – разработка и анализ алгоритмов шифрования не требовательных к аппаратным ресурсам устройства;

– методы, связанные с особенностями распространения радиосигналов;

– применение методов сетевой стеганографии.

Стеганография реализует метод передачи информации с учетом сохранения в тайне самого факта передачи (рис. 1).

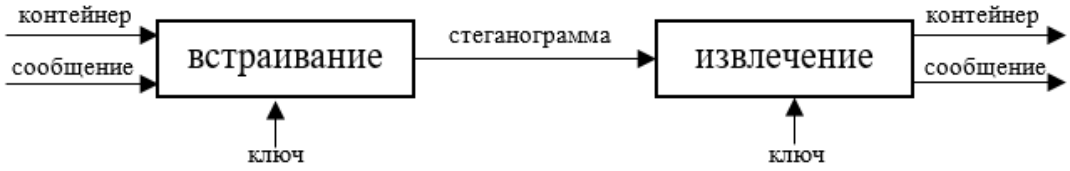


Рис. 1. Общая схема стегосистемы

При этом контейнером для вложения может выступать широкий ряд различных сущностей (звуковой файл, видео, текст и т. д.), однако в сетевой стеганографии вложение информации, как правило, осуществляется в заголовки пакетов сетевых протоколов (рис. 2).

Version	IHL	Type of Service	Total Length	
Identification			Flags	Fragment Offset
Time to Live		Protocol		
Source Address				
Destination Address				
Options + Padding				

Рис. 2. Заголовок IP пакета с помеченными полями,
в которые можно осуществить вложение

По предположению авторов, сетевая стеганография может быть успешно использована в рамках концепции Интернета Вещей в качестве одного из методов обеспечения сетевой безопасности, однако этот вопрос требует дополнительных исследований, направленных на анализ возможности вложения данных в поля заголовков наиболее широко используемых протоколов.

Список используемых источников

1. Кучерявый А. Е. Интернет Вещей // Электросвязь. 2013. № 1. С. 21–24.
2. Кучерявый А. Е., Прокопьев А. В., Кучерявый Е. А. Самоорганизующиеся сети. СПб. : Любавич, 2011. 312 с.
3. Kirichek R., Koucheryavy A. Internet of Things Laboratory Test Bed // Lecture Notes in Electrical Engineering – Heidelberg: Springer, 2016. Т. 348. PP. 485–494.
4. Evans D. The Internet of Things How the Next Evolution of the Internet Is Changing Everything [Электронный ресурс] // Cisco [сайт]. URL: http://www.cisco.com/c/dam/en_us/about/ac79/docs/innov/IoT_IBSG_0411FINAL.pdf (дата обращения 15.03.2016).
5. Кучерявый А. Е., Киричек Р. В., Парамонов А. И., Прокопьев А. В. Эволюция исследований в области беспроводных сенсорных сетей // Информационные технологии и телекоммуникации. 2014. № 4 (8). С. 29–41.
6. Воеводин Ю. В., Киричек Р. В. Обзор уникальных программно-аппаратных параметров различных технологий Интернета Вещей // Информационные технологии и телекоммуникации. 2015. № 4 (12). С. 40–47.
7. Интернет вещей и информационная безопасность [Электронный ресурс] // Cisco [сайт]. URL: http://www.cisco.com/web/RU/news/releases/txt/2013/03/032813c.html (дата обращения: 15.03.2016).
8. Kirichek R., Kulik V., Koucheryavy A. False clouds for Internet of Things and methods of protection // Proceedings of the 18th International Conference on Advanced Communication Technology (ICACT) 2016. PP. 201–205.
9. Киричек Р. В., Нгуен Д. К. Исследование влияния потока ложных запросов в беспроводных сенсорных сетях на разряд батареи питания конечных узлов // Информационные технологии и телекоммуникации. 2015. № 1 (9). С. 128–138.
10. Six Technologies with Potential Impacts on US Interests Out to 2025 [Электронный ресурс] // Conference report. URL: http://fas.org/irp/nic/disruptive.pdf (дата обращения: 15.03.2016).
11. Кулик В. А, Киричек Р. В., Бондарев А. Н. Методы исследования беспроводных каналов связи Интернета Вещей в условиях совместной работы // Информационные технологии и телекоммуникации. 2015. № 1 (9). С. 106–114.
12. Hoang T., Kirichek R., Paramonov A., Koucheryavy A. Influence of intentional electromagnetic interference on the functioning of the terrestrial segment of flying ubiquitous sensor network // Lecture Notes in Electrical Engineering. 2016. Т. 376. PP. 1249-–1259.

УДК 519.223.41

ИССЛЕДОВАНИЕ ВЛИЯНИЯ ПРЕДНАМЕРЕННЫХ ЭЛЕКТРОМАГНИТНЫХ ВОЗДЕЙСТВИЙ НА КАНАЛЫ СВЯЗИ ИНТЕРНЕТА ВЕЩЕЙ

Р. В. Киричек, А. А. Разумов

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

Широкое распространение технологий, связанных с использованием Интернета Вещей, ставит новые задачи по повышению стойкости и отказоустойчивости каналов беспроводной связи. Одним из критериев безопасного использования беспроводных каналов связи является их защищенность от воздействия сверхкоротких электромагнитных импульсов как наиболее вероятного фактора воздействия на процесс передачи данных.

Интернет Вещей, сверхкороткий электромагнитный импульс, matlab, simulink.

В настоящее время широкое распространение получила концепция Интерне Вещей [1, 2]. Согласно этой концепции, множество Вещей подключаются к Интернет посредствам различных каналов связи, среди которых преобладают беспроводные. Для формирования каналов связи Интернет Вещей на базе стандартов IEEE 802.11x, 802.15.1, 802.15.4 применяется широкополосный канал связи, преимущественно работающий в диапазонах частот от 300 МГц до 3 ГГц (рис. 1) [3, 4]. К основным преимуществам можно отнести высокую пропускную способность каналов связи до 6 Гбит/с и высокую проникающую способность радиоволн указанного диапазона. Таким образом, преимуществом данного вида связи является возможность организации каналов с большей пропускной способностью и высокой помехоустойчивостью.

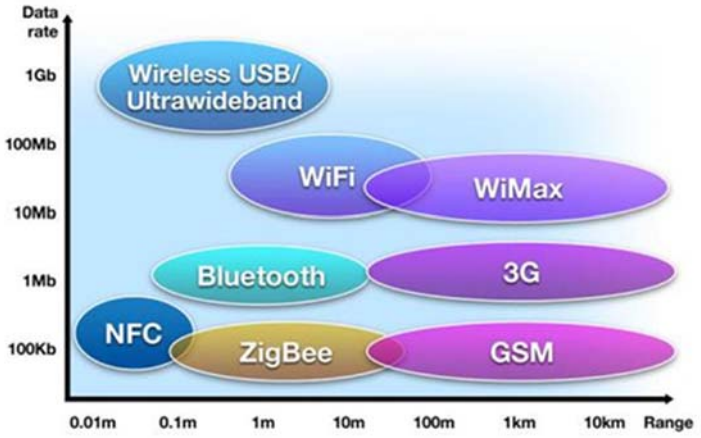


Рис. 1. БС на базе стандартов IEEE 802.11x, 802.15.1, 802.15.4

Рассмотрим структуру кадров в стандартах IEEE 802.11, 802.15.1, 802.15.4. Структура кадров данных для стандарта IEEE 802.15.1 представлена на рисунке 2.

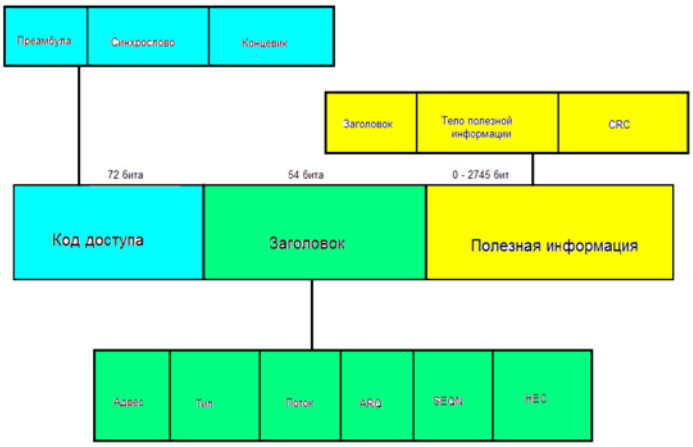


Рис. 2. Структура кадра IEEE 802.15.1

Стандарт IEEE 802.11 использует три класса кадров, передающихся в канале: информационные, служебные и управляющие. Рассмотрим структуру информационного кадра (рис. 3).

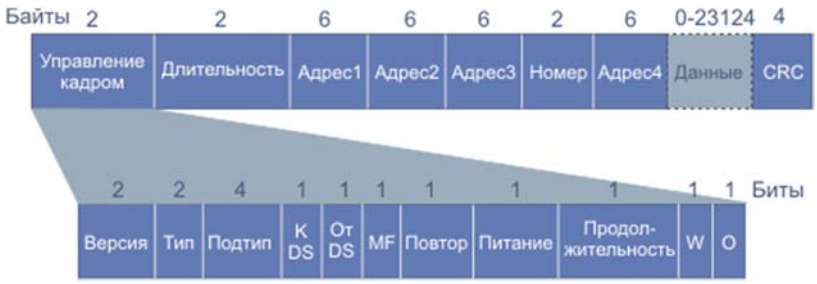


Рис. 3. Структура кадра IEEE 802.11

В стандарте IEEE 802.15.4 структура кадров была разработана по критерию минимальной сложности, обеспечивающей надежную передачу данных в зашумленном низкоскоростном канале (рис. 4).

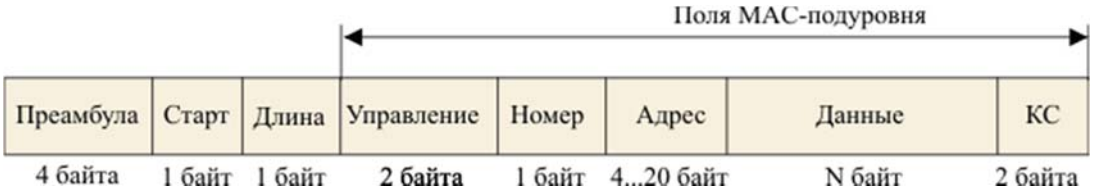


Рис. 4. Формат кадра данных в стандарте IEEE 802.15.4

Для исследования влияния преднамеренных электромагнитных воздействий на каналы связи Интернета Вещей требуется разработать имитацион-

ную модель. Данная модель с одной стороны должна учитывать особенности различных технологий передачи данных (IEEE 802.11, 802.15.1, 802.15.4), а с другой стороны выполнять необходимые функции с заданным уровнем абстракции т. е. допущениях, которые не скажутся на результатах моделирования.

На сегодняшний день одним из потенциально опасных источников помех являются преднамеренное электромагнитное воздействие. Данное воздействие, маскируясь под электромагнитные помехи, приводит к уничтожению, искажению и блокированию информации в канале связи [5, 6].

Исходя из специфики СК ЭМИ, для оценки его потенциального влияния необходим подход, анализирующий перекрытие областей спектра воздействующего импульса и спектра сигнала в точке приема [7, 8]. Потенциально влияние может быть оказано при перекрытии большей площади спектра полезного сигнала [9]. На рисунке 5 условно изображены спектры сверхширокополосного, широкополосного, узкополосного сигналов связи и сверхкороткого электромагнитного импульса.

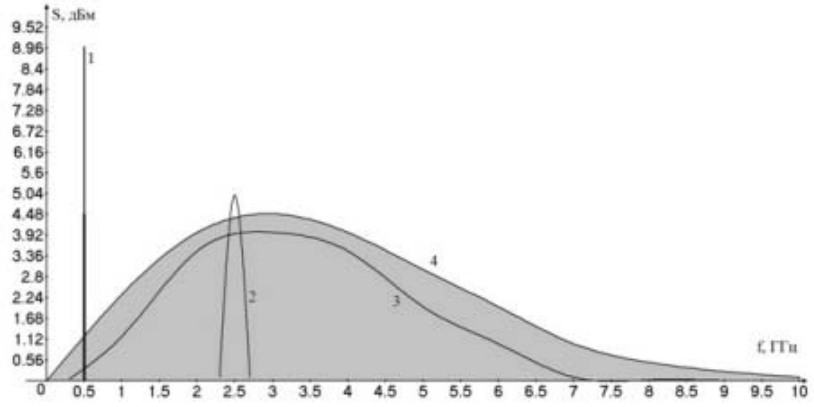


Рис. 5. Условные спектры каналов: 1 – узкополосная связь, 2 – широкополосная связь, 3 – сверхширокополосная связь, 4 – сверхкороткий электромагнитный импульс

Стоит отметить, что при частоте следования импульсов широкополосной помехи ниже, чем символьная последовательность модулированного сигнала, оказываемое влияние будет ниже, чем при соизмеримой или более высокой частоте следования импульсов широкополосной помехи [10].

Для реализации поставленной задачи по моделированию воздействия СК ЭМИ на беспроводной канал связи была выбрана технология IEEE 802.11x и проведен анализ существующих на сегодняшний день пакетов имитационного моделирования.

Были рассмотрены пакеты имитационного моделирования, обеспечивающие максимальную визуализацию процесса передачи данных ZyXEL Wireless Optimizer, Wi-Fi Planner PRO и т. п. – это приложения, представляющие собой инструмент планирования и оценки производительности беспроводных сетей Wi-Fi стандарта 802.11a/b/g/n.

Далее были рассмотрены симуляторы, написанные на языках высокого уровня, решающие задачи проектирования и анализа беспроводных сетей: Riverbad Modele, QualNet, GloMoSim и т. п.

В рассмотренных пакетах имитационного моделирования отсутствует возможность реализации воздействия СК ЭМИ на беспроводной канал передачи данных.

Проведя анализ программных продуктов, ориентированных для имитации различных телекоммуникационных технологий и отвечающего критериям необходимым для построения имитационной модели воздействия СК ЭМИ на канал связи Интернета Вещей можно констатировать, что на данный момент не существует готового решения для реализации поставленной задачи. В связи с этим рассмотрим универсальные пакеты визуального моделирования MATLAB; EASY5; MATRIX; LabView.

Среди данных пакетов визуального моделирования наиболее подходящий для целей проводимого исследования – пакет MATLAB/Simulink. В этом пакете на всех этапах работы, особенно при подготовке моделей систем, пользователь практически не имеет дела с программированием, а создается из большой библиотеки готовых модулей.

Для проведения исследования была разработана имитационная модель в пакете MATLAB/Simulink (рис. 6), состоящая из следующих блоков: блок генерации/формирования и кодирования кадров (Transmitter); блок беспроводного канала связи (Channel) с аддитивным белым гауссовым шумом (AWGN) и генератором СК ЭМИ (Pulse generator); блок приема и декодирования кадров (Receiver); датчиков скорости, осциллографа и блока для отображения значений квадратично амплитудной модуляции.

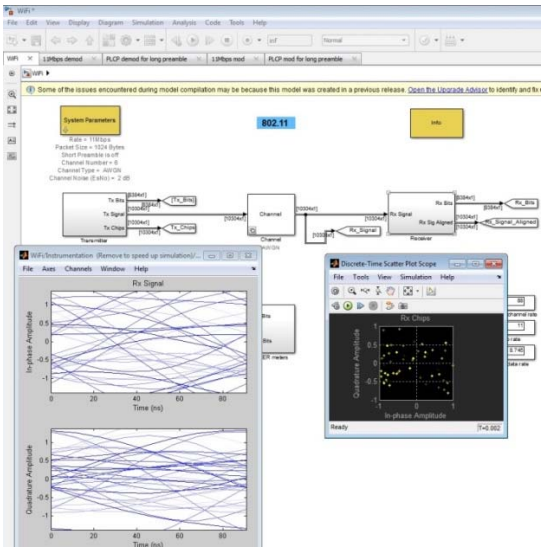


Рис. 6. Имитационная модель передачи данных
в БС при воздействии СК ЭМИ

Имитируемая помеха характеризуется равномерной спектральной плотностью, нормально распределённым значением амплитуды и аддитивным способом воздействия на полезный сигнал (передача данных). Термин «аддитивный» означает, что данный вид шума суммируется с полезным сигналом.

Для моделирования помехи в виде сверхкоротких электромагнитных импульсов был разработан блок Pulse generator, в котором задавались такие параметры СК ЭМИ, как: частота следования импульсов, длительность импульсов и амплитуда импульсов, частота осцилляций. Наибольшая потеря кадров была зафиксирована при увеличении частоты следования сверхкоротких импульсов, что связанно с перекрытием каналов передачи данных.

Ввиду того, что результаты полученные в ходе серии компьютерных экспериментов с разработанной имитационной моделью значительно отличались от допустимых параметров, было принято решение о проведении натурных испытаний и калибровки модели.

Список используемых источников

1. Кучерявый А. Е. Интернет Вещей / А. Е. Кучерявый // Электросвязь. 2013. № 1. С. 21–24.

2. Kirichek R., Koucheryavy A. Internet of Things Laboratory Test Bed // Lecture Notes in Electrical Engineering – Heidelberg: Springer, 2016. Т. 348. PP. 485–494.

3. Кучерявый А. Е., Киричек Р. В., Парамонов А. И., Прокопьев А. В. Эволюция исследований в области беспроводных сенсорных сетей // Информационные технологии и телекоммуникации. 2014. № 4. С. 29–41.

4. Кулик В. А, Киричек Р. В., Бондарев А. Н. Методы исследования беспроводных каналов связи Интернета Вещей в условиях совместной работы // Информационные технологии и телекоммуникации. 2015. № 1 (9). С. 106–114.

5. Электромагнитный терроризм на рубеже тысячелетий / Под ред. Т. Р. Газизова. Томск : Томский государственный университет, 2002. 206 с.

6. Zhukovsky M., Kirichek R., Larionov S., Chvanov V. Testing of technical security equipment for stability to inten-tional electromagnetic interference // Conference on Electromagnetic Compatibility Europe: proceedings. York, 2011. PP. 820–823.

7. Киричек Р. В. Вероятностная оценка влияния сверхкоротких электромагнитных импульсов на процесс передачи данных в сетях Ethernet // Электросвязь. 2011. № 8. С. 51–54.

8. Баталов Л. А., Киричек Р. В., Лазарев Б. Н. Вероятностные характеристики электрических сигналов Fast Ethernet // Естественные и технические науки. 2011. № 3. С. 339–344.

9. Данилин С. В., Киричек Р. В. Вопросы устойчивости активного сетевого оборудования к воздействию сверхкоротких электромагнитных импульсов // Технологии ЭМС. 2009. № 1. С. 54–57.

10. Hoang T., Kirichek R., Paramonov A., Koucheryavy A. Influence of intentional electromagnetic interference on the functioning of the terrestrial segment of flying ubiquitous sensor network // Lecture Notes in Electrical Engineering. 2016. Т. 376. PP. 1249–1259.

УДК 519.223.41

СРАВНИТЕЛЬНЫЙ АНАЛИЗ ФУНКЦИОНИРОВАНИЯ АЛГОРИТМОВ МАРШРУТИЗАЦИИ В БЕСПРОВОДНЫХ СЕНСОРНЫХ СЕТЯХ В УСЛОВИЯХ ПРЕДНАМЕРЕННОГО ЭЛЕКТРОМАГНИТНОГО ВОЗДЕЙСТВИЯ

Р. В. Киричек, Л. Ч. Хоанг

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

Статья посвящена исследованию возможных уязвимостей беспроводных сенсорных сетей к преднамеренному деструктивному электромагнитному воздействию. Проведен сравнительный анализ протоколов маршрутизации, применяемых в беспроводных сенсорных сетях с учетом набора критериев, необходимых для эффективного функционирования в условиях преднамеренных электромагнитных воздействий.

беспроводные сенсорные сети (WSN), отказоустойчивость, маршрутизация, надежность, сенсорный узел, преднамеренные электромагнитные воздействия.

В настоящее время одним из популярных направлений в области самоорганизующихся сетей связи является беспроводные сенсорные сети [1, 2]. Беспроводные сенсорные сети обладают рядом особенностей по сравнению с существующими сетями, ключевыми из которых являются самоорганизация и низкое энергопотребление. Интерес к изучению таких сетей обусловлен в первую очередь широкими возможностями их применения: мониторинг окружающей среды, мониторинг состояния промышленных объектов, мониторинг транспорта, системы обнаружения вторжений и слежения за целью, пожарная безопасность, автомобилестроение, медицина и т. д. Также стоит отметить, что беспроводные сенсорные сети являются базовой основой Интернета Вещей [3].

Одним из новых видов дестабилизирующих воздействий в беспроводных сенсорных сетях являются преднамеренные электромагнитные воздействия (ПД ЭМВ) [4]. ПД ЭМВ это электромагнитное воздействие, осуществляемое путем применения портативных генераторов электромагнитного поля и приводящее к уничтожению, искажению и блокированию передаваемой информации. Искажения в структуре передаваемых данных происходят на физическом уровне в результате наводок на среду передачи. В результате воздействия с амплитудой, длительностью и энергией сопоставимой с параметрами передаваемых сигналов происходит нарушение нормального функционирования (сбои в работе) электронных устройств и передаваемой информации. Такие воздействия трудно обнаружить, так как они создаются с помощью специальных генераторов с большого расстояния

и маскируются под обычные электромагнитные помехи. Согласно ГОСТ Р 56115-2014 [5], ПД ЭМВ могут осуществляться по следующим каналам:

- электромагнитным полем;
- по линиям связи;
- по цепям питания;
- металлоконструкциям;
- заземлению.

Вследствие такого воздействия, нарушается не только функционирование (отказ) отдельных сенсорных узлов, но и целостность беспроводной сенсорной сети, находящейся в зоне электромагнитного воздействия [6]. В этой связи, необходима разработка моделей, методов и алгоритмов, которые позволят сохранить структурную целостность беспроводной сенсорной сети на базе алгоритмов маршрутизации.

Требования к алгоритмам маршрутизации в БСС

Беспроводные сенсорные сети могут иметь как постоянную структуру, так и изменяющуюся вследствие перемещения сенсорных узлов в течении времени. В этой связи, возможно использовать различные алгоритмы маршрутизации, ориентированные, в первую очередь, на увеличения жизненного цикла беспроводной сенсорной сети в целом.

Поскольку сенсорная сеть может не иметь постоянной инфраструктуры, вряд ли возможно использовать классические алгоритмы маршрутизации для сенсорных сетей. Кроме того, в USN-трафик данных может быть сгенерирован так, что одна и та же информация может быть передана в сети от различных сенсорных узлов, функционирующих в какой-либо зоне. Поскольку размеры сенсоров и затраты на их инсталляцию ограничены так же, как и их ресурсы: энергия, память, вычислительные возможности – передавать одну и ту же информацию по сети от многих сенсорных узлов нецелесообразно. Таким образом, в случае отказа 90 % узлов кластера – целесообразно доставить данные от оставшихся 10 % узлов. С этой целью применяются различные алгоритмы маршрутизации, которые позволяю решить поставленную задачу. На рисунке 1 показаны требования к алгоритмам маршрутизации в БСС [2].

Классификация алгоритмов маршрутизации в БСС

Существуют много работ посвящены вопросы классификации алгоритмов маршрутизации в БСС с учетом набор критериев, изложенных выше [1]. В таблице 1 представлена классификация алгоритмов маршрутизации в БСС с использованием типового подхода, изложенного в [1]:

Рис. 1. Требования к алгоритмам маршрутизации в БСС

ТАБЛИЦА 1. Простая классификация алгоритмов маршрутизации в БСС

Критерий	Категория	Примеры
Сетевая структура	Одноуровневая	SPIN
	Иерархическая	LEACH
Знания о ресурсах	На основе остаточной энергии	HEED
	На основе точности расположения	Directed Diffusion
Управление протоколами	Централизованное	SPIN
	Географическое	GFG
	На основе QoS-	SAR
	На основе теории очередей	COUGAR

Сравнение алгоритмов маршрутизации в БСС

В соответствии с вышеизложенным сравним различные алгоритмы маршрутизации в беспроводных сенсорных сетях (табл. 2):

ТАБЛИЦА 2. Сравнение алгоритмов маршрутизации в БСС

Протокол	Основан на атрибутах	Энерго-эффек-тивность	Местного типа	Multipath	QoS	Иерархи-ческий
SPIN	да					
Directed Diffusion	да					
COUGAR	да					

Протокол	Основан на атрибутах	Энерго-эффек-тивность	Местного типа	Multipath	QoS	Иерархи-ческий
ACQUIRE	да					
GAF		да	да			
GEAR		да	да	да		
LEACH		да				да
PEGASIS		да			да	да
TEEN		да				да
DirQ						да
SHRP		да		да	да	да
SAR		да		да	да	
Maximum Lifetime		да		да		
Energy Aware		да		да		

Альтернативная маршрутизации в БСС в условиях преднамеренного электромагнитного воздействия

Во всех случаях существенных электромагнитных воздействий реакцией БСС является перестроение маршрутов передачи трафика (изменения конфигурации), которое осуществляет используемый протокол маршрутизации. Для обеспечения функционирования БСС необходимо иметь возможность изменения (выбора) конфигурации, обеспечивающей альтернативную маршрутизацию как реакция сети на преднамеренное электромагнитное воздействие.

Предполагаем, что протокол маршрутизации выполняет изменение конфигурации маршрутов после изменения состояния сети, например, увеличения потерь/задержек при доставке данных, то периодическое электромагнитное воздействие на сеть приведет к вынужденным процедурам реорганизации сети для обеспечения ее функционирования. При этом необходим учитывать не только снижении связности и рост доли ошибок, но и затрат энергии на изменение конфигурации. Чем большее число транзитов в маршруте, тем выше расхода энергии, необходимой для передачи сообщения.

С учетом изложенных критериев, предлагается использовать протоколы маршрутизации LEACH, GEAR, TEEN в БСС в условиях преднамеренного электромагнитного воздействия для обеспечения эффективного функционирования сети. Рассмотрим более подробно наиболее популярные алгоритмы.

– Алгоритм LEACH: Low-Energy Adaptive Clustering Hierarchy [7] (рис. 2).

Узлы самоорганизуются в кластеры и выбирают головной узел кластера. Все узлы, которые не являются головными узлами кластера, передают информацию этого головному узлу. Головной узел кластера принимает данные, производит их обработку и передает на базовую станцию. Периодически происходит случайная смена головного узла кластера и изменение структуры кластеров.

Рис. 2. Структура построения сети при использовании алгоритма LEACH

– Алгоритм GEAR: Geographic and Energy Aware Routing [8] (рис. 3).

Ограничивает число пересылаемых запросов в направлении взаимодействия. Работает только в определенном кластере сети, вместо всей сети в целом. Каждый узел хранит текущую стоимость маршрутов и предшествующую стоимость. При выборе маршрутов учитывается оставшаяся энергия и расстояние до точки назначения.

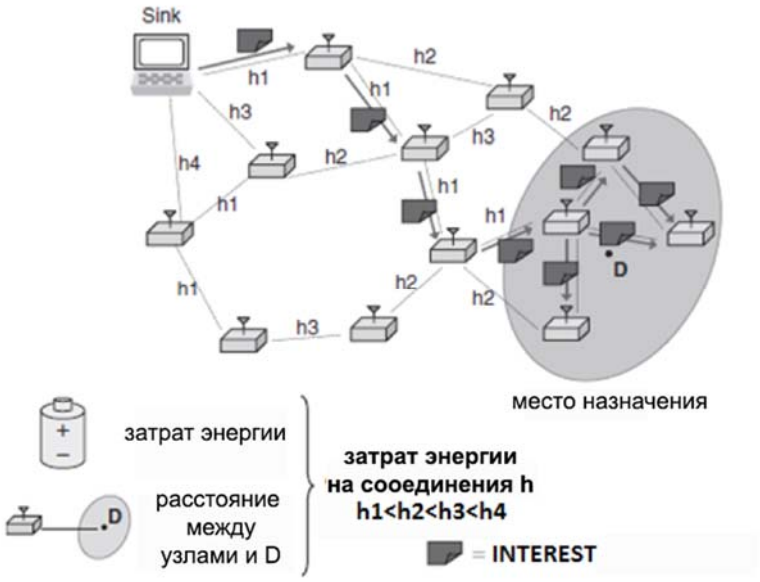


Рис. 3. Структура построения сети при использовании алгоритма GEAR

В заключении стоит отметить, что правильный выбор протоколов маршрутизации (LEACH, GEAR, TEEN) позволит сохранить структуру беспроводной сенсорной сети при отказе отдельных узлов в условиях преднамеренных электромагнитных воздействий. Дальнейшие исследования будут ориентированы на проведении серии натурных испытаний на модельной сети Лаборатории Интернета Вещей СПбГУТ.

Список используемых источников

1. Кучерявый А. Е., Прокопьев А. В., Кучерявый Е. А. Самоорганизующиеся сети. СПб. : Любавич, 2011. 312 с.

2. Кучерявый А. Е., Киричек Р. В., Парамонов А. И., Прокопьев А. В. Эволюция исследований в области беспроводных сенсорных сетей // Информационные технологии и телекоммуникации. 2014. №4. С. 29–41.

3. Кулик В. А, Киричек Р. В., Бондарев А. Н. Методы исследования беспроводных каналов связи Интернета Вещей в условиях совместной работы // Информационные технологии и телекоммуникации. 2015. № 1 (9). С. 106–114.

4. Zhukovsky M., Kirichek R., Larionov S., Chvanov V. Testing of technical security equipment for stability to intentional electromagnetic interference // Proceedings of EMC Europe 2011 York – 10th International Symposium on Electromagnetic Compatibility 2011. pp. 820–823.

5. ГОСТ Р. 56093-2014. Защита информации. Автоматизированные системы в защищенном исполнении. Средства обнаружения преднамеренных силовых электромагнитных воздействий. Общие требования. М. : Изд-во стандартов, 2015.

6. Hoang T., Kirichek R., Paramonov A., Koucheryavy A. Influence of intentional electromagnetic interference on the functioning of the terrestrial segment of flying ubiquitous sensor network // Lecture Notes in Electrical Engineering. 2016. Т. 376. С. 1249–1259.

7. Heinzelman W., Chandrakasan A., Balakrishnan H. An application-specific protocol architecture for wireless microsensor networks. IEEE Transactions on Wireless Communications 1 (4), 2002.

8. Yu Yan, Ramesh Govindan, and Deborah Estrin. Geographical and energy aware routing: A recursive data dissemination protocol for wireless sensor networks (2001).

УДК 004.75

ПРОГРАММНО-АППАРАТНЫЙ КОМПЛЕКС ПЛАНИРОВАНИЯ АВТОНОМНЫХ ПОЛЁТОВ ДЛЯ БЕСПИЛОТНЫХ ЛЕТАТЕЛЬНЫХ АППАРАТОВ ОБЩЕГО ПОЛЬЗОВАНИЯ

Р. В. Киричек, Е. Е. Ястребов

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

В настоящее время большую полярность получили беспилотные летательные аппараты (БПЛА) общего пользования ввиду простоты управления и низкой стоимости. Ввиду широкого распространения беспроводных сенсорных сетей в различных отраслях

сельского хозяйства и промышленности БПЛА стали применять для сбора данных с удаленных сенсорных полей для дальнейшей доставки в сеть связи общего пользования. Одна из ключевых задач в этой области – создание программно-аппаратного комплекса для автономных полетов БПЛА. В докладе представлено исследование существующих инструментов для планирования миссий БПЛА для различных платформ (PC, Android, iOS), а также модификация и использования этих решений в конкретных задачах. Разработанное приложение позволяет планировать маршрут БПЛА для оптимального облета сенсорных узлов, распределённых в пространстве, дает возможность загрузки полетного задания в полетный контроллер и отображения основных параметров полета по каналу телеметрии.

беспилотный летательный аппарат, маршрут, телеметрия, канал связи, программное обеспечение.

В настоящее время наибольшую актуальность приобретают Летающие сенсорные сети [1], которые стали применять в различных отраслях для сбора данных с удаленных сенсорных узлов для доставки в сеть связи общего пользования (ССОП). Существует два основных способа доставки данных с беспроводных сенсорных узлов:

– ретрансляция/транзит данных – БПЛА зависает над сенсорным узлом и в реальном времени передает получаемые данные на сервер или шлюз с ССОП;

– сбор и доставка данных к серверу или шлюзу при помощи БПЛА (идеология DTN-сетей, толерантных к задержкам).

Рассмотрим последний из перечисленных. Будем считать, что все сенсорные узлы расположены в одной горизонтальной плоскости.

Одна из ключевых нерешенных на сегодняшний день задач в этой области – автоматизированный сбор данных с сенсорного поля.

Обзор существующих инструментов для управления БПЛА

В рамках данной работы был проведен поиск и сравнение существующих программных средств для создания сценариев полета, загрузки в полетный контроллер и непосредственное управления БПЛА. Были рассмотрены два программных пакета:

– Tower & 3DR Services;

– UgCS.

Рассмотрим каждый из них более подробнее.

1 Обзор Tower & 3DR Services

3DRobotics Services дают возможность управления различными видами БПЛА и наземными аппаратами посредством открытого протокола MAV-Proxy. Соответственно, данный программный продукт может использоваться со всеми устройствами, которые поддерживают данный протокол. 3DR Services предоставляют высокоуровневое API для управления БПЛА

различных видов. 3DR Services распространяется по лицензии GPL version 3, что позволяет использовать данный программный продукта в собственных проектах без уведомления правообладателя.

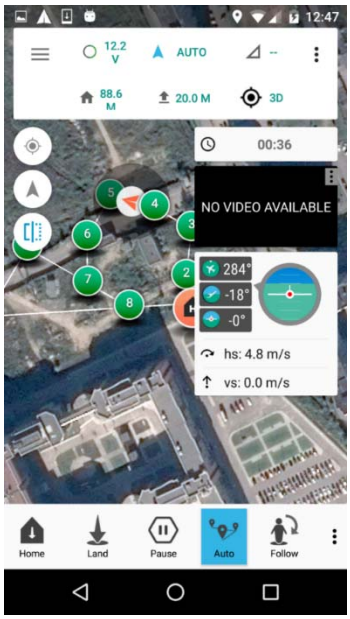


Рис. 1. Отображение маршрута следования и данных телеметрии БПЛА в Tower

На момент написания статьи данный программный продукт доступен для платформ: PC, Android.

Для создания сценариев полетов, получения и отображения показаний телеметрии пользователю используется программный продукт Tower (рис. 1), который использует API 3DR Services. Tower доступен в настоящий момент для двух платформ: PC и Android.

Tower и 3DR Service позволяют подключаться к устройствам несколькими способами: по Bluetooth, USB или через сеть, посредством технологии Wi-Fi.

В составе программных средств существует многофункциональный эмулятор БПЛА SITL, который работает, используя протокол MAVProxy. Данный эмулятор позволяет производить тестирование без использования реального оборудования.

2 Обзор UgCS – Universal Ground Control Station

UgCS – коммерческий продукт, который позволяет управлять БПЛА и планировать их полеты (миссии). UgCS имеет три вида лицензий, каждая из которых отличается набором возможных функций и ограничений для использования. UgCS также имеет в себе встроенный эмулятор некоторых видов БПЛА. В настоящий момент продукт доступен для PC и Android.

На момент написания статьи UgCS совместим с полетными контроллерами компаний DJI, Pixhawk, Mikrokopter, Micropilot, а также работает с Inspire, Phantom 3 и Phantom 2 Vision+.

Сравнение и выбор пакета ПО для разработки

Основным требованием к рассматриваемой среде разработки ПО для автономного планирования и полетов являлась необходимость наличия мобильного приложения.

В качестве основы для разработки программно-аппаратного комплекса автономного планирования и совершения полетов БПЛА были выбраны Tower и 3DR Services по нескольким причинам:

– более функциональное мобильное приложение, которое поддерживает большее количество устройств под управлением Android;

– распространение под лицензией GPL version 3;

– возможность внесения собственных изменения в программный код для достижения своих целей;

– большее количество настроек для тестирования ПО с использованием эмулятора БПЛА.

Разработка комплекса ПО для автономного планирования и полетов

Весь процесс автоматического сбора информации с сенсорных узлов можно описать в виде последовательности шагов.

1 Выбор зоны сенсорного поля на карте

Построение данной области приближенное и может корректироваться в зависимости от особенностей ландшафта местности.

2 Определение координат сенсорных узлов в заданной зоне для построения карты сенсорного поля

После взлета и прибытия в заданную зону БПЛА должен самостоятельно определить координаты сенсорных узлов в этой области. Для этого первоначально необходимо узнать координаты минимум трех сенсорных узлов (чем больше узлов с точными координатами, тем точнее будет определено местоположение остальных устройств). БПЛА, находясь в зоне расположения сенсорных узлов, путем перемещения обнаруживает радиосигналы от сенсорных узлов. Таким образом, найдя самый мощный сигнал, можно предположить, что БПЛА находится над сенсорным узлом и принять текущие координаты БПЛА за местоположение сенсорного узла. Координаты остальных сенсорных узлов можно определить путем анализа служебных данных узлов.

3 Составление карты сенсорного поля и определение оптимального маршрута для облета всех сенсорных узлов

После определения координат всех сенсорных узлов необходимо построить карту их местоположения и рассчитать оптимальный маршрут для автономного облета всех датчиков в зоне сенсорного поля. Операции расчета кратчайшего маршрута для облета сенсорных узлов являются требовательными к ресурсам процессора, а вычислительная мощность, а также заряд аккумулятора БПЛА ограничены.

Расчет оптимального маршрута облета с возвращением БПЛА в точку вылета является задачей коммивояжёра на графе [2, 3]. Эта задача является np-полной и не может иметь точного решения даже для небольшого количества узлов. Время, требуемое для расчета кратчайшего пути, экспоненциально растет от количества вершин в этом графе.

Следовательно, расчет оптимального маршрута необходимо производить по одному из описанных ниже алгоритмов.

3.1 Метод «ближайшего соседа»

Данный метод является одним из самых быстрых и менее требовательных к вычислительным ресурсам, что позволяет использовать этот алгоритм даже на самом БПЛА в процессе полета – БПЛА будет выбирать следующую точку полета в реальном времени (расчет в полетном контроллере). Однако этот алгоритм может давать погрешность до 50 % (рис. 2).

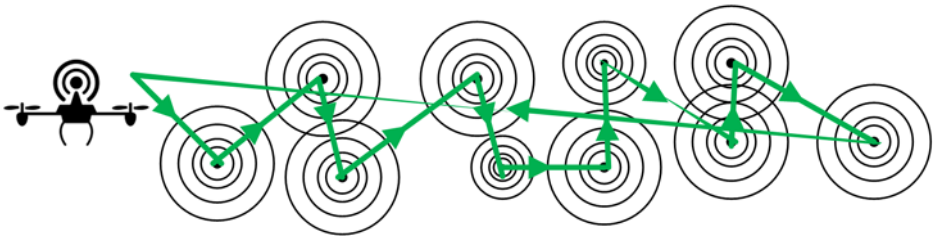


Рис. 2. Путь методом «ближайшего соседа»

3.2 Муравьиный алгоритм

Этот алгоритм основан на реальных взаимодействиях муравьев. Муравьи первоначально передвигаются в случайном порядке и по нахождению продовольствия возвращаются в свою колонию, помечая свой путь феромоном. Со временем феромоны на пути начинают испаряться, тем самым уменьшая вероятность муравьев идти по этому маршруту. На коротком пути прохождение будет более быстрым и как следствие, плотность феромонов остаётся высокой. В итоге постепенное повышение плотности приводит к конкретному кратчайшему пути (рис. 3).

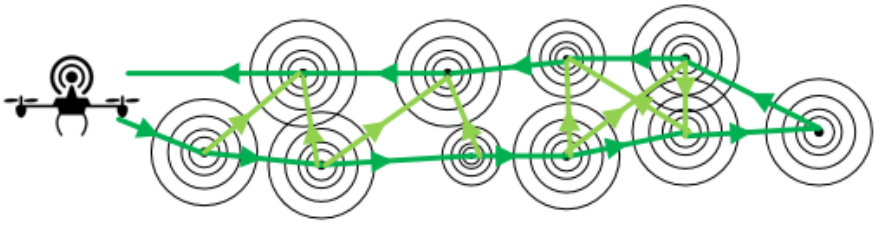


Рис. 3. Поиск маршрута «муравьиным» алгоритмом

3.3 Алгоритм штрафования вершин (Алгоритм Кристофидеса)

Этот алгоритм имеет относительно простую реализацию и обеспечивает сходимость к оптимальному решению в большинстве случаев. Метод, реализуемый алгоритмом штрафования вершин, основан на последовательном поиске кратчайших остовов графов (SST) и «штрафования» вершин, степень которых превышает 2 [4].

4 Автономный облет сенсорного поля и возврат «на базу»

После того как БПЛА совершит облет всего сенсорного поля, собранные данные необходимо доставить до шлюза с сетью связи общего пользования или к серверу, где они будут обработаны.

Заключение

В заключение стоит отметить, что все алгоритмы для построения оптимального пути являются приблизительными и не гарантируют нахождение кратчайшего пути. В зависимости от ситуации и доступных вычислительных мощностей предпочтительно использовать различные способы.

В дальнейшем планируется разработать программное обеспечение для автономных полетов, которое позволить выбирать использовать различные способы расчета оптимального маршрута.

Список используемых источников

1. Кучерявый А. Е., Владыко А. Г., Киричек Р. В., Парамонов А. И., Прокопьев А. В., Богданов И. А., Дорт-Гольц А. А. Летающие сенсорные сети // Электросвязь. 2014. № 9. С. 2–5.

2. Гараба И. В., Постников В. М. Сравнительный анализ методов решения задачи коммивояжера для выбора маршрута прокладки кабеля сети кольцевой архитектуры [Электронный ресурс] // Молодежный научно-технический вестник. 2013. № 11. URL: http://sntbul.bmstu.ru/doc/636966.html (дата обращения 16.03.2016).

3. Новиков Ф. А. Дискретная математика: учебник для вузов. 2-е изд. Стандарт третьего поколения. СПб. : Питер, 2013. 432 с.: ил. ISBN 978-5-496-00015-4.

4. Варельджян К. С., Парамонов А. И., Киричек Р. В. Оптимизация траектории движения БПЛА в Летающих сенсорных сетях // Электросвязь. 2015. № 7. С. 20–25.

УДК 004.5

АЛГОРИТМ ОПТИМИЗАЦИИ ПАРАМЕТРОВ СИСТЕМЫ WFM КАК ИНСТРУМЕНТ ПОВЫШЕНИЯ ЛОЯЛЬНОСТИ КЛИЕНТОВ ОПЕРАТОРА СВЯЗИ

С. В. Кисляков, К. Е. Ланкевич

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

Лояльность клиента зависит от множества факторов, в том числе от того, насколько корректно оператор выполняет договорённости с клиентом, в частности, как пунктуальны выездные специалисты. Двухступенчатый алгоритм оптимизации позволяет решить задачу оператора связи по улучшению качества обслуживания клиентов выездными специалистами за счёт сокращения времени выполнения наряда и гарантии обслуживания в точно подобранный временной интервал.

Workforce Management (WFM), лояльность клиентов, оптимизация.

Покажем, как система OSS-класса Workforce Management (WFM), может помочь оператору связи повысить качество обслуживания и лояльность клиентов. Рассмотрим в качестве примера непосредственное взаимодействие между клиентом и выездными специалистами, когда система WFM [1] осуществляет управление выездными бригадами сотрудников оператора связи в рамках обработки нарядов на подключение услуг.

Есть утверждение, что, если клиент будет обслужен качественно и точно в оговоренное время, то лояльность клиента возрастёт, или по крайней мере, не упадёт. Поэтому, как инструмент оператора, система должна решать задачи по подбору точного временного интервала прибытия монтёра. Под точностью временного интервала понимаем согласованный с клиентом промежуток времени, в рамках которого монтёр гарантированно сможет выполнить работы, например, по установке клиентского оборудования. Проблема подбора точного интервала определяется зависимостью от ряда таких параметров, как пожелание клиента, наличие/отсутствие специалиста с заданными компетенциями в нужное время в нужном месте, расстоянием до адреса клиента и т. д. При этом только один вариант расписания выездных специалистов может считаться оптимальным с точки зрения его эффективности [2, 3].

Предложенный алгоритм подбирает оптимальное по заданным критериям расписание задач для бригады выездных специалистов, включающее собственно участки/специалистов и их временные окна для выполнения заявок.

Задача оптимизации решается в несколько этапов. Прежде всего, необходимо решить подзадачу маршрутизации с ограничениями [4] – сформировать маршрут следования каждого монтёра так, чтобы монтёр мог оказаться у клиента в оговоренное время и при этом маршрут был кратчайшим.

Чтобы решить такую задачу оптимизации, адреса клиентов K представляем в виде вершин графа $G(K, E)$, где E – это путь монтёра между адресами, т. е. ребро графа $\{(k_i, k_j) \mid i \neq j\}$.

На каждом из адресов могут быть несколько нарядов, в случае если сразу несколько клиентов находятся на одном адресе. Т. е. с каждой вершиной K_i может быть ассоциировано некоторое количество нарядов, которые должны быть выполнены. Задача маршрутизации состоит в определении такого множества маршрутов для каждого монтёра с минимальной общей стоимостью, чтобы каждая вершина множества K была посещена только одним монтёром только один раз.

Для решения задачи необходимо:

- множества K разбить на подмножества (маршруты);
- задание порядка обхода на каждом подмножестве (перестановка вершин маршрута).

Приемлемость того или иного решения определяется дополнительными ограничениями задачи.

Целевой функцией является стоимость решения задачи:

$$F = \sum C(R_i),\ i = 1..m,$$

где $C(R_i)$ – сумма длин ребер маршрута R_i.; C – матрица стоимости пути c_{ij} между клиентами; m – количество монтёров; R_i – маршрут i-ой монтёра ($i = 1..m$).

В классическом варианте решения задачи требуется найти приемлемое решение с минимальной стоимостью. Но оптимизация должна быть выполнено по определённым критериям и в данном случае мы получаем задачу Vehicle Routing Problems (VRP) [3]. Задача программирования, которая относиться к классу NP сложных задач. Для решения поставленной нами задачи рассматривается задачу с ограничением по времени Vehicle Routing Problems with Time Windows.

Данная задача подобна VRP с основным дополнительным условием: для выполнения запроса каждого клиента k_i существует известный промежуток времени, который задаётся как дополнительное условие для построения маршрута. Это время является допустимым промежутком для выполнения наряда выездного специалиста. В рамках решения задачи мы получаем реальный момент времени выполнения наряда.

Для выполнения заказа каждого клиента существует допустимый интервал времени и реальный момент выполнения заказа в соответствии с полученным решением.

При решении данной задач мы можем минимизировать количество монтёров, необходимое для выполнения нарядов, сократить время, которое монтёр находиться в пути и, что важнее всего, сократить время ожидания клиентом специалиста.

Нужно также учитывать, что решение задачи может считаться приемлемым только в случае, если монтёр прибудет к клиенту до верхней границы допустимого временного интервала выполнения наряда.

В случае, если монтёр прибывает раньше допустимого интервала времени, ожидает его наступления.

Получив решение VRPTW имеется возможность точно подобрать время выезда монтёра избежать опозданий к клиенту.

Алгоритмы, которые лежат в основе решения задач оптимизации, являются эвристическими или чаще мета-эвристическими методами. Точные методы Branch and bound и Branch and cut не позволяют достичь требуемого результата в связи с тем, что превышается требуемое время решения задачи.

Эвристические методы позволяют найти приближенные к оптимальным решения, благодаря ограниченному поиску. Данные методы не всегда могут решать NP-сложные задачи в связи с тем, что нет гарантии получения

максимально приближенного к оптимальному варианту решения, но при этом решение задачи выполняется за требуемые промежуток времени.

Мета-эвристические методы позволяют достичь наилучшего результата в решении задач оптимизации. В мета-эвристических методах упор делается на тщательном изучении наиболее перспективных частей пространства решений. Качество получаемых решений получается выше, чем у полученных классическими эвристиками.

К данным типа алгоритмом относятся:

- Ant Algorithms;
- Constraint Programming;
- Deterministic Annealing;
- Genetic Algorithms;
- Simulated Annealing;
- Tabu Search;
- Granular Tabu;
- The adaptative memory procedure;
- Kelly and Xu (1999).

Задача по оптимизации также выполняется и на других этапах обротки наряда. Гарантия выполнения зависит порой от многих факторов, неявка монтёра может быть обусловлена форс-мажорами, которые в большей степени можно предупредить благодаря функциям системы таким как GPS-tracking [3], оперативной корректировки графика выездных работ, оптимизация расписания сотрудников по критериям.

В случае если работник по каким-либо причинам не может выполнить наряд, назначенный «на него», он может сообщить об этом диспетчеру, для того чтобы была возможность провести оперативную корректировку графиков работ выездных бригад. Реализация данного алгоритма чаще всего подразумевает автоматический подбор исполнителей для нарядов и внесение изменений в графики работ бригад.

Монтёр может получить информацию об изменении графика работ, назначенных на него, с помощью функций мобильного приложения, которое информирует сотрудника о любых изменениях в режиме реального времени.

Мобильное приложение [3] обладает не только функцией автоматического информирования сотрудников выездных служб, но также позволяет получать оптимальные маршруты выполнения задач и передавать информацию о местоположении работников и прогнозировать их прибытие к абонентам, если это требуется. Таким образом система WFM, построенная на основе предложенных алгоритмов, позволяет гарантировано выполнить наряд в указанное время и, таким образом повысить лояльность клиентов.

Список используемых источников

1. Самуйлов К. Е., Чукарин А. В., Яркина Н. В. Бизнес-процессы и информационные технологии в управлении телекоммуникационными компаниями. М. : Альпина Паблишерз, 2009. 442 с. ISBN 978-5-9614-1067-9.
2. OptaPlanner User Guide / Chapter 6. Optimization algorithms. URL: www.optaplanner.org (дата обращения 07.02.2016).
3. Кисляков С. В., Феноменов М А. Workforce Management: оптимизируем расписание // Технологии и средства связи. 2015. № 2 (107). С. 55–56.
4. Гольдштейн А., Чумачкова Е., Никулин В. Прикладная геометрия для Workforce Management // Технологии и средства связи. 2013. № 2. С. 50–51.

УДК 004.5

СПОСОБЫ УПРАВЛЕНИЯ ОТТОКОМ КЛИЕНТОВ С ПОМОЩЬЮ СИСТЕМЫ КОМПЛЕКСНОЙ ТЕХНИЧЕСКОЙ ПОДДЕРЖКИ

С. В. Кисляков, Н. С. Хабаев

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

В современном мире для телекоммуникационных компаний внедрение новых технических решений уже не является решающим для получения большего количества клиентов. Основное назначение систем автоматизации бизнес-процессов технической поддержки оператора связи – помощь клиентам в случае обращений по проблемам со связью или другими услугами. Однако, эти системы можно использовать и «не по прямому назначению» – для управления оттоком клиентов.

лояльность клиента, системы класса Assurance, управление оттоком.

На этапе обеспечения бесперебойной работы услуг с задачами повышения лояльности абонентов оператору связи помогут системы класса Assurance, например, комплексная техническая поддержка (КТП). Системы данного класса позволяют автоматизировать бизнес-процессы технической поддержки услуг и клиентов операторов связи в части:

– приема и обработки обращений клиентов, связанных со снижением качества или полным прекращением предоставления услуг связи;

– устранения повреждений проблемного оборудования, исправления массовых аварий, проведения плановых ремонтных работ и проверки подозрений на сбои в оборудовании сети и линиях связи.

В общем случае системы технической поддержки в OSS/BSS комплексе оператора связи призваны решить следующие задачи:

– повысить лояльность клиентов за счёт сокращения времени восстановления услуги и своевременного информирования о профилактических работах и неисправностях;

– уменьшить нагрузку на персонал технической поддержки за счет снижения количества обращений посредством профилактического мониторинга сети, что даст сокращение времени отклика при обращении клиента;

– собрать и проанализировать истории обращений, статистику и отчётность по различным ключевым параметрам услуги (количество нарядов, причины, тип, объем поврежденных услуг и т. д.) для разработки стратегий повышения качества услуг и обслуживания клиентов.

Первый способ – сокращение ожидания абонента при обращении в техническую поддержку оператора. Как бы хороши ни были предлагаемые услуги и тарифы, всегда бывают проблемы по их получению абонентом. Если для решения проблемы необходимо ожидать достаточно большое количество времени, все плюсы не уравновешивают этого минуса.

Система КТП может работать в нескольких режимах, позволяя регистрировать обращения как в ручном (когда оператор технической поддержки заносит в систему клиентский инцидент, получив от абонента жалобу на неисправность услуги при обращении в контактный центр оператора связи), так и в автоматическом режиме (когда абонент самостоятельно создает инцидент с помощью личного кабинета или специальной формы на сайте оператора).

В зависимости от рассчитанных показателей лояльности и важности клиента, информация о которых подгружается из соответствующих CRM или BI систем, КТП ранжирует инциденты в первоочередных задачах для обработки.

Результатом обработки является определение причины инцидента. Причиной может быть единичное повреждение или групповое повреждение, которое является причиной нескольких инцидентов одновременно. Так же для создания группового повреждения могут использоваться системы мониторинга или заявления от технического персонала, обнаружившего проблему.

Системы мониторинга (системы *fault management*) действуют по принципу опроса ключевых точек сети. Если ответ по запросу выдал значения, которые превышают выставленный пороговый критерий, то по данному элементу сети автоматически создается повреждение в системе комплексной технической поддержки, и назначается на участок для устранения аварии. По данному элементу вычисляются все услуги, затронутые повреждением.

Во втором способе управления оттоком определяем те услуги, которые затронуты повреждением, но абоненты не обращались к оператору. Для их

предупреждения о неисправностях используются системы автоинформирования, такие как системы e-mail, sms оповещения, или информирование голосовым помощником (системы *Interactive Voice Response* – IVR). При звонке от абонента такая система определяет номер звонящего, и проверяет, есть ли по услугам данного абонента проблемы. Это позволяет повысить лояльность клиентов и предотвратить их отток из компании.

Третий способ реализовывается с помощью интеграции ТП с биллинговыми системами оператора связи, что позволяет создать и автоматизировать стратегию поощрения конкретного пула клиентов компании. В рамках данной модели происходит сегментация клиентской базы на группы в зависимости от значения показателя лояльности клиента и происходит перераспределение маркетинговых ресурсов на поощрение выбранных клиентов [1]. Например, предложение не лояльным клиентам изменения условия тарифа на более выгодные, для удержания их в компании.

Для исследования используется градация типов лояльности, состоящая из трех пунктов – лояльный, не лояльный, неизвестный [2]. На первоначальном этапе все абоненты попадают в категорию неизвестных. Для каждого абонента хранится необходимая внутренняя информация, влияющая на категорию обслуживания, такая как тип абонента (физическое или юридическое лицо), давность нахождения в данном статусе лояльности, давность использования услуги, статус VIP, желание уйти к другому оператору, а также некоторый набор вычисленных коэффициентов, отображающих, например, количество нестандартных ситуаций по услуге абонента, или уровень активности абонента. На последующем этапе возможно уменьшение числа неизвестных абонентов матрицы с помощью систем обратной связи («горячие» звонки, формы на сайте, e-mail исследования). Для поддержания актуальности матрицы необходимо периодически обновлять информацию по клиентам оператора. В итоге имеем обширную матрицу, с минимальным количеством неизвестных абонентов, с помощью которой возможно делать выводы относительно качества обслуживания, а также изменения категории обслуживания у конкретных типов клиентов.

Для каждой заявки в системе технической поддержки есть рассчитываемый контрольный срок. При влиянии на него таких параметров, как количество проблем по услуге, лояльность клиента, его важность и тип, мы можем манипулировать быстротой обслуживания проблемного оборудования. Таким образом, мы добьемся исправления клиентской проблемы в кратчайшие сроки как для важных и прибыльных абонентов, так и для недовольных, тех, которые готовы уйти к другому оператору.

Итак, *четвертый способ* управления заключается в уменьшении времени обработки заявки.

Для любой компании важность удержания существующих клиентов стоит на том же уровне, что и важность привлечения новых. В современной ситуации, когда большинство абонентов уже распределено по операторам

связи, удержание абонентов выходит на первый план. Причем удержание определенной группы абонентов, приносящих большую часть прибыли, необходимо обслуживать быстрее и качественнее остальной части. Косвенно это возможно реализовать с помощью системы технической поддержки.

Список используемых источников

1. Герпотт Т. Й. Эмпирические исследования лояльности клиента. Швейцария. Издательство «Пауль Хаупт», 2004. 278 с.

2. Шуремов Е. Л. Информационные технологии управления взаимоотношениями с клиентами. М. : 1С-Паблишинг, 2005. 97 с. : ил. ISBN 5-9677-0059-5.

УДК 004.05

МЕТОДИКА ОРГАНИЗАЦИИ АККРЕДИТОВАННОГО УДОСТОВЕРЯЮЩЕГО ЦЕНТРА

М. М. Ковцур, М. В. Павлюкович

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

В связи с повсеместным распространением сети Интернет и ее популярностью наблюдается тенденция на увеличение электронного документооборота, а также возникает необходимость контроля целостности данных при передаче в канале связи. Для защиты электронного документа используется усиленная квалифицированная электронная подпись, которая формируется в специальных учреждениях – удостоверяющих центрах. Данная статья посвящена изложению методики, которая позволяет создать удостоверяющий центр. В работе структурирован набор процессов и отдельных условий, выполнение которых является обязательным при функционировании аккредитованного удостоверяющего центра.

квалифицированная электронная подпись, цифровая подпись, удостоверяющий центр, электронный документооборот, целостность документа.

С 2012 года наблюдается тенденция увеличения электронного документооборота, что делает актуальным вопрос защиты и контроля целостности данных при передаче в канале связи. Усиленная квалифицированная электронная подпись позволяет проверить целостность электронного документа, авторство, факт подписания и выдается только в специальных учреждениях – аккредитованных удостоверяющих центрах (УЦ) [1]. В конце 2015 г. насчитывалось 368 удостоверяющих центров и их количество постепенно увеличивается, что делает актуальным вопрос систематизации процессов по их созданию [2].

Стоит отметить, что существует три вида электронной подписи (ЭП): простая, усиленная неквалифицированная и усиленная квалифицированная [1]. Последняя из них позволяет подтвердить авторство, целостность данных, придать юридическую силу электронному документу и выдается исключительно в аккредитованных УЦ.

Общая концепция методики организации аккредитованного удостоверяющего центра представлена в таблице.

ТАБЛИЦА 1.Общее представление методики организации аккредитованного УЦ

№ этапа методики	Название этапа методики
1	Комплектация рабочих мест
2	Проектирование УЦ
3	Поставка ПО
4	Отладка ПО
5	Выпуск организационных документов
6	Аттестация технических средств УЦ по ФСТЭК
7	Получение лицензии ФСБ
8	Аккредитация в Минкомсвязи РФ
9	Включение в единый реестр
10	Обработка персональных данных пользователей

На первом этапе, с которого начинается процесс создания аккредитованного УЦ, выполняется набор сотрудников. Учитывая в дальнейшем необходимость получения лицензии ФСБ, должности формируются согласно требованиям ФСБ, которые подразумевают как минимум две должности. Первая – руководитель, лицо, уполномоченное управлять работами в рамках лицензируемой деятельности, имеющее высшее профессиональное образование по направлению подготовки «Информационная безопасность» (ИБ), или прошедшее подготовку по одной из специальностей этого направления не менее 500 аудиторских часов, а также имеющее стаж в области выполняемых работ в рамках лицензируемой деятельности не менее 5 лет. Вторая должность – инженерно-технический работник – лицо, имеющее высшее профессиональное образование по направлению подготовки ИБ, уполномоченное осуществлять работу в сфере лицензируемой деятельности и имеющее стаж работы в данной области не менее 1 года.

На втором этапе осуществляется проектирование УЦ. Данная процедура может выполняться как в рамках Государственного контракта по проектированию УЦ, если его работа организуется на государственном предприятии, так и силами самого УЦ. К месту размещения УЦ предъявляется ряд требований, основными из которых являются: отдельное изолированное помещение, которое делится перегородкой на серверную и административную часть, наличие видеонаблюдения, источники бесперебойного питания, способные поддерживать жизнеспособность серверного оборудования 30 минут, охранно-пожарная сигнализация, вентиляция и кондиционирование воздуха серверной части, расположение сетевого оборудования УЦ на территории УЦ.

На третьем этапе организуется поставка оборудования и программного обеспечения (ПО) для УЦ, которая может быть выполнена как путем приобретения лицензионного оборудования и ПО у официального производителя или представителя, так и путем передачи лицензионного оборудования и ПО из одного отдела предприятия в УЦ. Не рекомендуется скачивание ПО из интернета, поскольку при проверке ФСБ потребуется акт, в котором указан ресурс, время, дата, подтверждающие установку. Надежным способом получения дистрибутива считается его получение на материальном носителе, содержащем спецификацию и хеш для проверки подлинности.

На четвертом этапе выполняется монтаж и настройка комплекса УЦ. Работы могут быть выполнены силами персонала, например, настройка центра сертификации и ПО КриптоПРО.

На пятом этапе осуществляется выпуск организационных документов УЦ. Этап подразумевает разработку и издание документов, регламентирующих юридическую правомерность функционирования УЦ, среди которых: приказ об организации работы органа криптографической защиты, приказ о назначении уполномоченного лица, приказ о введении в действие регламента работы УЦ и его публикацию, регламент УЦ, должностные инструкции УЦ [3].

На шестом этапе производится аттестация технических средств УЦ по ФСТЭК. К сфере деятельности сертификата ФСТЭК относятся средства защиты информации без использования средств криптографической защиты и не составляющие государственную тайну. Аттестат подтверждает соответствие стандартам безопасности информации РФ. Его наличие вызвано необходимостью подтверждения эффективности мер и средств защиты информации. УЦ не принимается к рассмотрению на выдачу лицензии ФСБ на деятельность без аттестата соответствия ФСТЭК.

Седьмой этап состоит в получении лицензии ФСБ [4]. Происходит путем подачи заявления в уполномоченный орган. Предоставляется одна лицензия на несколько видов деятельности, УЦ касается пункт № 12 (Монтаж, установка и наладка шифровальных криптографических средств (ШФК)), № 20 (Работы по обслуживанию ШФК), № 25 (Предоставление услуг

по шифрованию информации, не составляющей государственную тайну), № 28 (Изготовление и распределение ключевых документов), № 21 (Передача ШФК).

Восьмой этап – аккредитация в Минкомсвязи РФ [2]. Происходит путем подачи заявления в уполномоченный орган, при наличии аттестата соответствия ФСТЭК, лицензии ФСБ на деятельность, а также финансового обеспечения ответственности за убытки, в сумме не менее 1,5 миллиона рублей, стоимости чистых активов УЦ не менее 1 миллиона рублей и как минимум двух сотрудников, укомплектованных согласно требованиям ФСБ России.

Девятый этап – включение УЦ в единый реестр сертификатов [5]. УЦ направляет в адрес министерства связи заявку на включение в единый реестр, при наличии как минимум аттестата соответствия ФСТЭК и лицензии ФСБ на распространение ШФК, техническое обслуживание ШФК и предоставление услуг в области ШФК, а также прочие нормативно-технические документы, требуемые для включения в реестр. После рассмотрения комплектности и содержания документов оформляется заключение о включении в перечень ЕС УЦ и впоследствии выдается свидетельство о включении в перечень ЕС УЦ.

Десятый этап подразумевает обработку персональных данных пользователей [6]. Для осуществления данной деятельности необходима подача уведомления о намерении обрабатывать такие данные в Роскомнадзор, подкрепленное частной моделью угроз, подтверждающей актуальность средств защиты УЦ и спроектированной системы защиты персональных данных.

Разработанная методика позволяет организовать аккредитованный удостоверяющий центр и обладает такими преимуществами, как актуальность и общедоступность, позволяет сократить затраты при развертывании УЦ. В работе также учтены основные изменения в нормативной законодательной базе на начало 2016 года, что подтверждает практическую ценность предлагаемой методики.

Список используемых источников

1. Об электронной подписи: федер. закон Рос. Федерации от 6 апреля 2011 г. № 63-ФЗ (ред. от 30.12.2015): принят Гос. Думой Федер. Собр. Рос. Федерации 23 марта 2011 г.: одобр. Советом Федерации Федер. Собр. Рос. Федерации 30 марта 2011 г. // Рос. газ. – 2011. – 8 апреля.

2. Аккредитация удостоверяющих центров [Электронный ресурс] // Минкомсвязь России : URL: http://www.minsvyaz.ru/ru/activity/govservices/2/ (11.04.2016).

3. О связи: федер. закон рос. Федерации от 7 июля 2003 № 126-ФЗ (ред. от 02.03.2016): принят Гос. Думой Федер. Собр. Рос. Федерации 18 июня 2003 г.: одобр. Советом Федерации Федер. Собр. Рос. Федерации 25 июня 2003 г. // Рос. газ. – 2003. – 10 июля.

4. «Об утверждении Положения о лицензировании деятельности по разработке, производству, распространению шифровальных (криптографических) средств, информационных систем и телекоммуникационных систем, защищенных с использованием шифровальных (криптографических) средств, выполнению работ, оказанию услуг в области шифрования информации, техническому обслуживанию шифровальных (криптографических) средств, информационных систем и телекоммуникационных систем, защищенных с использованием шифровальных (криптографических) средств (за исключением случая, если техническое обслуживание шифровальных (криптографических) средств, информационных систем и телекоммуникационных систем, защищенных с использованием шифровальных (криптографических) средств, осуществляется для обеспечения собственных нужд юридического лица или индивидуального предпринимателя)» [Электронный ресурс]: постановление Правительства РФ от от 16.04.2012 № 313 // СПС КонсультантПлюс: Законодательство: Версия Проф. http://www.consultant.ru/document/cons_doc_LAW_128739 (11.04.16).

5. Соглашение Минкомсвязи России, Росреестра от 26.12.2011 N ИМ-П13-21387/58 «О взаимном признании электронных подписей» (вместе с «Порядком включения удостоверяющего центра в Перечень уполномоченных удостоверяющих центров единой системы удостоверяющих центров», «Порядком разрешения конфликтных ситуаций, связанных с применением ЭП при межведомственном взаимодействии», «Требованиями к единой структуре сертификата ключа проверки электронной подписи») [Электронный ресурс] // СПС КонсультантПлюс: Законодательство: Версия Проф. http://www.consultant.ru/document/cons_doc_LAW_132235, доступ осуществляется по рабочим дням с 20-00 до 24-00 (время московское), в выходные и праздничные дни в любое время (11.04.16)

6. О персональных данных: федер. закон Рос. Федерации от 27 июля 2006 (ред. от 21.07.2014), (вступ. в силу с 01.09.2015): принят Гос. Думой Федер. Собр. Рос. Федерации 8 июля 2006 г.: одобр. Советом Федерации Федер. Собр. Рос. Федерации 14 июля 2006 г. // Рос. газ. – 2011. – 29 июля.

7. Штеренберг С. И., Виткова Л. А., В. И. Андрианов, К. А. Небаева. Комплексный подход к защите электронного документооборота : учебное пособие. СПб. : СПбГУТ, 2015. 93 с.

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

УДК 004.05

ПУТИ МОДЕРНИЗАЦИИ ПРОТОКОЛА РАСПРЕДЕЛЕНИЯ КЛЮЧЕЙ ЗАЩИЩЕННОЙ IP-ТЕЛЕФОНИИ

М. М. Ковцур

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

IP-телефония на современном этапе развития телекоммуникационных конвергентных сетей в Российской Федерации используется повсеместно для оказания услуг

связи населению и корпоративному сектору. Для предоставления сервисов применяются как выделенные каналы связи, так и каналы связи общего пользования, что делает актуальным вопрос защиты медиа трафика от несанкционированного доступа. Безопасность криптографического протокола IP-телефонии Secure Real-time Transport Protocol и время установления защищенного соединения во многом определяются протоколом распределения ключей, одним из которых является Zimmermann Real-time Transport Protocol. Статья посвящена описанию предложений по модификации протокола ZRTP с целью сокращения времени успешного выполнения протокола и повышения информационной безопасности за счет внедрения в протокол метода автоматического выявления активного нарушителя.

IP-телефония, модификация ZRTP, протокол распределения ключей, VoIP, SRTP.

Для работы IP-телефонии часто используются открытые каналы связи, которые могут содержать нарушителей, желающих получить доступ к передаваемой речевой информации [1]. Для защиты данных используется несколько криптографических протоколов – Secure SIP для защиты сигнализации, SRTP для защиты медиаинформации, а также протоколы распределения ключей (ПРК) – SDES, MIKEY, DTLS, ZRTP [2]. Безопасность при этом во многом определяется возможностями протокола распределения ключей. Одним из наиболее перспективных с точки зрения защиты от активного нарушителя является протокол Zimerman Real time protocol (ZRTP). Однако данный протокол не устойчив против атаки человек посередине активного нарушителя, владеющего технологией синтеза голоса. Поэтому целесообразно доработать данный протокол, внедрив метод обнаружения активного нарушителя [3].

Существующие исследования показывают [4], что при работе по каналам связи (КС) с высокими задержками d успешное выполнение ПРК требует значительных временных затрат, что влияет на время установления защищенного соединения Tср. В соответствии с Приказом 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» «время выполнения соединения… не должно превышать 1,5 с в сети ... телефонной связи» [5]. Однако при задержке $d > 160$ мс Tср превышает данный порог. Целесообразно сократить время успешного завершения ПРК.

Предлагается несколько модификаций метода повышения информационной безопасности (ИБ): использование двух виртуальных каналов, использование трех виртуальных каналов в режиме обнаружения нарушителя (ОН) или в режиме исключения нарушителя (ИН).

Показатели для оценки обеспечения ИБ: вероятность успешной атаки MITM $P_{УА,}$ вероятность обнаружения атаки MITM $P_{ОН,}$ вероятность успеш-

ной генерации общего секрета $P_{УК}$. В качестве входного параметра используется $P_{Н1К}$ – вероятность, что нарушитель может выполнять атаку MITM в одном из каналов связи (КС).

В двухканальной модификации – каждый из пользователей подключен к двум КС, по которым организуется взаимодействие корреспондентов. Корреспондент А передает, а респондент Б принимает два одинаковые сообщения Диффи-Хелмана (ДХ) по двум открытым КС. Если респондент получает разные сообщения, значит присутствует нарушитель в КС и протокол завершается неуспешно после отправки ответных сообщений ДХ. Аналогичная проверка выполняется у корреспондента А. Показатели для оценки ИБ определяются по формулам (1)–(3):

$$P_{УА2} = (P_{Н1К})^2, \quad (1)$$

$$P_{ОН2} = 2(1 - P_{Н1К})\, P_{Н1К}, \quad (2)$$

$$P_{УК2} = (1 - P_{Н1К})^2. \quad (3)$$

В трехканальной модификации корреспондент А передает, а респондент Б принимает одинаковые сообщения ДХ по трем КС. Если респондент принимает одинаковые сообщения, он отправляет одинаковые сообщения ДХ и ПРК завершается успешно. Если респондент получает разные сообщения, значит присутствует нарушитель в канале связи и ПРК завершается неуспешно в режиме обнаружения нарушителя после отправки ответных сообщений ДХ. В режиме исключения нарушителя при отличии только одного сообщения от двух других определяется КС, который исключается из дальнейшего обмена сообщениями. Аналогичная проверка выполняется у корреспондента А. Показатели для трехканального ПРК в режиме ОН определяются по формулам (4)–(6):

$$P_{УА3\_ОН} = (P_{Н1К})^3 \quad (4)$$

$$P_{ОН3\_ОН} = 3(1 - P_{Н1К})^2\, P_{Н1К} + 3(1 - P_{Н1К})\, P_{Н1К}^2 \quad (5)$$

$$P_{УК3\_ОН} = (1 - P_{Н1К})^3 \quad (6)$$

Показатели для трехканального протокола в режиме ИН (7)–(9):

$$P_{УА3\_ИН} = (P_{Н1К})^3 + 3(1 - P_{Н1К})\, P_{Н1К}^2 \quad (7)$$

$$P_{ОН3\_ИН} = 3(1 - P_{Н1К})^2\, P_{Н1К} \quad (8)$$

$$P_{УК3\_ИН} = (1 - P_{Н1К})^3 + 3(1 - P_{Н1К})^2\, P_{Н1К} \quad (9)$$

Итоговые графики зависимостей показателей для оценки ИБ приведены на рисунке 1. Модификация протокола, реализующая метод повышения ИБ, представлены на рисунке 2.

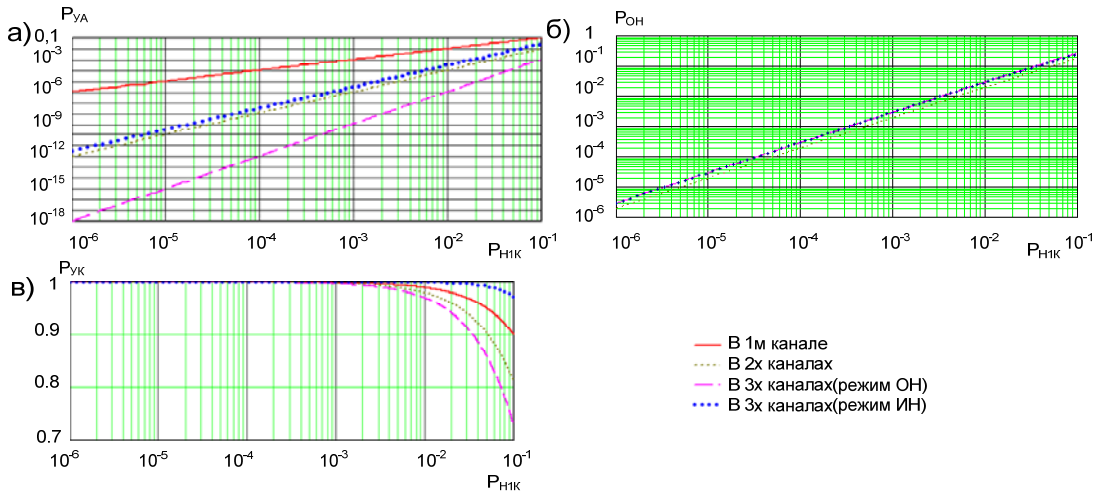


Рис. 1. Сравнительные характеристики ПРК: а) вероятности успешной атаки MITM; б) вероятности обнаружения нарушителя; в) вероятности успешной выработки общего секрета

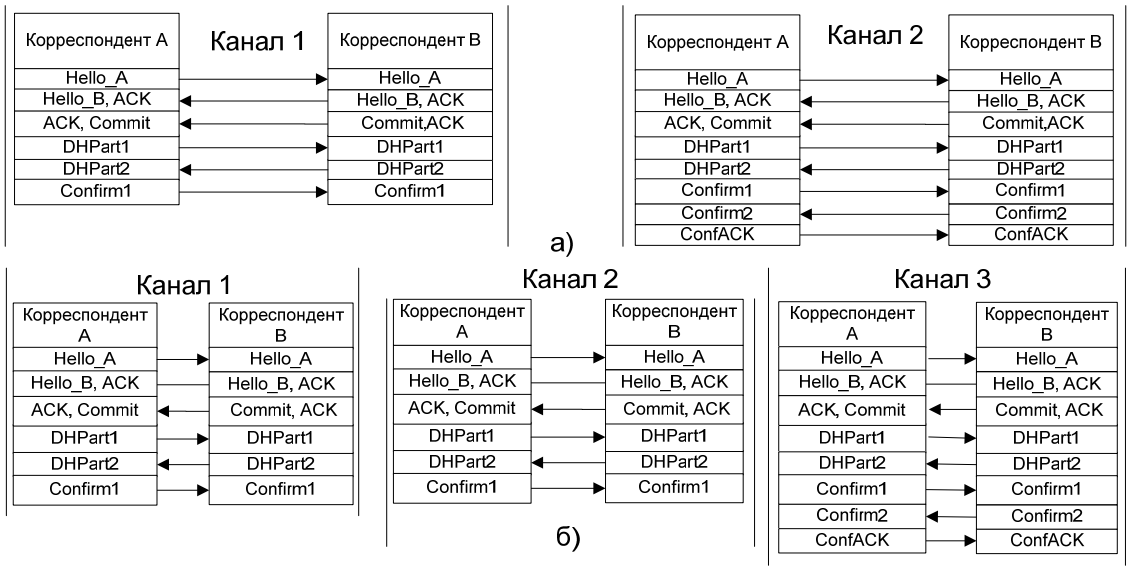


Рис. 2. Вариант взаимодействия корреспондентов при использовании: а) двухканального режима ZRTP; б) трехканального режима ZRTP

Следует отметить, что сообщения Confirm2 и ConfACK отправляются только по каналу связи, который был выбран для работы протокола SRTP.

При использовании предлагаемого метода повышения безопасности важно, чтоб используемые каналы были независимыми, то есть не имели общих точек. Для проверки этого условия предлагается использовать методику оценки вероятности совпадения маршрутов, описанную в [3]. Экспериментальная оценка показала, только 4,9 % из возможных пар и 7,2 % из троек маршрутов имели общие точки между собой. В результате практического эксперимента также не было обнаружено ни одного крупного города, с которым не было бы хоть одной пары маршрутов без общих точек. Можно сделать вывод, что применение двух и более КС, предоставляемых

разными операторами связи, позволяет организовать между абонентами с большой вероятностью два независимых КС.

Для оценки *T*ср предлагается использовать методику, описанную в [4]. Метод улучшения среднего времени выполнения ПРК *T*ср состоит в объединении нескольких фаз. В первой модификации протокола (МП) улучшение *T*ср достигается за счет исключения алгоритма распределения ролей инициатора и респондента. Инициатором в этом случае выступает корреспондент, который первым отправил сообщение протокола ДХ.

Во второй МП дополнительно выполняется объединение информационных данных о поддерживаемых криптографических наборах и информационных блоков ДХ. Обмен сообщениями во второй МП, а также соответствующий вероятностный граф приведены на рисунке 3.

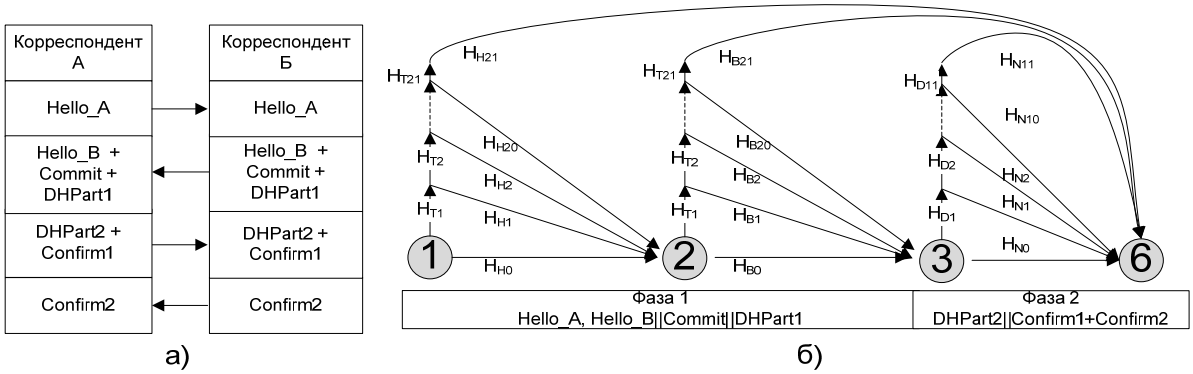


Рис. 3. Вторая модификация протокола: а) сценарий обмена сообщениями; б) вероятностный граф

Выигрыш по сравнению с исходным ZRTP составил от 39,42 % до 48,34 % и представлен в таблице. Сравнение графиков *T*ср исходного протокола ZRTP, первой и второй МП представлено на рисунке 4.

ТАБЛИЦА 1. Оценка выигрыша среднего времени успешного завершения модифицированного ZRTP

Задержка d	50 мс			150 мс			300 мс		
p_0	10^{-5}	$5\cdot10^{-5}$	10^{-4}	10^{-5}	$5\cdot10^{-5}$	10^{-4}	10^{-5}	$5\cdot10^{-5}$	10^{-4}
$T_{прот}$, с	0,52	0,58	0,7	1,3	1,38	1,5	2,5	2,59	2,7
$T_{мод2}$, с	0,315	0,36	0,451	0,715	0,76	0,851	1,315	1,36	1,45
B_{B2}, выигрыш, %	39,42	37,93	35,57	45,0	44,93	43,27	47,4	47,49	46,26

Насколько видно, при $d = 300$ мс и $p_0 < 10^{-4}$ *T*ср < 1,5 для ZRTP. Следует отметить, что при реализации метода повышения безопасности во второй МП – время успешного завершения будет определяться максимальной задержкой, возникающей в этих КС.

Перспективной задачей исследования является доработка решения за счет внедрения элементов стеганографии в предлагаемые методы повышения безопасности.

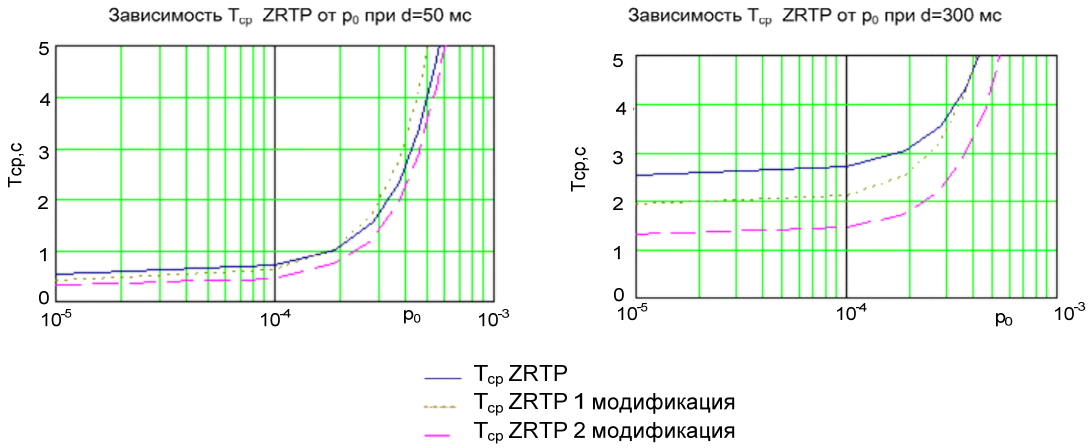


Рис. 4. Сравнение среднего времени успешного завершения оригинального ZRTP, первой и второй модификаций ZRTP: а) при d = 50 мс; б) при d = 300 мс

Список используемых источников

1. Ковцур М. М., Никитин В. Н. Математическая модель активного нарушителя для защищенной IP-телефонии // Актуальные проблемы инфотелекоммуникаций в науке и образовании. IV Международная научно-техническая и научно-методическая конференция: сб. науч. тр. в 2 т. / под. ред. С. В. Бачевского. СПб. : СПбГУТ, 2015. С. 330–335.

2. Ковцур М. М., Никитин В. Н., Юркин Д. В. Протоколы обеспечения безопасности VoIP-телефонии // Защита информации. Инсайд. 2012. № 3. С. 74–81.

3. Ковцур М. М., Никитин В. Н., Юркин Д. В. Повышение защиты протоколов распределения ключей от атак вторжения в середину канала связи // Информационно-управляющие системы. 2014. № 1 (68). С. 70–75.

4. Ковцур М. М., Никитин В. Н., Винель А. В. Исследование вероятностно-временных характеристик протокола распределения ключей защищенной IP-телефонии // Информационно-управляющие системы. 2013. № 1 (62). С. 54–63.

5. Об утверждении Требований к организационно-техническому обеспечению устойчивого функционирования сети связи общего пользования [Электронный ресурс] // приказ Министерства информационных технологий и связи Российской Федерации от 27.09.2007 № 113. Минюст РФ 22 октября 2007 г. N 10380. Доступ из справ.-правовой системы «КонсультантПлюс».

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

УДК 004.021

ИССЛЕДОВАНИЕ МЕТОДОВ ОБНАРУЖЕНИЯ АКУСТИЧЕСКОЙ СТЕГОСИСТЕМЫ, ИСПОЛЬЗУЮЩЕЙ ВЛОЖЕНИЕ ИНФОРМАЦИИ ПРИ ПОМОЩИ ЭХО-СИГНАЛОВ

В. И. Коржик, И. В. Кропивко

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

Разработка стегосистем для передачи сигналов через акустическую среду является достаточно новым и эффективным средством обеспечения информационной безопасности. В статье теоретически и экспериментально исследуются методы обнаружения таких стегосистем с использованием технологии кепстрального анализа. Показывается, что при определенном выборе параметров стегосистемы, эти методы обеспечивают достаточную надежность обнаружения.

стегосистема, аудиосигналы, эхо-сигналы, кепстральный анализ.

Стеганография – это семейство методов, при помощи которых некоторая дополнительная информация погружается в основное сообщение (так называемое покрывающее сообщение) при сохранении хорошего качества покрывающего сообщения [1, 2, 3].

В данной работе были исследованы методы обнаружения такой стегосистемы, параметры которой позволяли бы передавать скрытую информацию с помощью аудиосигнала через акустическую среду. Данную стегосистему можно применять при передаче скрытой информации с помощью аудиосигналов, которые будут воспроизводиться с помощью мегафона. Также данный метод возможен для использования в качестве цифрового водяного знака с целью сохранения подлинности передаваемого сообщения. Схема работы, исследуемой стегосистемы изображена на рисунке 1.

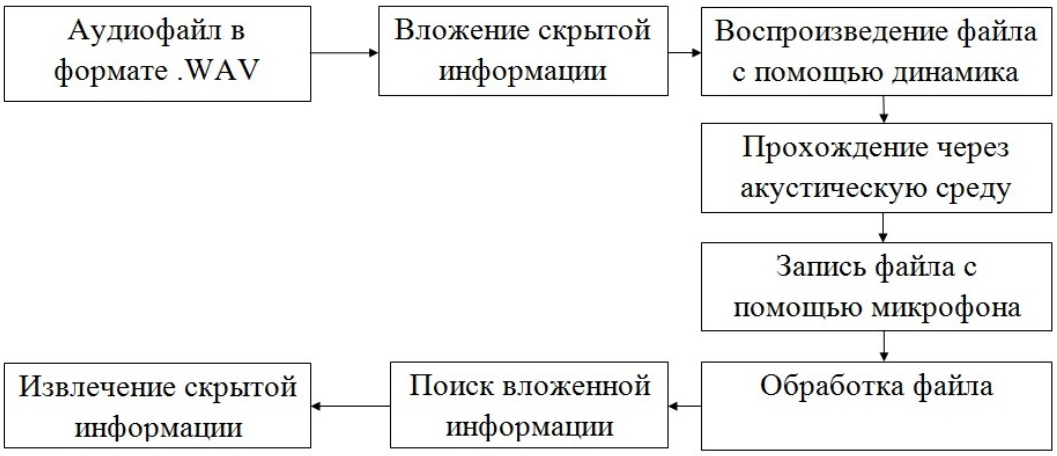
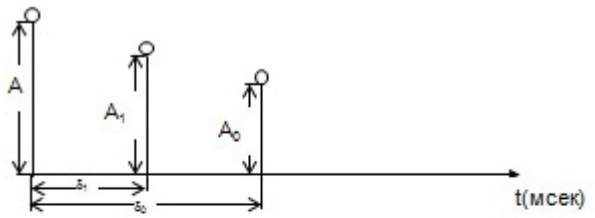


Рис. 1. Схема работы, предложенной стегосистемы

В качестве используемого метода вложения в исследуемой стегосистеме применяется метод, основанный на эхо-сигналах. Он заключается в добавлении «эхо» (сдвинутого по времени сигнала) к основному аудио сигналу. При этом данная «добавка» воспринимается человеком не как добавление аддитивного шума, а как появление дополнительных резонансов (рис. 2).



A – амплитуда исходного сигнала,
A_1 – амплитуда эхо сигнала, соответствующая вложению «1».
A_0 – амплитуда эхо сигнала, соответствующая вложению «0».
δ_1 – задержка эхо-сигнала, соответствующая вложению «1».
δ_0 – задержка эхо-сигнала, соответствующая вложению «0».

Рис. 2. Схема вложения информации с использованием эхо-сигналов

В качестве метода обнаружения подобной стегосистемы используется кепстральный метод приема сигналов. Основная идея кепстрального анализа заключается в том, что свёртка двух сигналов соответствует сумме их кептремов:

$$\tilde{x}(n) = \tilde{S}(n) + \tilde{h}_b(n), \quad \text{n} = 1,2,... \tag{1}$$

При этом сам корреляционный прием сигналов, основанный на кепстреме, определяется следующей формулой:

$$\sum_n \hat{x}(n) \cdot \hat{h}_0(n) \underset{b1}{\overset{b0}{\gtrless}} \sum_n \hat{x}(n) \cdot \hat{h}_1(n). \tag{2}$$

Одним из ключевых факторов при выборе данного метода обнаружения стал тот факт, что в кепстральной области не имеет значения абсолютное значение амплитуды сигнала, которое меняется на протяжении всего сигнала и мешает выбрать порог для правила решения с автокорреляционной функцией.

В ходе исследования был проведен следующий эксперимент. В три различных аудиосигнала было произведено вложение с использованием эхо-сигналов с различными параметрами вложения (глубина вложения, задержка сигнала и количество бит, использующихся для вложения одного

информационного бита). После прохождения акустической среды данный аудиосигнал подвергался кепстральному анализу, при этом у стегоаналитика не было информации о том, было ли осуществлено вложение в данный сигнал.

Рассмотрим алгоритм обнаружения вложения. Согласно принципу Кирхгоффа, нелегитимному пользователю известно о стегосистеме все (включая методы вложения и извлечения), кроме стегоключа. Таким образом, стегоаналитику известны параметры вложения, в том числе и задержка сигнала, на которой осуществляется вложение скрытой информации. После приема аудиосигнала производится вычисление кепстра на всех задержках, на которых целесообразно осуществлять вложение. Целесообразными являются те значения задержки, при которых, с одной стороны, легитимный пользователь может достоверно извлечь вложенную информацию, и, с другой стороны, те значения, при которых эхо будет незаметно для стороннего наблюдателя.

Далее производится анализ полученных значений кепстрема. Данное исследование по обнаружению вложения может осуществляться в графической (рис. 3) или аналитической формах. При аналитической форме исследования необходимо выбрать порог для решения о наличии вложения. В данной работе решение принималось следующим образом: производилось сравнение значения кепстра, при котором могло быть вложение скрытой информации, с близлежащими значениями кепстра (со средним значением ближайших в отношении задержки кепстров) и максимальными значениями кепстра при всех задержках. При условии, что значение кепстра при задержке, на которой осуществлялось вложение, и являлось максимальным, а также значительном превышении ближайших значений кепстра принималось решение о присутствии вложения в аудиосигнале.

Пример параметров при вложении в аудиосигнал, а также получившиеся соотношения при кепстральном анализе представлены в таблице 1.

ТАБЛИЦА 1. Пример параметров при вложении и соотношений при анализе

	CL	QWATC	Penelope
Глубина вложения (α)	0,5	0,5	0,5
Количество используемых бит при вложении одного информационного бита (*N*)	5000	5000	5000
Задержки (σ)	45 и 48	45 и 48	45 и 48
Соотношение между вложениями (%)	84,5	93,5	81,1
Соотношение между значение кепструма вложения и максимальным значением остальных кепструмов (%)	42,6	35,6	33,1

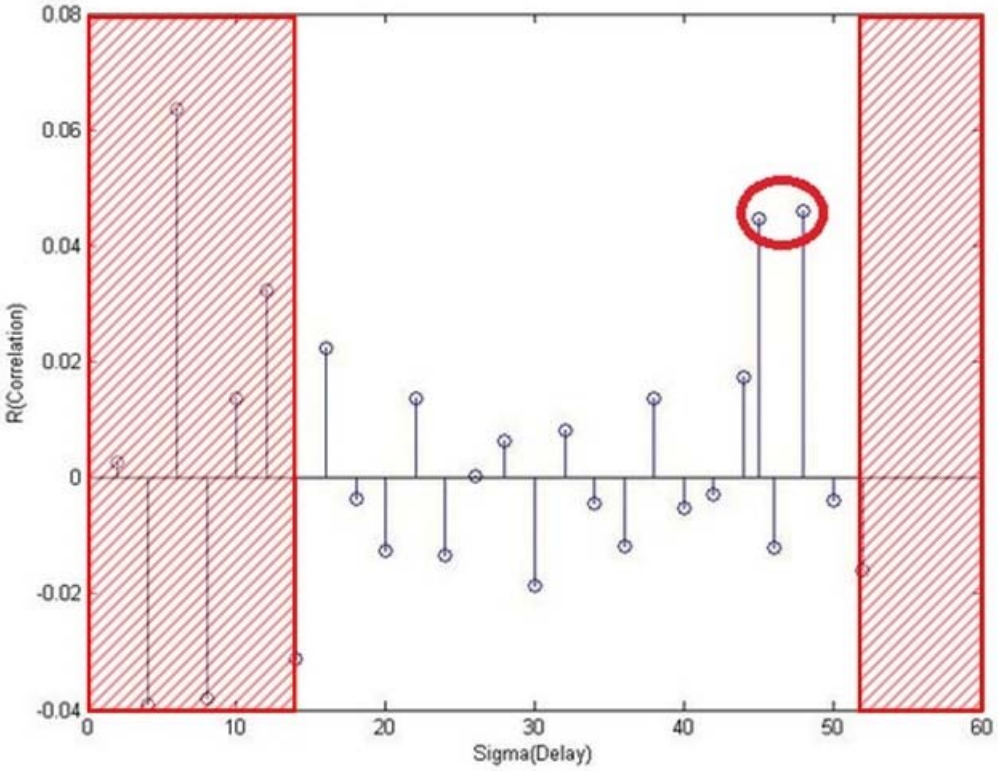


Рис. 3. Значения кепструмов при различных задержках
в одном из исследуемых аудиосигналов

Результаты эксперимента по обнаружению вложения представлены в таблицах 2 и 3.

ТАБЛИЦА 2. Статистика обнаружения по аудиофайлам

	CL	QWATC	Penelope
Вероятность ложного обнаружения (%)	2,29	0,43	2,71
Вероятность пропуска (%)	14,29	14,29	0,00

ТАБЛИЦА 3. Общая статистика

Вероятность ложного обнаружения (%)	1,81
Вероятность пропуска (%)	9,52

Как видно из приведенных выше таблиц, эксперимент завершился успешно. Вероятность ложного обнаружения получилась достаточно низкой для любых параметров вложения. Вероятность пропуска стегосигнала получилась несколько выше, однако данный факт объясняется тем, что ошибка подобного типа при проведении эксперимента происходила при самых минимальных параметрах вложения. Условно говоря, ошибка происходила в случаях, когда и легитимный пользователь, зная о вложении и зная

в точности параметры вложения, может ошибочно извлечь данные вследствие искажения сигнала после прохождения через акустическую среду и вследствие подобных параметров вложения.

Подводя итоги, следует сказать, что предложенный метод по обнаружению акустической стегосистемы, использующей вложение информации при помощи эхо-сигналов по результатам теоретического и практического исследования подходит для обозначенных целей и при соответствующих параметрах вложения в аудиосигнал обеспечивает надежное извлечение информации из покрывающего сообщения.

Список используемых источников

1. Коржик В. И., Алексеев В. Г., Федянин И. А. Выделение цифровых “водяных” знаков из аудиосигналов с использованием методов кепстрального анализа // 63-я научно-техническая конференция профессорского-преподавательского состава, научных сотрудников и аспирантов : материалы; ГОУВПО СПбГУТ. СПб., 2011. С. 225.

2. Bender W., Gruhl D., and Lu A. Echo Hiding // Lecture Notes in Computer Science, 1996.

3. Donald G. Childers, David P. Skinner, and Robert C. Kemerait. The Cepstrum: A Guide to Processing // Proceedings of IEEE, vol. 65, no 10, October 1977.

УДК 004.021

МЕТОД ОБНАРУЖЕНИЯ СТЕГОСИСТЕМ НА ОСНОВЕ АНАЛИЗА СТАТИСТИКИ КРИПТОГРАММ, ФОРМИРУЕМЫХ ПРИ ШИФРОВАНИИ ВКЛАДЫВАЕМЫХ СООБЩЕНИЙ

В. И. Коржик, М. В. Токарева

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

Предполагается новая системная атака обнаружения стегосистем цифровых изображений. При известном алгоритме извлечения вложенной информации, решение о наличии стегосистемы принимается после анализа статистики извлеченных последовательностей если она удовлетворяет критериям псевдослучайности по критериям NIST. Приводятся результаты экспериментальных исследований, подтверждающие возможности такой атаки.

стегосистема, криптограмма, цифровое изображение, критерии псевдослучайности NIST.

Стегосистемы (СГ) являются важной частью информационной безопасности (ИБ), поскольку они позволяют скрыть от нелегитимных пользователей не только содержание конфиденциальных сообщений (подобно крипто-

графии), но и сам факт присутствия скрытых вложений в «невинных» покрывающих объектах (ПО). В качестве покрывающих объектов могут быть использованы: аудио и видео цифровые сигналы, обычные текстовые сообщения и др. В настоящем докладе, мы ограничиваемся для простоты изложения, только неподвижными цифровыми изображениями (ЦИ).

Помимо собственно СГ важной частью ИБ является стегоанализ (СГА), т. е. методы обнаружения присутствия СГ в ПО, поскольку это обеспечивает защиту от несанкционированной передачи информации за допустимые пределы корпораций. (В этом случае СГА оказывается важным дополнением к системе Data Loss Prevention (DLP) [1], обеспечивая защиту от промышленного шпионажа, осуществляемого, например, путем скрытия вложения конфиденциальной информации в электронную почту).

Описанию методов СГА посвящена обширная литература, при чем более полные сведения для ПО в виде неподвижных изображений изложены в монографии [2]. Однако, эту проблему нельзя считать полностью решенной особенно для таких случаев построения СГ, как [2]: матричное вложение, ±1НЗБ вложение, вложение с использованием широкополосных сигналов и адаптивное квантование.

В настоящем докладе мы рассмотрим пока только лишь метод НЗБ с различными скоростями вложения. Напомним, что при данном методе в цветовую компоненту яркости каждого пикселя ЦИ, которая для стандарта RGB отображается цепочкой из 8-ми бит, производится вложение секретной информации при помощи замены наименьшего значащего бита (НЗБ) каждого пикселя бита битом секретной информации.

Согласно условию Кирхгофа [3], распространенного от криптографии на стеганографию, о СГ должны быть известны алгоритм вложения и извлечения информации, за исключением крипто- и стегоключей. При выполнении этого условия, вкладываемая информация должна быть предварительно зашифрована на неизвестном атакующему ключе, иначе стегоаналитик может, следуя известному ему методу извлечения, извлечь вложенные данные и обнаружить присутствие СГ, если эти данные будут иметь смысловой характер. При отсутствии же вложения, выделенные данные будут выглядеть «хаотично», что и является признаком отсутствия какого-либо вложения в данное ПО. Очевидно, что используемый шифр должен быть достаточно устойчивым ко взлому (при неизвестном ключе), иначе, как было отмечено вначале, задача СГА становится тривиальной для любого алгоритма вложения.

С другой стороны, для криптограмм, полученных с использованием стойкого шифра, должны выполняться критерии их псевдослучайности (т. е. сходства с чисто случайными последовательностями). Эти условия были впервые сформулированы С. Голомбом [3], а в дальнейшем уточнены и расширены в списке, так называемых, NIST критериев [4].

В таблице 1 приведен список тестов с нумерацией, которая будет использована в дальнейшем.

Таблица 1. Тесты NIST на псевдослучайность последовательностей

№	Тест
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 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 Approximate Entropy Test
12	The Cumulative Sums Test
13	The Serial Test
14	The Random Excursions Test
15	The Random Excursions Variant Test

Теперь мы можем сформулировать принцип новой системной СГА следующим образом: *Если в данный ПО было произведено погружение информации, то анализ извлеченной последовательности должен удовлетворять критериям NIST на псевдослучайность. Если же вложение не производилось, то все критерии NIST не будут удовлетворяться.*

Действительно, первая часть этой гипотезы основывается на стойкости метода шифрования. Что же касается второй части, то маловероятно, что чисто случайная последовательность, выделенная, например, из НЗБ яркостей пикселей изображения, удовлетворяет всем NIST критериям псевдослучайности.

В таблице 2 и 3 приведены результаты тестирования NIST в случае НЗБ вложения с шифрованием при использовании блочного шифра ГОСТ-28147-89, а также без вложения в эти же изображения, соответственно.

Таблица 2. Результаты NIST тестирования при полном НЗБ вложении в 15 различных изображений с использованием шифра ГОСТ-28147-89

Тест	1 *lsb*	2 *lsb*	3 *lsb*	4 *lsb*	5 l*sb*	6 *lsb*	7 *lsb*	8 *lsb*	9 *lsb*	10 *lsb*	11 *lsb*	12 *lsb*	13 *lsb*	14 *lsb*	15 *lsb*
1															
2															
3															
4															
5															
6															
7															
8															
9															
10															
11															
12															
13															
14															
15															

Таблица 3. Результаты NIST тестирования при отсутствии вложения в 15 различных изображений

Тест	1 lsb	2 lsb	3 lsb	4 lsb	5 lsb	6 lsb	7 lsb	8 lsb	9 lsb	10 lsb	11 lsb	12 lsb	13 lsb	14 lsb	15 lsb
1															
2															
3															
4															
5															
6															
7															
8															
9															
10															
11															
12															
13															
14															
15															

Серым цветом отмечены случаи прохождения теста, а белым – отсутствие прохождения. (Аналогичные результаты были получены и при использовании шифра DES).

Однако следует отметить, что помимо «полного» НЗБ вложения в каждый пиксель изображения, часто используется вложение в часть пикселей.

В частности, можно производить вложение только в пиксели, выбираемые по секретному стегоключу.

Если стегоаналитик не может вскрыть данный ключ, то для него подобная ситуация представляется моделью, когда в каждый пиксель производится вложение случайно, с некоторой вероятностью P, и не производится вложение с вероятностью 1 – P.

Результаты NIST тестирования при P = 0,6 и использовании шифра ГОСТ-28147-89 представлены в таблице 4.

Таблица 4. Результаты NIST тестирования при использовании НЗБ вложения с вероятностью вложения в пиксель P = 0,6 криптограммы шифра ГОСТ в 15 различных изображений

Тест	1 lsb	2 lsb	3 lsb	4 lsb	5 lsb	6 lsb	7 lsb	8 lsb	9 lsb	10 lsb	11 lsb	12 lsb	13 lsb	14 lsb	15 lsb
1	■	■			■						■		■		■
2	■	■									■		■		■
3	■	■			■						■		■		■
4	■	■	■		■	■	■			■	■		■		■
5	■	■	■	■	■	■	■	■	■	■	■		■		■
6	■	■			■	■	■		■	■	■		■		■
7	■	■			■	■	■				■		■		■
8	■	■				■	■			■	■		■		■
9	■	■				■	■			■	■		■		■
10	■	■	■	■	■	■	■	■	■	■	■	■	■	■	■
11	■	■					■			■	■				■
12	■	■			■						■		■		■
13		■			■		■				■		■		
14					■										
15					■										

Сравнивая таблицу 4 с таблицей 3, видим, что они стали ближе друг к другу, но все еще возможно отличить случай СГ и ПО. Наши эксперименты (не представленные в настоящем статье из-за ограничения на его объем) показали, что достаточно просто отличить СГ от ПО при вероятности $P \geq 0{,}5$, а при P = 0,1 это становится практически невозможным для большинства изображений, поскольку большие сложности возникают с выбором порогов для прошедших тестов, при прохождении которых принимается решение о наличии СГ.

В настоящее время нами прорабатывается подход с использованием алгоритма с опорными векторами (метод SVM [5]).

Список используемых источников

1. Википедия. Предотвращение утечек информации [Электронный ресурс] // URL: https://ru.wikipedia.org/wiki/Предотвращение_утечек_информации, 12.10.2015.

2. Fridrich J. Steganography in digital media // Cambridge University Press, 2009. 466 p. ISBN-10: 0521190193, ISBN-13: 978-0521190190.Коржик В. И., Просихин В. П., Яковлев В. А. Основы криптографии : учебн. пособие. С.-Петерб. гос. ун-т телекоммуникаций им. М. А. Бонч-Бруевича. 2-е изд. СПб. : СПбГУТ, 2014. 275 с. : ил. ISBN 978-5-89160-097-3.

3. Revision1a, A Statistical Test Suite for Random and Pseudorandom Numb / Andrew Rukhin, Juan Soto, James Nechvatal, Miles Smid, Elaine Barker, Stefan Leigh, Mark Levenson, Mark Vangel, David Banks, Alan Heckert, James Dray, SanVo // NIST SP 800-22, 2010.

4. Pevny T., Filler T., Bas P. Using high-dimensional image models to perform highly un-detectable steganography // IH'10 Proceedings of the 12th international conference on Information hiding. – Heidelberg : Springer-Verlag Berlin, 2010. PP. 161–177.

УДК 621.39

ИССЛЕДОВАНИЕ ЭРБИЕВОГО УСИЛИТЕЛЯ

В. С. Кузнецов, В. Р. Сумкин

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

Целью работы является исследование спроектированного авторами оптического усилителя EDFA. В статье рассмотрены принципы работы и применение усилителей EDFA, проведены исследования зависимости параметров усилителя при изменении уровня мощности входного сигнала, сигнала накачки, длины эрбиевого волоконного световода.

оптический усилитель, волоконный световод, сигнал накачки, мощность сигнала, длина волны, усиленное спонтанное излучение, коэффициент усиления, пороговая мощность.

В настоящее время оптические усилители (ОУ) EDFA (*Erbium Doped Fiber Amplifier)* являются важной составляющей магистральных волоконно-оптических систем связи с плотным спектральным мультиплексированием DWDM (*Dense Wavelength Division Multiplexing*).

ОУ EDFA обеспечивают непосредственное усиление оптических сигналов без их преобразования в электрические сигналы и обратно, при этом обладают низким уровнем шумов. Благодаря ОУ EDFA системы DWDM стали экономически привлекательными [1].

В зависимости от применения, различают предварительные ОУ, линейные ОУ и бустеры [2]. Предварительные ОУ устанавливаются на входе оптоэлектронного каскада усиления приемника регенератора и способствуют увеличению отношения сигнал/шум в оптоэлектронном блоке приемника. Линейные ОУ устанавливаются в промежуточных точках протяженных линий связи между регенераторами. Бустеры устанавливаются после передатчиков и предназначены для дополнительного увеличения

мощности сигнала, поступающего в линию. Целью данной работы было исследование параметров предварительного ОУ EDFA. Основными требованиями к предварительным ОУ являются низкий уровень пороговой мощности, при котором на приемной стороне регенератор сможет с допустимым коэффициентом ошибок выделить полезный сигнал на фоне шума, а также высокий коэффициент усиления.

ОУ построен по схеме со встречной накачкой эрбиевого волоконного световода ЭВС (рис. 1), где:

– ЛД-980 – лазерный диод накачки на длине волны λ = 980 нм;
– МП – мультиплексор 980/1550 нм;
– ЭВС – волоконный световод НЕ-980, легированный ионами эрбия;
– ОИ – оптический изолятор.

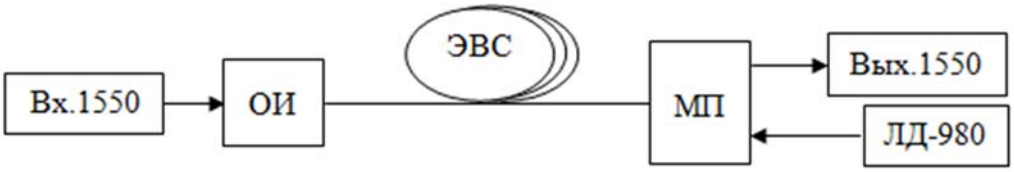


Рис. 1. Схема ОУ EDFA со встречной накачкой

При выполнении данной работы использовался ЛД-980 с возможностью установки заданных значений мощности накачки p_p: 19, 20, 21, и 22 дБм. Длина ЭВС составляла $l_{ЭВС}$ = 7, 10, 13 м.

Для проведения исследований в работе были использованы:

– оптический анализатор спектра AQ6370C;
– измеритель оптической мощности РУБИН 202;
– регулируемый оптический аттенюатор АОИ-3;
– источник оптического излучения ОТМ-1-1550 нм.

В исследование ОУ входила задача измерения уровня усиленного спонтанного излучения p_{ase} (*Amplified Spontaneous Emission*) от $l_{ЭВС}$ при различных p_p. Ниже представлены пример спектрограммы ОУ EDFA с $l_{ЭВС}$ = 13 м при отсутствии входного сигнала (p_{in}) и при p_p = 22 дБм (рис. 2), а также таблица с зависимостью p_{ASE} от $l_{ЭВС}$ и p_p (табл. 1).

ТАБЛИЦА 1. Зависимость p_{ASE} от $l_{ЭВС}$ и p_p

$l_{ЭВС}$, м	p_{ASE1}, дБм	p_{ASE2}, дБм	p_{ASE3}, дБм	p_{ASE4}, дБм
7	−23,90	−23,76	−23,68	−23,60
10	−9,94	−9,45	−9,22	−8,90
13	−5,79	−4,49	−3,81	−2,92

p_{ASEi} – уровень мощности ASE при p_p = 19, 20, 21 и 22 дБм, дБм.

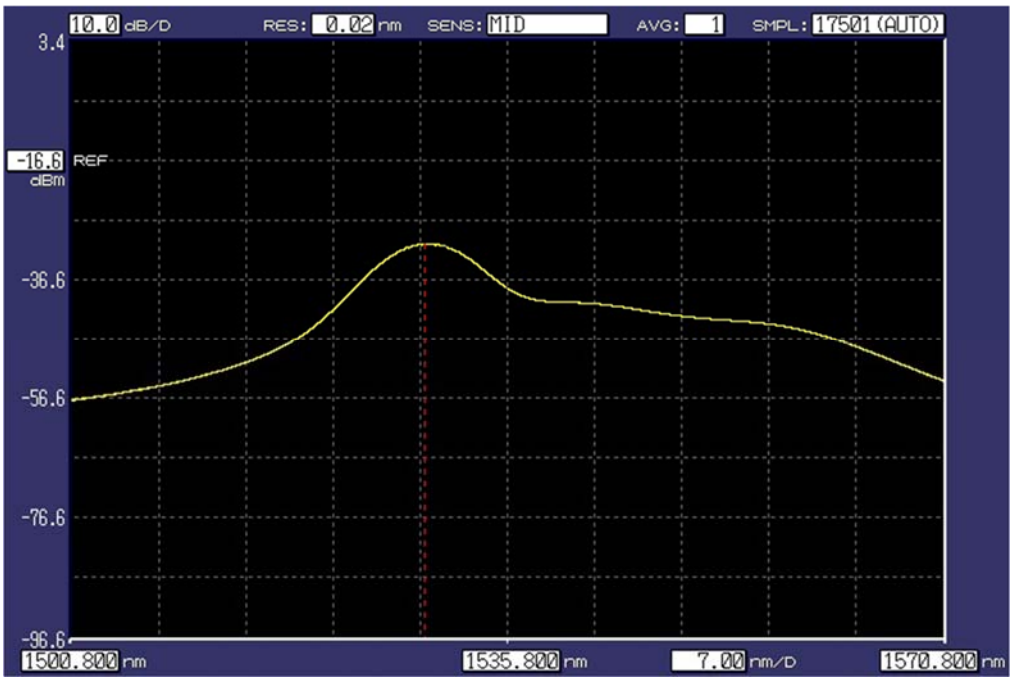


Рис. 2. Спектрограмма ASE при p_p = 22 дБм и $l_{ЭВС}$ = 13 м

Дальнейшие эксперименты проводились при наличии p_{in}, в качестве которого использовался источник излучения на длине волны λ = 1550 нм с изменением уровня мощности p_{in} с помощью аттенюатора от −15 дБм до −60 дБм. Данные экспериментов помещены в таблицы 2–4.

ТАБЛИЦА 2. Результаты экспериментов для $l_{ЭВС}$ = 7 м

p_{in}, дБм	p_{out1}, дБм	p_{out2}, дБм	p_{out3}, дБм	p_{out4}, дБм
−15	−11,15	−10,95	−10,89	−10,71
−20	−15,51	−15,4	−15,23	−15,03
−25	−19,34	−18,94	−18,90	−18,87
−30	−21,72	−21,58	−21,57	−21,51
−35	−22,99	−22,88	−22,86	−22,78
−40	−23,57	−23,44	−23,38	−23,30

ТАБЛИЦА 3. Результаты экспериментов для $l_{ЭВС}$ = 10 м

p_{in}, дБм	p_{out1}, дБм	p_{out2}, дБм	p_{out3}, дБм	p_{out4}, дБм
−15	0,45	0,63	0,87	1,39
−20	−3,74	−3,16	−2,85	−2,49
−25	−6,76	−6,20	−5,93	−5,63
−30	−8,76	−8,21	−7,93	−7,59

p_{in}, дБм	p_{out1}, дБм	p_{out2}, дБм	p_{out3}, дБм	p_{out4}, дБм
−35	−9,58	−9,04	−8,77	−8,44
−40	−9,87	−9,34	−9,07	−8,73

ТАБЛИЦА 4. Результаты экспериментов для $l_{ЭВС}$ = 13 м

p_{in}, дБм	p_{out1}, дБм	p_{out2}, дБм	p_{out3}, дБм	p_{out4}, дБм
−15	1,21	2,70	3,42	4,53
−20	−1,13	0,16	0,88	1,87
−25	−3,44	−2,17	−1,53	−0,62
−30	−4,89	−3,60	−2,91	−2,02
−35	−5,58	−4,28	−3,62	−2,68
−40	−5,85	−4,56	−3,88	−2,94
−45	−5,98	−4,67	−3,96	−3,04
−50	−6,04	−4,72	−4,02	−3,06
−60	−6,07	−4,80	−4,08	−3,12

Для наглядности результаты по таблице 4 представлены в виде графиков (рис. 3).

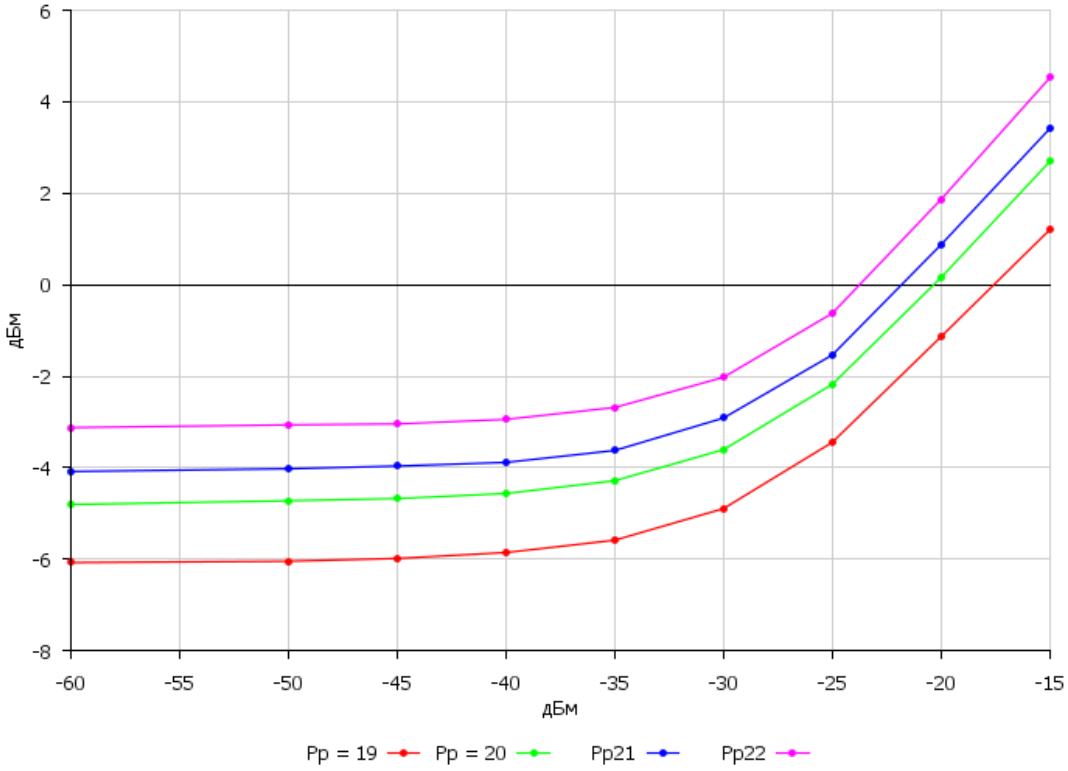


Рис. 3. График зависимости выходного сигнала от входного при $l_{ЭВС}$ = 13 м при различных p_p

Пример спектрограммы при p_{in} = −30 дБм, p_p = 22 дБм и $l_{ЭВС}$ = 13 м представлен на рисунке 4.

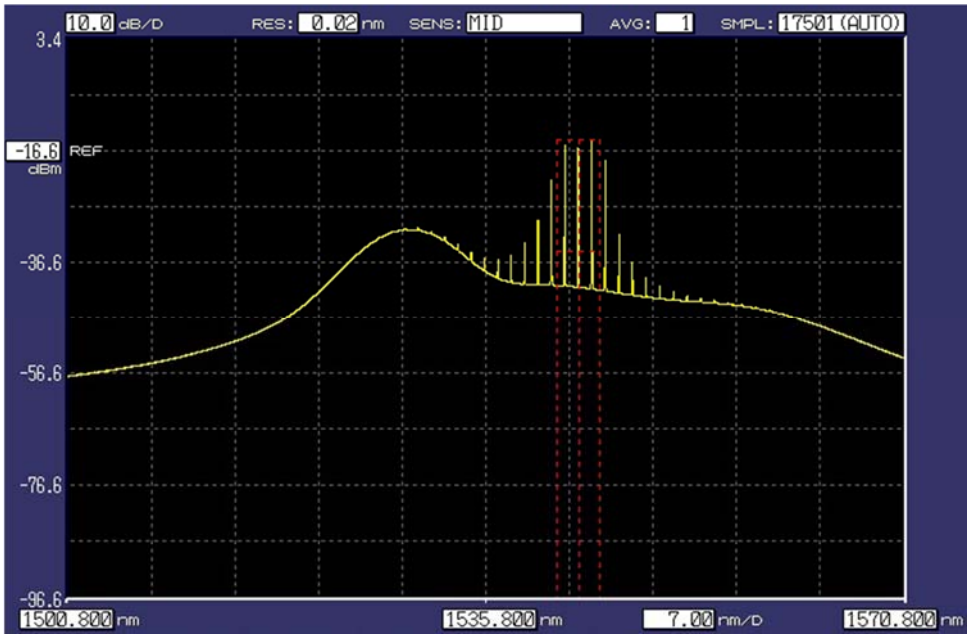


Рис. 4. Спектрограмма при уровне мощности входного сигнала p_{in} = −30 дБм, p_p = 22 дБм и $l_{ЭВС}$ = 13 м

При $l_{ЭВС}$ = 13 м, p_{in} = −60 дБм и p_p = 22 дБм на спектрограмме полезный сигнал мало, но всё ещё различим на фоне ASE:

Рис. 5. Пример спектрограммы при p_{in} = −60 дБм, p_p = 22 дБм и $l_{ЭВС}$ = 13 м

В результате проведения исследований были получены оптимальные значения $l_{ЭВС}$ и p_p , при которых значение пороговой мощности составляет −60 дБм, а коэффициент усиления – 20 дБ, высчитываемый как разница между p_{in} и уровнем мощности сигнала по спектрограмме (рис. 5). Таким образом, данный ОУ EDFA соответствует требованиям, предъявляемым к предварительным ОУ.

Список используемых источников

1. Листвин В. Н., Трещиков В. Н. DWDM системы : научное издание. М. : Издательский дом «Наука», 2013. 300 с. ISBN 978-5-9902333-6-2.

2. Усиление оптических сигналов. [Электронный ресурс] // Сайт ООО «Проинтех». URL: http://www.prointech.ru/kb/usiliteli-i-mediakonvertery/usilenie-opticheskikh-signalov.html (дата обращения 30.03.2016).

Статья представлена заведующим кафедрой, кандидатом технических наук, доцентом С. Ф. Глаголевым.

УДК 004.49.5

СПОСОБ УПРАВЛЕНИЯ ИНФОРМАЦИОННО-ВЫЧИСЛИТЕЛЬНОЙ СЕТЬЮ НА ОСНОВЕ КРАТКОСРОЧНОГО ПРОГНОЗИРОВАНИЯ РАСПРОСТРАНЕНИЯ КОМПЬЮТЕРНОГО ВИРУСА

И. А. Кузнецов[1], В. А. Липатников[1], Д. В. Сахаров[2]

[1]Военная академия связи им. Маршала Советского Союза С. М. Буденного

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

В статье изложен способ управления информационно- вычислительной сетью на основе краткосрочного прогнозирования распространения компьютерного вируса, разработанный на основе применения модели распространения эпидемиологических заболеваний, а также одного из методов управления с использованием прогнозирующих моделей.

информационно-вычислительная сеть; компьютерный вирус; защита информации; управление с применением прогнозирующих моделей; Model Predictive Control (MPC); State-Space Model Predictive Control (SSMPC); SSMPC; ЗИ; ИВС; МРС; модель пространства состояний, эпидемиологическая модель.

Требуется разработать способ управления ИВС на основе краткосрочного прогнозирования распространения компьютерного вируса.

Одним из преимуществ методологии управления с использованием прогнозирующих моделей является возможность исследования многофакторного процесса в опережающем режиме. В связи с чем, на основе анализа [1], выбран метод прогнозирования на основе модели пространства состояний: State-Space Model Predictive Control (SSMPC).

Для применения метода SSMPC необходимо составить математическую модель объекта управления, в последствии использующуюся для предсказания выходных данных ИВС на основе прошлых и текущих значений (величин) и предполагаемых оптимальных управляющих воздействий в будущем. Эти воздействия вычисляются оптимизатором, который также учитывает критерий качества (где принимаются во внимание ошибки в будущем) и ограничения, накладываемые на переменные процесса, описывающего объект управления.

Выбранная модель должна охватывать динамику процесса для точного предсказания будущих выходных значений, быть простой для внедрения и понимания.

Процесс распространения вредоносного кода в ИВС на промежутке времени $[0, T]$ описывается с помощью эпидемиологической модели в следующих предположениях [2]:

1) N-общее количество машин в ИВС. ИВС, состоящая из N узлов может быть описана матрицей вида $G = \{0,1\}^{N^2}$:

$$G_{ij} = \begin{cases} 1, \text{если узлы } i \text{ и } j \text{ связаны между собой,} \\ 0, \text{ если узлы } i \text{ и } j \text{ не связаны.} \end{cases}$$

2) Произвольный узел сети может находится в одном из трех состояний: уязвимом S, инфицированном I и невосприимчивом R.

3) Распространение копии вредоносной программы описывается с помощью функции $f(S(t),\ I(t),\ R(t), B,\ \bar{t}_{\text{восст}},\ P_{\text{пор. уз. сети}},\ \bar{t}_{\text{зар. уз. сети}})$, где $S(t)$ – количество уязвимых узлов сети, $I(t)$ – количество инфицированных узлов сети, $R(t)$ – количество невосприимчивых узлов сети, $B = \left(\beta^1(t), \dots, \beta^m(t)\right)$ – вектор известных нарушителю параметров сети, $P_{\text{пор. уз. сети}}$ – вероятность поражения уязвимого узла сети, $\bar{t}_{\text{восст}}$ – среднее время, требуемое для перехода узла из уязвимого или инфицированного состояния в невосприимчивое, $\bar{t}_{\text{зар. уз. сети}}$ – среднее время, требующееся нарушителю (либо само распространяющемуся вредоносному коду) для инфицирования уязвимого узла ИВС.

4) Вирус размножается по сети без участия пользователя, и повторное заражение узла одним и тем же вирусом невозможно.

5) В реальных условиях лечение компьютера происходит за счет установки или обновления антивирусного программного обеспечения или установки/настройки межсетевых экранов. При этом вектор оптимальных

управляющих воздействий $U(t) = (u_1(t), \dots, u_n(t))$ характеризует пропорциональное удаление уязвимых узлов или связей в ИВС [3, 4].

В простейшем случае β определяется средней скоростью сканирования сети вредоносной программой (v_s) и размером ее адресного пространства (N_{ip}) [8]:

$$\beta = v_s \times \frac{N}{N_{ip}}.$$

На основе анализа данной модели можно сделать следующие выводы:

1) Распространение эпидемии возможно только в том случае, если $R_0 = \frac{\beta}{g} > 1$;

2) $S(t)$, $I(t)$, $R(t)$ – монотонно возрастающая, монотонно убывающая и унимодальная функции соответственно.

Уравнения, используемые в [4], позволяют более точно описывать состояние ИВС, уходя от традиционного подхода, описывающего только состояния во времени отдельных узлов ИВС, что позволяет более обширно оценить темп и площадь распространения вредоносного программного обеспечения. В описании модели процесса будем использовать уравнения, описывающие процесс появления и изменения во времени числа (состояния) пар узлов [AB], а также троек узлов [ABC], где A и B принимают значения из множества $\{S, I, R\}$. Введем следующие параметры: τ – характеризует темп распространения инфекции, связанный с контактом инфицированного узла с уязвимым, n – среднее число узлов-соседей, приходящее на один узел, ϕ – величина, характеризующая отношение количества треугольников к тройкам. ϕ является мерой взаимосвязанности локальных узлов-соседей. Если значение ϕ – большое, то можно сказать, что элементы пары (вершины) будут соединены с большим количеством общих узлов, в случае если ϕ – мало, что можно сказать, что в сети преобладают соединения, предназначенные для передачи информации на дальние расстояния. Параметры n и ϕ надлежащим образом характеризуют базовую структуру сети [5, 6].

Исходя из данной модели возможно существование девяти различных пар узлов, однако, исключив симметрию, введем следующие необходимые дифференциальные управления для описания состояния заражения ИВС [5]:

$$[\dot{SS}] = -2\tau[SSI];$$
$$[\dot{SI}] = \tau([SSI] - [ISI] - [SI]) - g[SI];$$
$$[\dot{SR}] = -\tau[RSI] + g[SI];$$
$$[\dot{II}] = 2\tau([ISI] + [SI]) - 2g[II];$$
$$[\dot{IR}] = \tau[RSI] + g([II] - [IR]);$$
$$[ABC] \approx \frac{(n-1)N}{n^2}\frac{[AB][BC][AC]}{[A][B][C]}.$$

Согласно [8] развитие эпидемии, вызванной распространением вредоносного ПО на узлы и персональные компьютеры ИВС можно разделить на три этапа:

1) Сравнительно медленное (но тем не менее экспоненциальное) нарастание зараженности (коэффициента зараженности) до порогового уровня 0,05, определяемого как $k_{\text{зараж.}} = \frac{I}{N}$. Скорость удвоения доли пораженных машин равна $\ln(2)/\beta$.

2) Взрывная фаза в диапазоне $0{,}05 < k_{\text{зараж.}} < 0{,}95$. Продолжительность определяется приблизительно равна $5{,}89/\beta$.

3) Насыщение, $k_{\text{зараж.}} > 0{,}95$. На этом участке при случайном сканировании адресного пространства зараженные узлы контактируют преимущественно друг с другом, поэтому уцелевшие узлы могут оставаться «чистыми» неопределенно продолжительное время.

Для достижения порога насыщения $k_{\text{зараж.}}$=0,95 требуется время

$$\frac{1}{\beta}\ln\left[19\left(\frac{1}{k_{\text{зараж. нач.}}}\right)-1\right],$$

где $k_{\text{зараж. нач.}}$ – зараженность ИВС в начальный момент времени t_0.

Из приведенных данных можно сделать вывод, что безопасным состоянием сети можно считать состояние, в котором доля зараженных компьютеров или узлов сети не будет превышать 5 % [5, 6].

Расчет закона управления с помощью метода SSMPC включает в себя следующую последовательность действий. На каждом шаге алгоритма SSMPC для горизонта прогнозирования фиксированной длины вычисляется последовательности управляющих воздействий на основе минимизации целевой функции, включающей в себя вычисленные выходные данные системы для момента времени $(t+1)$. Оптимизация данной функции представляет собой задачу нелинейного программирования, которая решается относительно ограничений, наложенных на входные и выходные сигналы системы. Управляющая последовательность передается органу управления, далее, горизонт прогнозирования сдвигается на шаг вперед, и подсчитываются следующие управляющие воздействия. Данная методика получила название «Управление с использованием удаляющегося горизонта прогнозирования» (*Receiding Horizon Control*) [6].

Алгоритм способа управления сетью на основе краткосрочного прогнозирования распространения КВ представлен на рисунке:

Использование данного алгоритма позволяет генерировать управляющие воздействия, согласно заданным целям (доля зараженных узлов не должна превышать 5 %) при этом учитывается распространение вируса по сети в режиме реального времени, на каждом шаге управления учитываются актуальные данные распространения КВ по узлам сети. При этом в расчете закона управления используется прогнозирование эпидемии вируса,

и полученные управляющие значения обеспечивают так называемое проактивное управление, что позволяет заранее принимать эффективные меры противодействия распространению КВ, а не реагировать на ситуацию только после очередного шага злоумышленника или угроз, реализованных вредоносным ПО.

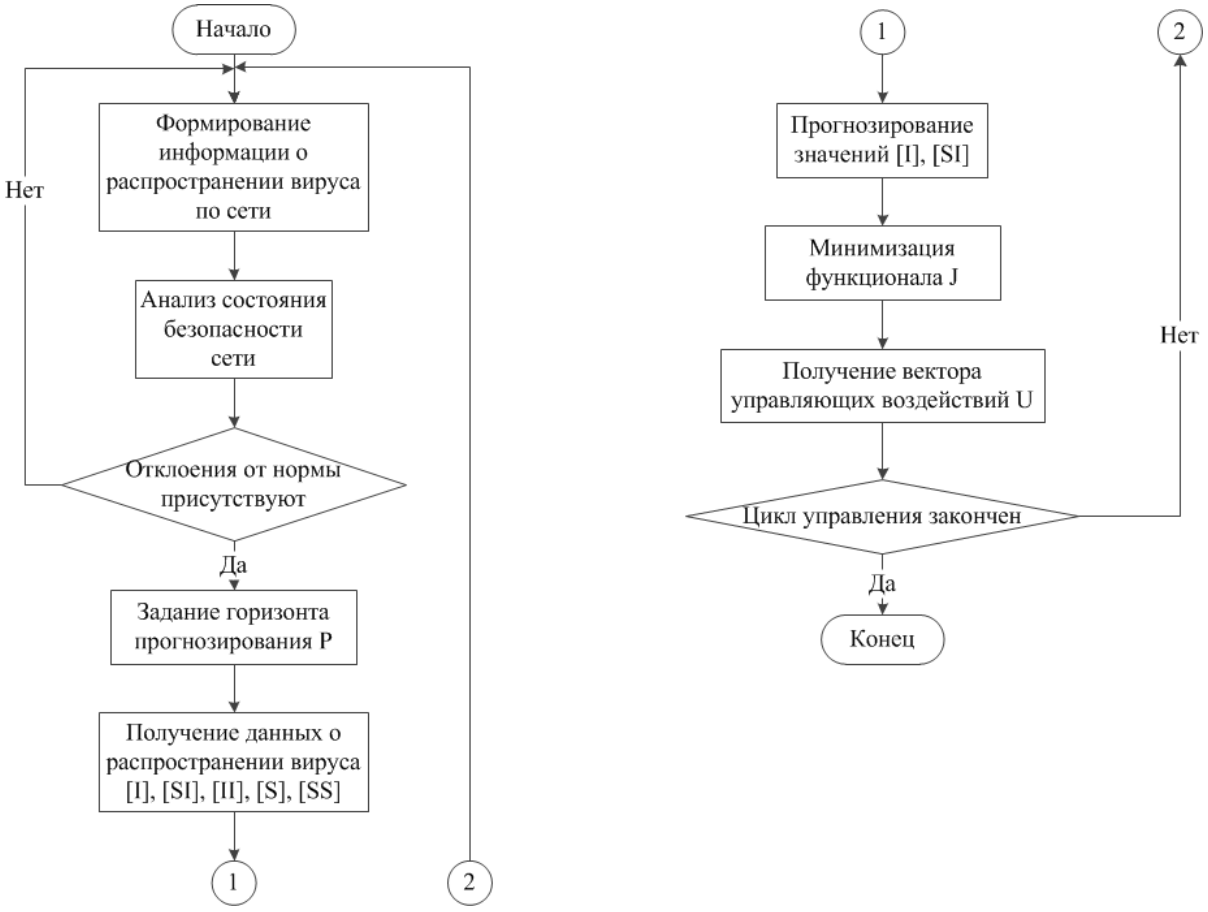


Рисунок. Алгоритм способа управления ИВС
на основе краткосрочного прогнозирования распространения КВ

В заключении можно сказать, что:

1. Описана модель распространение КВ по узлам сети на основе модели распространения эпидемиологических заболеваний, учитывающая не только скорость прироста инфицированных и уязвимых компьютеров, но число связей зараженных и уязвимых узлов.

2. Представлен цикл управления сетью с использованием прогнозирования распространения вредоносного кода по сети.

3. Составлен критерий безопасного сети на основе анализа темпа распространения вируса по сети.

4. Предложен способ управления ИВС на основе краткосрочного прогнозирования распространения КВ.

Список используемых источников

1. Rohloff K. Stochastic Behavior of Random Constant Scanning Worms // Computer Communications and Networks, 2005. ICCCN 2005. – Proceedings. 14th International Conference on 17–19 Oct. 2005.
2. Бухарин В. В., Липатников В. А., Сахаров Д. В., Метод управления информационной безопасностью организации на основе процессного подхода // Информационные системы и технологии. 2013. № 3–77. С. 102–109.
3. 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.
4. Костарев С. В., Липатников В. А. Анализ состояния и динамики качества объектов автоматизированной системы менеджмента предприятия интегрированной структуры//Информационные системы и технологии. 2013. № 3–89. С. 52–64.
5. Штеренберг С. И. Анализ алгоритмов защиты информации на основе самомодифицирующегося кода с применением стеговложения // Наукоемкие технологии в космических исследованиях Земли. 2016. Т. 8. № 2. С. 86–90.
6. Красов А. В., Левин М. В., Штеренберг С. И., Исаченков П. А. Модель управления потоками трафика с изменяющейся нагрузкой // Наукоемкие технологии в космических исследованиях Земли. 2016. Т. 8. № 4. С. 70–74.

УДК 621.396

ИСПОЛЬЗОВАНИЕ SDN ДЛЯ ОБЕСПЕЧЕНИЯ QOS В БЕСПРОВОДНЫХ СЕТЯХ С ВЫСОКОЙ ПЛОТНОСТЬЮ УСТРОЙСТВ

Ч. Д. Ле, О. А. Симонина

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

В статье предлагается использовать решение на основе программно-конфигурируемых сетей для управления потоками трафика в беспроводных сетях Wi-Fi с большой плотностью сетевых устройств. В качестве коммутаторов предлагается использовать Openvswitch, классификацию трафика производить на основе значения поля ToS или DSCP в IP-заголовках пакетов. Такой метод позволяет организовать сквозную поддержку качества и поддержку классификации трафика при межсетевом взаимодействии.

классификация, SDN, QoS, Wi-Fi, DSCP.

В связи с быстрым ростом числа беспроводных устройств и внедрения решений Интернета вещей (IoT) обеспечение качества обслуживания (QoS) на беспроводных сетях доступа становится актуальной задачей. Несмотря

на большое количество механизмов обеспечения сосуществования различных технологий [1], вопрос интерференции в диапазоне 2,4 ГГц до сих пор остается открытым. Точки доступа Wi-Fi в современном мегаполисе располагаются плотно, обуславливая взаимное влияние, что приводит к существенным трудностям обеспечения качества обслуживания в Wi-Fi сетях. Поэтому внимание сместилось от обеспечения, гарантированного QoS для одной точки доступа (AP – *Access Point*) в сторону обеспечения QoS в беспроводных сетях с высокой плотностью устройств (много точек доступа – APs). Одновременно появление программно-конфигурируемых сетей (SDN) открыло новые возможности в области управления сетью. В статье предлагается использовать решение на основе SDN для управления потоками трафика в случае высокой плотности устройств Wi-Fi сетей. Это решение состоит из двух фаз:

1. Классификация Wi-Fi трафика, входящего или исходящего из APs, в OpenFlow-коммутаторах на основе значения поля DSCP в IP-заголовках пакетов.

2. Назначение потока трафика в очередь с приоритетом на порту коммутатора.

Связанные работы

Существует несколько исследований, относящихся к решениям в области промышленного Интернета, предлагающих использовать SDN и OpenFlow для уменьшения интерференции в WLAN на предприятиях. В работе [2] авторы определили ограничения для одного SDN-контроллера, контролирующего все APs через OpenFlow-интерфейс. Предлагаемые ограничения добавляют особые правила в различные APs, согласно чему, каждая точка доступа должна обеспечить поддержку протокола OpenFlow. Аналогичное решение было предложено в работе [3] – это точка доступа с программным обеспечением (SAE – *Software Access Point*) для удобного управления мобильностью и балансировки нагрузки.

Другие попытки применить SDN для сетей IEEE 802.11 предлагают создание виртуальных точек доступа для каждого отдельного мобильного решения: Odin [4] и OpenSDWN [5]. Такое решение может хорошо обеспечивать мобильность пользователя, но приводит к накладным расходам с точки зрения вычислительной нагрузки и к увеличению трафика во время перемещения, особенно в настройках с большим числом клиентов и при высокой мобильности пользователя.

Классификация трафика в SDN/OpenFlow сети

Классификация Wi-Fi трафика является первым шагом для обеспечения QoS и основывается на DSCP-значениях в записях, установленных

в таблицах OpenFlow-коммутаторов. Каждому DSCP-значению соответствует различное действие, например: отбрасывать пакеты, перемещать пакеты на указанный порт, назначить трафик в указанную очередь. Известно, что согласно IEEE 802.11e [6] и WMM определяются 4 типа категорий: WMM приоритет голосового трафика (AC_VO – наивысший приоритет), WMM приоритет видеотрафика (AC_VI), WMM приоритет негарантированной доставки (AC_BE – *Best Effort Service*), WMM низкий приоритет (AC_BK – низкоприоритетный трафик). Соотнесем эти категории доступа с DSCP-значениями для организации классификации Wi-Fi трафика на коммутаторах SDN и разделим DSCP-значения по приоритетам, организуя в соответствии этими приоритетами 8 очередей на портах OpenFlow-коммутатора (табл. 1). Алгоритм классификации трафика на основе DSCP значения в SDN сети приведен на рисунке 1.

ТАБЛИЦА 1. Тип трафика и соответствующее DSCP значение

Тип трафика	IP DSCP значение	DSCP приоритет	802.11e / WMM	Очередь
Контроль сети	56 (CS7)	7	7 (AC_VO)	7
Межсетевое управление	48 (CS6)	6	7 (AC_VO)	6
Голосовой	46 (EF)	5	6 (AC_VO)	5
Интерактивное видео	34 (AF41)	4	5 (AC_VI)	4
Потоковое видео	32 (CS4)	4	5 (AC_VI)	4
Критически важные трафики	26 (AF31)	3	4 (AC_VI)	3
Сигнализации вызова	24 (CS3)	3	4 (AC_VI)	3
Транзакционный	18 (AF21)	2	3 (AC_BK)	2
Сетевое управление	16 (CS2)	2	3 (AC_BK)	2
Большой массив данных	10 (AF11)	1	2 (AC_BK)	1
Негарантированная доставка данных	0 (BE)	0	0 (AC_BE)	0
Опционный класс – Интернет/scavenger	8 (CS1)	1	1 (AC_BK)	1

Механизм назначения трафика в очередь с приоритетом

Для каждой очереди задается своя политика обработки трафика. Например: очередь_0 обеспечивает минимальную пропускную способность *min-rate* = 1 Мб/с, очередь_1 обеспечивает *min-rate* = 10 Мб/с.

Трафик классифицируется на основе DSCP-значения и перемещается на заданные порты и назначается в соответствующую очередь. Каждой очереди будет присвоено значение приоритета соответственно DSCP значению

трафика чтобы ограничить количество одновременно работающих устройств.

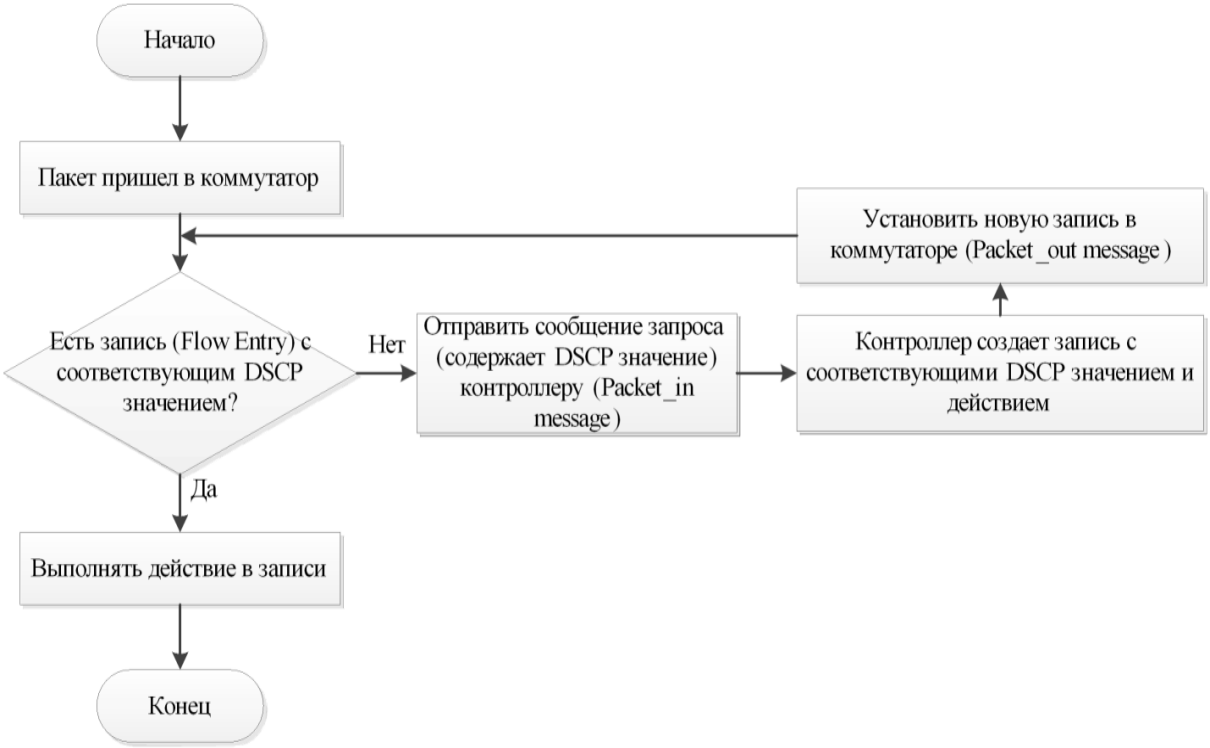


Рис. 1. Классификация Wi-Fi трафика в SDN/OpenFlow сети с помощью DSCP значения

Таким образом, трафик с высоким приоритетом передается прежде, чем трафик с низким приоритетом в зависимости от приоритетов очередей у портов. Согласно примеру на рисунке 2, трафик_1 (запись 1) имеет DSCP=46, и приоритет этого DSCP значения больше, чем приоритет DSCP-значения (DSCP=10) трафика_2 (запись 2) (табл. 1). Несмотря на то, что они перемещаются в одинаковый порт (output=2), трафик_1 будет передан раньше трафика_2 потому, что приоритет его очереди выше (5 > 1).

Запись 1	… dscp = 46, priority = 500, action = queue:5, output:2
Запись 2	… dscp = 10, priority = 500, action = queue:1, output:2

Рис. 2. Записи потоков в OpenFlow таблице

После процесса классификации и назначения приоритета, контроллер будет устанавливать разные правила для разных типов трафика в зависимости от конкретных QoS-политик. Например, с использованием данного механизма можно решить классическую задачу управления мультисервисным

трафиком с использованием REST API для SDN [7, 8]: отправить трафик данных по кратчайшим путям, а мультимедиа трафик по путям с маленькой задержкой и гарантируемой пропускной способностью.

Вывод

Предложенный механизм на основе SDN для управления потоками мультисервисного трафика в беспроводных сетях Wi-Fi с большой плотностью сетевых устройств основывается на DSCP-значениях в IP-заголовках пакетов. Механизм позволит уменьшить количество одновременно работающих беспроводных устройств (то есть снизить интерференцию) и повысить приоритет трафика чувствительных к задержке приложений в сравнении с остальным.

Достоинство этого решения заключается в легкости применения новых QoS-политик через программные приложения, установленные в SDN-контроллере. Кроме того, контроллер позволяет легко удалить старые записи потока и установить новые записи в OpenFlow-таблицах, и поэтому развертывает механизмы для обеспечения QoS более динамично.

Список используемых источников

1. Ле Ч. Д., Симонина О. А. Анализ механизмов сосуществования беспроводных технологий в нелицензируемом диапазоне 2,4 ГГц // Актуальные проблемы инфотелекоммуникаций в науке и образовании. IV Международная научно-техническая и научно-методическая конференция: материалы конференции. СПб. : СПбГУТ, 2015. С. 137–141.

2. Zhao D., Zhu M., & Xu M. Leveraging SDN and OpenFlow to mitigate interference in enterprise WLAN // Journal of Networks. 2014. № 9, issue 6. PP. 1526–1533.

3. Lei T., Lu Z., Wen X., Zhao X., & Wang L. SWAN: An SDN based campus WLAN framework // Wireless Communications, Vehicular Technology, Information Theory and Aerospace & Electronic Systems (VITAE), 4th IEEE International Conference. May 2015. PP. 1–5.

4. Suresh L., Schulz-Zander J., Merz R., Feldmann A., & Vazao T. Towards programmable enterprise WLANS with Odin // Proceedings of the first workshop on Hot topics in software defined networks. Aug. 2012. ACM. PP. 115–120.

5. Schulz-Zander J., Mayer C., Ciobotaru B., Schmid S., & Feldmann A. OpenSDWN: Programmatic control over home and enterprise Wi-Fi // Proceedings of the 1st ACM SIGCOMM Symposium on Software Defined Networking Research. Jun. 2015. P. 16.

6. IEEE Draft for Wireless Medium Access Control (MAC) and Physical Layer (PHY) Specifications: Medium Access Control (MAC) Enhancements for Quality of Service (QoS) // IEEE Std 802.11e/ Draft 11.0. Oct. 2004.

7. Tsung-Feng Y., Wang K., & Hsu Y. H. Adaptive routing for video streaming with QoS support over SDN networks // In Information Networking (ICOIN), IEEE International Conference. Jan. 2015. PP. 318–323.

8. Akella A. V., & Xiong K. Quality of service (QoS)-guaranteed network resource allocation via software defined networking (SDN) // Dependable, Autonomic and Secure Computing (DASC), IEEE 12th International Conference. Aug. 2014. PP. 7–13.

УДК 004.057.4

СРАВНЕНИЕ РЕШЕНИЙ БЕЗОПАСНОСТИ ДЛЯ SCTP

А. В. Лейкин

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

Протокол SCTP изначально разрабатывался для транспортировки сигнальных сообщений ОКС № 7 по IP-сетям. Этот протокол может быть использован любыми приложениями верхних уровней, которым требуются услуги гарантированной, негарантированной, упорядоченной или неупорядоченной сквозной доставки данных через сеть между оконечными открытыми системами ВОС. Многие из таких приложений могут предъявлять строгие требования в отношении безопасности передаваемых из конца в конец данных. Для решения этой задачи широко применяются хорошо известные механизмы IPSec и TLS, но использование данных механизмов в сочетании с протоколом SCTP приводит к существенному ограничению его функциональных и эксплуатационных характеристик. Этого можно избежать путем внедрения функций безопасности непосредственно в протокол SCTP.

SCTP, SIGTRAN, S-SCTP, TLS, IPSec, End-to-End Security.

Протокол SCTP изначально разрабатывался для транспортировки сигнальных сообщений ОКС № 7 по IP-сетям. Его задача состоит в том, чтобы обеспечить такие же надежность и качество обслуживания, как и в сети ОКС № 7. Несмотря на свою первоначальную цель SCTP является универсальным транспортным протоколом с несколькими особенностями, что делает его подходящим для большинства приложений, которые используют уже ставшие классическими транспортные протоколы TCP и UDP. Ранее мы уже проводили сравнение протоколов транспортного уровня [1], но в интересах данной статьи напомним, что основным отличием протокола SCTP от предшественников является поддержка:

– многопоточности (англ. *multistreaming*), позволяющей организовывать отдельные двунаправленные потоки для передачи данных в рамках одной ассоциации;

– множественной адресации (англ. *multihoming*), когда конечная точка ассоциации имеет несколько IP-адресов для повышения отказоустойчивости;

– услуги неупорядоченной доставки, благодаря чему на принимающей стороне устраняется задержка, возникающая на транспортном уровне, при передаче данных вышележащему.

Подробное описание предоставляемых услуг, сигнальных процедур, форматов сообщений и параметров приведено в рекомендации IETF RFC4960 [2].

Существующие решения безопасности

Для защиты передаваемых данных существует два основных решения в области безопасности. Эти решения могут использовать одни и те же наборы шифров и алгоритмы кодов аутентификации, использующих хеш-функции (англ. HMAC – *hash-based message authentication code*). Также они используют аналогичные механизмы обмена ключами и управления безопасными сеансами связи. Рассмотрим более подробно функциональные и эксплуатационные ограничения, накладываемые на протокол SCTP при его работе с IPSec [3] и TLS (англ. Transport Layer Security [4].

1 SCTP поверх IPSec

Протокол IPSec работает на сетевом уровне и был разработан, чтобы быть независимым от используемого транспортного протокола. Текущая версия [3] превратилась в довольно-таки сложный составной протокол и фактически может рассматриваться как целый набор протоколов. Например, когда требуется только проверка целостности, используется протокол аутентификации заголовка AH (англ. *authentication header*) [5], если дополнительно требуется обеспечение защиты пользовательских данных, то вместо AH используется протокол шифрования пользовательского трафика ESP (англ. *encapsulating security payload*) [6]. В случае если необходима безопасная передача, то SCTP может использовать этот набор протоколов для обеспечения целостности, аутентификации, конфиденциальности и защиты данных, передаваемых по IP-сети из конца в конец, что описывается в рекомендации RFC3554 [7]. Также этот RFC отражает проблемы, возникающие при использовании IPSec. Рассмотрим некоторые из них.

Для того чтобы динамически устанавливать безопасные ассоциации IPSec SA (англ. *IPSec Security Associations*) протокол может использовать процедуры согласования ключей IKE [8]. Управление и обработка такой безопасной ассоциацией является сложным процессом даже когда используется TCP. В случае SCTP возникают проблемы с поддержкой динамического реконфигурации ассоциации (добавления новых IP-адресов (ADDIP)), так как IPSec не очень хорошо поддерживает множественную адресацию узла сети, в связи с тем, что SA определяется ровно одним IP-адресом для каждой конечной точки. Предлагаемое решение заключается в использовании листа IP-адресов в базе данных политик безопасности вместо единичных IP адресов. Тем не менее, не существует доступных на сегодняшний день реализаций, которые бы полностью поддерживали этот RFC, поэтому при использовании SCTP поверх IPSec каждый путь ассоциации управляется индивидуально [7].

В эталонной модели BOC (OSI) IPSec находится на один уровень ниже SCTP, поэтому он не способен различать границы передаваемых SCTP-сообщений и SCTP-потоков. В связи с этим при использовании IPSec осуществляется шифрование всех данных, передаваемых в рамках ассоциации, даже если приложение не выставляло таких требований. Также во время работы SA не поддерживается возможность изменения уровня требуемой безопасности. Все это приводит к неоправданному увеличению вычислительной нагрузки (эксплуатационных расходов) на концах ассоциации.

2 TLS поверх SCTP

Данное решение позволяет устранить некоторые рассмотренные недостатки IPSec при использовании с SCTP. Так как TLS является байт-ориентированным протоколом, то для корректной работы ему требуется транспортный протокол, обеспечивающий гарантированную и упорядоченную доставку. Поэтому в настоящий момент TLS главным образом используется поверх протокола TCP, но может использоваться и поверх SCTP, при этом на SCTP накладывается ряд ограничений. Работа протокола TLS поверх SCTP описывается RFC3436 [9]. Исключается использование протоколом SCTP неупорядоченной доставки и по той же причине не может быть использовано расширение частично надежной доставки PR-SCTP [10].

Пользовательские данные передаются через двустороннее TLS-соединение, которое работает поверх SCTP и использует одну TLS сессию для каждого потока. Это является потенциальным недостатком, приводящим к проблемам производительности оконечных систем, так как с числом потоков эти проблемы будут только масштабироваться. Для *N* безопасных потоков должно быть создано *N* TLS соединений и проведено *N* процедур установки соединений, так называемых «рукопожатий». Если число *N* мало, то это не является большой проблемой, но, если число *N* достаточно велико (протокол SCTP поддерживает до 65535 входящих и такое же количество исходящих потоков в рамках одной ассоциации), то это становится большой проблемой потому что установка соединения – это медленный и ресурсоемкий процесс. Таким образом, когда приложение выполняет *N* соединений, нагрузка с точки зрения использования памяти, ЦПУ и т. п. линейно увеличивается с течением времени.

Следует отметить, что при отправке приложением большого количества сообщений малого размера, каждое такое сообщение зашифровывается TLS отдельно перед передачей его на транспортный уровень. Из-за этого SCTP не может осуществить сборку в один SCTP-пакет нескольких полученных от приложения команд (англ. *chunk*), что приводит

к увеличению передаваемой служебной информации и оказывает существенное влияние на производительность решения.

Самым серьезным недостатком этого решения является отсутствие возможности защиты управляющих команд (используемых при процедурах установления, сопровождения и разрушения ассоциации), а также общих заголовков SCTP-пакетов, передаваемых между двумя конечными точками. Это вызвано тем, что в эталонной модели BOC TLS располагается выше транспортного уровня и SCTP-заголовки будут добавлены после того как TLS пропустит уже зашифрованные пользовательские данные от приложения к SCTP.

Преимущество данного решения по сравнению с SCTP поверх IPSec заключается в том, что оно позволяет передавать шифрованные и нешифрованные данные в пределах одной SCTP ассоциации. В то же время оно осуществляет поддержку множественной адресации и динамическое добавление IP-адресов в действующую ассоциацию SCTP без модификации TLS.

3 Secure SCTP (S-SCTP)

Очевидно, что оба рассмотренных выше решения обладают рядом недостатков, не позволяющих использовать преимущества протокола SCTP в полной мере. В связи с этим предпочтительно интегрировать криптографические функции непосредственно в SCTP для обеспечения функций безопасности на транспортном уровне без необходимости использования других протоколов безопасности. Изменения SCTP предлагается ввести в виде нового расширения, получившего название Secure SCTP [11]. Это решение позволяет полностью избежать недостатков не интегрированных решений, при этом обеспечивает полную совместимость с оригинальным SCTP [2], когда использование функций безопасности не требуется. Безопасный сеанс S-SCTP инициализируется уже после того как была установлена обычная ассоциация SCTP. Если одна из конечных точек не поддерживает это расширение или установка безопасного сеанса была завершена неуспешно, то приложение может решить: хочет ли оно использовать незащищенную ассоциацию или же завершит ее вовсе.

Основная концепция решения S-SCTP заключается в том, что ассоциация имеет один общий сеанс безопасности для всех адресов в случае множественной адресации и для всех потоков данных в случае с многопоточностью (но не обязательно, что все потоки будут зашифровываться). Для этого механизм безопасности интегрирован между верхним функциональным блоком SCTP, который осуществляет группировку SCTP команд в SCTP-пакет и нижним функциональным блоком, который выбирает адрес назначения для отправки SCTP пакета.

S-SCTP обеспечивает те же самые функции безопасности, что и два стандартных решения безопасности, а именно аутентификацию, проверку

целостности и шифрование. Единственным недостатком производительности S-SCTP в сравнении с TLS над SCTP происходит, когда длинные сообщения должны быть фрагментированы на транспортном уровне [12, 13].

Для интеграции функций безопасности в SCTP необходимо ввести несколько новых процедур, команд и параметров, но, к сожалению, объем статьи не позволяет их рассмотреть. Читатель может изучить их самостоятельно [11].

Приложение, использующее S-SCTP, имеет возможность использовать четыре различных уровня безопасности, при этом может изменить уровень безопасности в любое время в течение срока службы безопасного сеанса связи.

В таблице приводится итог проведенного сравнения решений безопасности в отношении практичности, эксплуатационных расходов, затрат на управление и производительности. В таблице «+» указывает, что в данном решении функция хорошо поддерживается, «–» обозначает недостатки решения, «(–)» проблема решена теоретически [12].

ТАБЛИЦА 1. Сравнение решений безопасности

Критерии	TLS	IPSec	S-SCTP
Масштабируемость для нескольких потоков	–	+	+
Поддержка множественной адресации SCTP	+	(–)	+
Эксплуатационные расходы на короткие сообщения	–	+	+
Эксплуатационные расходы на длинные сообщения	+	–	–
Безопасность при неупорядоченной доставке	нет	+	+
Безопасность для управляющих SCTP команд	нет	+	+
Поддержка защищенных и не защищенных потоков	+	нет	+
Управление безопасными сессиями	+	–	+
Поддержка частично надежной передачи (PR-SCTP)	нет	+	+
Динамическая реконфигурация адресов	+	–	+

Список используемых источников

1. Лейкин А. В. Протоколы транспортного уровня UDP, TCP, SCTP: достоинства и недостатки // Проводные сети. Первая миля. 2013. № 5. С. 62–69.

2. Stewart R. RFC4960 Stream Control Transmission Protocol. 2007. URL: https://tools.ietf.org/html/rfc4960 (дата обращения 05.04.2016).

3. Kent S., Seo K. RFC4301 Security architecture for the Internet protocol. 2005. URL: https://tools.ietf.org/html/rfc4301 (дата обращения 05.04.2016).

4. Dierks T., Rescorla E. RFC5246 the Transport Layer Security (TLS). 2008. URL: https://tools.ietf.org/html/rfc5246 (дата обращения 05.04.2016).

5. Kent S. RFC4302 IP authentication header. 2005. URL: https://tools.ietf.org/html/rfc4302 (дата обращения 05.04.2016).

6. Kent S. RFC4303 IP encapsulating security payload (ESP). 2005. URL: https://tools.ietf.org/html/rfc4303 (дата обращения 05.04.2016).

7. Bellovin S., Ioannidis J., Keromytis A., Stewart R. RFC3554 On the Use of Stream Control Transmission Protocol (SCTP) with IPsec. 2003. URL: https://tools.ietf.org/html/rfc3554 (дата обращения 05.04.2016).

8. Kaufman C. RFC4306 Internet key exchange (IKEv2) protocol. 2005. URL: https://tools.ietf.org/html/rfc4306 (дата обращения 05.04.2016).

9. Jungmaier A., Rescorla E., Tuexen M. RFC3436 Transport Layer Security over Stream Control Transmission Protocol. 2002. URL: https://tools.ietf.org/html/rfc3436 (дата обращения 05.04.2016).

10. Stewart R., Ramalho M., Xie Q., Tuexen M., Conrad P. RFC3758 Stream Control Transmission Protocol (SCTP) Partial Reliability Extension. 2004. URL: https://tools.ietf.org/html/rfc3758 (дата обращения 05.04.2016).

11. Hohendorf C., Unurkhaan E., Dreibholz T. Secure SCTP draft-hohendorf-secure-sctp-22.txt. 2016. URL: https://tools.ietf.org/html/draft-hohendorf-secure-sctp-22 (дата обращения 05.04.2016).

12. Hohendorf C., Rathgeb E., Unurkhaan E., Tuxen M. Secure End-to-End Transport Over SCTP // Journal of Computers. June 2007. Vol 2. No. 4. C. 31–40.

13. Lindskog S., Brunstrom A. A Comparison of End-to-End Security Solutions for SCTP // Availability, Reliability and Security. ARES 08. 2008. C. 526–531.

Статья представлена заведующим кафедрой, доктором технических наук, профессором Б. С. Гольдштейном.

УДК 004.72

ИСПОЛЬЗОВАНИЕ МУЛЬТИАГЕНТНЫХ СИСТЕМ ДЛЯ УПРАВЛЕНИЯ В СЕТЯХ СВЯЗИ

С. С. Логинов

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

В настоящей статье обосновывается актуальность создания новых моделей и методов, которые смогли бы описать взаимодействие устройств в беспроводной ad hoc сети с учетом новых требований бизнеса. Для описания взаимодействия устройств в статье предлагается описывать поведение таких ресурсов как интеллектуальных агентов и использовать результаты наработок теории игр для описания их поведения.

теория игр, коалиционная теория игр, ad hoc сети.

Постановка проблемы

Предстоящая в самое ближайшее время миграция современных инфокоммуникаций от уже ставших традиционными сетями связи

NGN/IMS *(Next-Generation Network/IP Multimedia Subsystem)* к новой парадигме сетей SDN/NFV *(Software Defined Networking/Network Functions Virtualization)* позволяет операторам связи по-новому взглянуть на внедрение телекоммуникационных услуг и более эффективно использовать инфокоммуникационные ресурсы сети.

Эта новая парадигма SDN/NFV обуславливает необходимость и по-новому взглянуть на сетевое управление. В этих новых сетях сбор и измерение бизнес-метрик становится относительно менее сложной задачей, но появляется все больше способов использования полученной информации для повышения эффективности сети и, как следствие, повышению прибылей операторов/провайдеров. Эти способы постоянно усложняются и имеют большие перспективы [1].

SDN-контроллеры этих новых сетей не работают с реальными сетевыми ресурсами напрямую. Ресурсы в такой сети представляют собой абстракции. Происходит это из-за того, что ресурсы стали слишком гетерогенными, а услуги для конечных пользователей стали гораздо более инвариантными относительно физической сущности этих ресурсов. Сегодня сетевыми ресурсами могут выступать место в облаке, пропускная способность оптического канала, ограниченный спектр радиочастот или даже ограничение по количеству запросов к ограниченному контенту. И вопрос распределения таких ресурсов встает все более остро.

В настоящей статье обосновывается актуальность создания новых моделей и методов, которые смогли бы описать взаимодействие устройств в беспроводной ad hoc сети с учетом новых требований бизнеса. Для решения этой задачи в статье предлагается описывать поведение таких ресурсов как интеллектуальных агентов и использовать результаты наработок теории игр для описания их поведения.

Состояние вопроса

Новые результаты теории игр, полученные в интересах разных дисциплин, в том числе экономики, политики, философии и даже психологии [2], предоставляются перспективными для построения формальной аналитической структуры с набором математических инструментов для изучения этих сложных взаимодействий в сетях SDN/NFV. Этому способствует несколько причин: во-первых, это задачи управления в автономных, распределенных мобильных сетях, в которых сетевые устройства могли бы принимать независимые рациональные решения; а во-вторых, это потребность в распределенных алгоритмах с низкой сложностью, которые могли бы эффективно представлять сценарии конкуренции или взаимодействия между сетевыми устройствами.

С этой точки зрения в теории игр можно выделить две группы игр: кооперативные [2, 3] и некооперативные игры [4]. Некооперативная теория

игр занимается вопросами выбора стратегии в среде конкурирующих игроков. В таких играх каждый из игроков выбирает свою стратегию самостоятельно, с целью увеличить свой выигрыш или уменьшить потери. Существует несколько концептов для решения некооперативных игр, в том числе широко известное равновесие Нэша [4]. Большинство существующих исследований используют наработки некооперативной теории игр для решения проблем распределенного выделения ресурсов [5], распределения нагрузки [6], контроля мощности [7], а также распределения спектра в когнитивном радио и др.

Если некооперативная теория игр изучает сценарии с конкуренцией игроков, то кооперативная теория предлагает инструменты для изучения поведения рациональных игроков, когда они сотрудничают. Основная часть кооперативных игр описывает каким образом формируются группы игроков, называемые коалициями [2]. Участвуя в коалиции, игрок только усиливает свое положение в игре. Кооперативные игры были довольно широко изучены в рамках экономических и политических наук. Хотя применение этих наработок в больших телекоммуникационных сетях связанно с некоторыми сложностями (например, моделирование поведения агентов, вопросы, связанные с эффективностью, сложностью, честностью распределения ресурсов и др.), коалиционные игры предоставляют мощные инструменты для создания устойчивых, практичных и эффективных стратегий кооперации в телекоммуникационных сетях. Большая часть работ в данном направлении ограничивается применением стандартных моделей коалиционных игр для изучения узкого набора аспектов кооперации в сетях. Скорее всего данная ситуация сложилась из-за недостатка литературы, которая бы описывала коалиционные игры.

Коалиционные игры

В общем случае, коалиционные игры происходят между несколькими игроками, их множество можно обозначить как $P = \{1,\ldots,N\}$. Игроки стремятся к созданию и формированию кооперативных групп, т. н. коалиций, для того, чтобы улучшить свои позиции в игре. Любая коалиция $S \subseteq P$ представляет собой договор между несколькими игроками, входящими в S, действовать как единая сущность. Можно легко найти примеры таких коалиций или союзов. Например, в политических играх партии или отдельные игроки могут сформировать коалицию для достижения желаемого результата голосования. Так же существует понятие «ценности» коалиции. Обычно ценность коалиции, обозначаемая как v, определяет стоимость коалиции в игре.

Кооперативная теория игр уже нашла свое применение для решения некоторых проблем в телекоммуникациях. Перечислим некоторые из них.

Интересное использование коалиционных игр в телекоммуникационных сетях можно найти в [8], где рассматривается распределение пропускной способности в каналах с множественным доступом (*multiple access channels*). Модель, приведенная в [8], пытается решить проблему честного распределения пропускной способности между пользователями в беспроводных гауссовских каналов с множественным доступом. В этой модели пользователи выступают за честное распределение пропускной способности. Если же пользователь или группа пользователей не получает должного обслуживания, то они могут начать действовать по собственному усмотрению, что понизит качество связи для остальных участников.

Коалиционные игры также могут быть полезны для изучения возможности кооперации между передатчиками и приемниками с одной антенной в канале с интерференцией [9]. Рассматриваемая модель состоит из нескольких пар передатчик-приемник, которые находятся в гауссовом канале с интерференцией. Авторы изучают возможность кооперации по двум моделям коалиционной теории игр: модель TU (с трансферабельной полезностью), в которой приемники информации имеют возможность взаимодействия по каналу без помех и декодируют получаемые сигналы сообща; и модель NTU (без трансферабельной полезности), в которой приемники формируют линейный многопользовательский детектор (в этом случае канал с интерференцией рассматривается как канал с множественным доступом).

Существуют решения для проблемы пересылки пакетов в ad hoc сетях [10]. В них узлы, находящиеся в центре сети, заинтересованы в передачи пакетов между собой. В то же время им не выгодно передавать пакеты узлов, находящихся на периферии, т. к. им никогда не понадобится помощь отдаленных узлов. В таком случае у пограничных узлов вообще нет возможности передать свои пакеты другим узлам. В [10] предлагается модель коалиционной теории игр, в которой взаимодействуют N игроков – все граничные узлы и один центральный. В предложенной модели формирование коалиции влечет за собой следующие преимущества: при взаимодействии с несколькими граничными узлами и использовании совместную передачу, центральный узел может уменьшить потребляемую мощность; и взамен центральный узел соглашается передавать пакеты пограничных узлов.

Исследования коалиционных моделей взаимодействия между устройствами в ad hoc сетях

Таким образом имеет смысл использовать наработки кооперативной теории игр для создания модели взаимодействия ресурсов в беспроводных ad hoc сетях. Для этого необходимо:

1) Создать и описать модель формирования коалиции из нескольких расположенных рядом устройств, количество устройств в коалиции, взаимодействие между коалициями.

Для этого следует выбрать метрики, по которым будет определяться в какую именно коалиции должно входить устройство для наиболее эффективного взаимодействия сети. Определить, должны ли устройства входить в сразу несколько коалиций.

2) Проанализировать составленную модель.

Проанализировать модель и найти наименее энергозатратные способы передачи информации между устройствами, наиболее эффективные способы передачи с т. з. топологии и др.

3) Показать, какие изменения необходимы в модели с учетом факторов, рассмотренных в пункте 2.

Необходимо решить задачу по выявлению применения факторов, которые производят желательные изменения в системе для решения основных бизнес и эксплуатационных задач. При проведении в комплексе подобного моделирования и анализа сценариев определяются такие управляющие воздействия, которые приводят к назначенным целевым показателям в зависимости от исходной ситуации.

Выводы

Рассмотренные в статье аппарат теории игр и, в частности, кооперативной теории игр, может быть использован для моделирования процессов управления в будущих сетях связи. Данный инструментарий можно использовать для оптимизации процессов телекоммуникациями, улучшая тем самым качество предоставления услуг, эффективность эксплуатационной деятельности, минимизацию рисков и пр.

Также видится преимущество использования подхода кооперативной теории игр перед некооперативной. Этому подходу до сих пор уделялось меньше внимания при описании мультиагентных систем.

Список используемых источников

1. Гольдштейн Б. С., Кучерявый А. Е. Сети связи пост-NGN. СПб. : БХВ-Петербург, 2013. 160 с.

2. Myerson R. B. Game Theory, Analysis of Conflict. Cambridge : Harvard University Press, 1991. 232 p.

3. Owen G. Game Theory, 3rd edition. London : Academic Press, 1995. 356 p.

4. Basar T., Olsder G. J. Dynamic Noncooperative Game Theory. Philadelphia, PA : SIAM Series in Classics in Applied Mathematics, 1999. 234 p.

5. Han Z., Liu K. J. Resource Allocation for Wireless Networks: Basics, Techniques, and Applications. New York : Cambridge University Press, 2008. 43 p.

6. Alpcan T., Basar T. A globally stable adaptive congestion control scheme for Internet-style networks with delay // IEEE/ACM Trans. on Networking. 2005. Vol. 13. PP. 1261–1275.

7. Alpcan T., Basar T., Srikat R. CDMA uplink power control as a noncooperative game // Wireless Networks. 2002. Vol. 8. PP. 659–670.

8. La R., Anantharam V. A game-theoretic look at the Gaussian multiaccess channel. New Jersey : Proc. of the DIMACS Workshop on Network Information Theory, 2003. 56 p.

9. Mathur S., Sankaranarayanan L., Mandayam M. Coalitions in cooperative wireless networks // IEEE J. Select. Areas Commun. 2008. Vol. 26. PP. 1104–1115.

10. Han Z., Poor V. Coalition games with cooperative transmission: a cure for the curse of boundary nodes in selfish packet-forwarding wireless networks // IEEE Trans. Comm. 2009. Vol. 57. PP. 203–213.

Статья представлена научным руководителем, доктором технических наук, профессором Б. С. Гольдштейном.

УДК 621.391

ИСПОЛЬЗОВАНИЕ NETFLOW ДЛЯ АНАЛИЗА СЕТЕВОГО ТРАФИКА

Т. Ю. Лушникова

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

Протокол Netflow является одним из наиболее популярных средств мониторинга трафика сети, однако его использование для научных исследований накладывает ряд ограничений на анализ характеристик трафика.

В статье подробно рассмотрены особенности работы протокола и формат экспортированных данных, а также предложен алгоритм их преобразования для дальнейшего исследования сессий.

Netflow, flow-tools, флаги TCP, восстановление сессий, средства мониторинга трафика.

Анализ сетевого трафика является не только актуальной научной проблемой, но также и прикладной задачей в сетях связи любого масштаба. Целью этого анализа может быть, как сбор статистики по использованию сети, так и проведение исследования природы трафика и законов его распределения во времени.

Существует несколько подходов к анализу трафика. В качестве минимальной единицы могут служить пакеты переданной информации [1] или агрегированный трафик [2], частным случаем которого можно считать сессии. От выбора подхода к анализу зависит и выбор инструментов мониторинга сети.

Мониторинг трафика

Систем мониторинга и анализа трафика, используемые в различных сетях, различаются своей методологией и режимами работы. Анализ собранных данных может происходить как в режиме реального времени,

так и постфактум. Подробный обзор систем мониторинга и анализа в режиме реального времени проведен в [3]. Однако многие современные инструменты позволяют проводить анализ данных в обоих режимах работы, поэтому разделение систем по критерию возможности работы в реальном времени не отражает их основных особенностей.

В работе [4] предложена классификация инструментов мониторинга и анализа сети на основе зависимости от оборудования. Автор разделяет рассматриваемые техники также на 2 группы: основанные на маршрутизаторах и не ориентированные на маршрутизаторы. К первой группе относятся такие широко известные техники, как SNMP и Cisco Netflow. Ко второй группе принадлежат новые методы мониторинга WREN и SCAM, не набравшие пока популярности из-за относительной сложности развертывания системы.

Несмотря на недостатки (например, низкая гибкость из-за жестко заданной на маршрутизаторах логики), как отмечает автор [4], «маршрутизаторо-ориентированные» методы мониторинга и анализа сети более популярны на сегодняшний момент, поскольку представляют собой готовые решения и часто не требуют от администраторов сетей серьезных дополнительных настроек. На данный момент одним из самых популярных инструментов для мониторинга и анализа трафика сети является протокол Netflow.

Протокол Netflow

Протокол Netflow, разработанный компанией Cisco Systems [5], – это протокол учета сетевого трафика, быстро набравший популярность и на данный момент являющийся, по сути, промышленным стандартом, поддерживаемым не только Cisco Systems, но и другими производителями сетевого оборудования, в частности, Mikrotik и Juniper.

Существует несколько версий протокола, последняя версия 9 работает с IPv6 [6], однако чаще всего для организации мониторинга сети достаточно версии 5. Архитектура протокола вне зависимости от версий остается той же, а между собой версии отличаются только наличием дополнительных полей в отчете Netflow v9. Для сбора информации о трафике Netflow использует один или несколько сенсоров, собирающих статистику о проходящем через маршрутизаторы трафике, и коллектор, получающий информацию от сенсоров и помещающий ее в хранилище.

Для хранения информации о переданных данных Netflow использует потоки (flows) – наборы пакетов с одинаковыми параметрами, проходящими в одном направлении. Для отделения одного потока от другого Netflow использует 5 параметров:

– IP-адрес источника;
– IP-адрес назначения;

– порт источника;
– порт назначения;
– код протокола IP (TCP, UDP, ICMP и т. п.).

Когда сенсор определяет, что поток закончен, данные о нем отправляются в коллектор. Кроме того, в зависимости от настроек сенсор может отправлять данные и о текущем потоке. В настройках по умолчанию поток считается законченным, если получено сообщение завершения сессии (для TCP), либо в текущем потоке не было передано ни одного пакета более 15 секунд (для TCP и UDP).

Собранная информация хранится в файлах собственного формата, однако многие анализаторы позволяют экспортировать данные в виде таблиц формата csv. Утилиты Netflow (например, *flow-tools*, работающая под управлением ОС Linux) допускают экспорт всех интересующих полей. Экспорт пакетов при работе с flow-tools осуществляется утилитами flow-cat для чтения исходных данных и flow-export для непосредственной выгрузки данных.

После экспорта всех полей информация представляется в виде таблицы, каждая строка при этом соответствует потоку Netflow. Все поля, доступные после экспорта данных, собранных Netflow v5, представлены в таблице 1. Следует различать потоки в понимании Netflow и сессии сеансов связи. Под потоком Netflow подразумевается только набор пакетов, передающихся между двумя хостами непрерывно в одном направлении в течение некоторого времени. Таких потоков в сессии может быть несколько, однако Netflow воспримет их как отдельные.

ТАБЛИЦА 1. Описание полей формата Netflow v5

Название поля	Содержание
Unix_secs	Время экспорта записи в секундах в формате Unix
Unix_nsecs	Остаточные наносекунды времени экспорта данных
Sysuptime	Время работы устройства экспорта (системы) с момента его загрузки в милисекундах
Exaddr	Адрес экспортирующей системы
Dpkts	Количество пакетов, переданных в течение потока
Doktets	Количество байт, переданных в потоке на уровне IP
First	Время системы Sysuptime на момент старта потока
Last	Время системы Sysuptime в момент прихода последнего пакета потока
Engine_type	Поля, идентифицирующие сенсор, который собрал и отправил в коллектор поток, и его настройки
Engine_id	
Src_addr	IP-адрес источника пакетов потока

Название поля	Содержание
Dst_addr	IP-адрес назначения пакетов потока
Next_hop	IP-адрес следующего маршрутизатора
Input	SNMP-метка входящего интерфейса
Output	SNMP-метка исходящего интерфейса
Src_port	Порт источника пакетов
Dst_port	Порт назначения пакетов
Prot	Код протокола IP (например, TCP = 6, UDP = 17)
ToS	Метка Type of Service
Tcp_flags	Сумма флагов всех пакетов TCP, полученных в этом потоке
Src_mask	Маска адреса источника
Dst_mask	Маска адреса назначения
Src_as	Номер автономной системы источника
Dst_as	Номер автономной системы назначения

Помимо экспорта пакет flow-tools предоставляет множество других возможностей для работы с собранными данными. Например, статистику принятых пакетов в зависимости от порта или адреса назначения можно получить, настроив утилиту flow-stat, что может быть достаточно для системного администрирования. Однако встроенные средства не подходят для анализа экспортированных данных с точки зрения сессий.

Восстановление сессий

Характер современного трафика определяется в основном информацией, передающейся поверх транспортного протокола TCP, поэтому для исследования характеристик трафика необходимо работать с TCP-сессиями.

Поскольку Netflow представляет данные в виде потоков, для анализа сессий необходимо объединять несколько потоков. Понятие сессия может быть применено только к пакетам протокола TCP [7]. Сессия определяется комбинацией IP-адресов источника и назначения, портов источника и назначения и временными метками. По умолчанию сенсоры Netflow отправляют информацию в коллектор после 15 секунд тишины в канале установленного соединения. Индикатором того, является ли поток полной сессией TCP или же какой-то ее частью, может служить поле Tcp_flags.

Пакет TCP имеет 6 возможных флагов (URG, ACK, PUSH, RST, SIN, FIN). Всего на поле Flags в пакете TCP отведено 6 бит, на каждый флаг выделен 1 бит, и любая комбинация флагов является уникальной. Так, если в течение сессии были получены пакеты TCP, содержащие флаги SIN, FIN

и ACK, то сумма всех флагов будет 010011 в двоичном виде или 19 при переводе в десятичную систему счисления.

Под полной сессией TCP подразумевается сессия, которая была открыта сообщением с флагом SIN, и закончена флагами FIN или RST. Если же в потоке не присутствовало хотя бы одного флага из флагов начала или окончания сессии, то он может являться лишь частью сессии. В таблице 2 перечислены все выявленные суммы флагов TCP.

Таблица 2. Суммы флагов TCP

Группа	Описание группы	Флаги
Полные сессии	Содержит комбинации SIN+FIN, SIN+RST, их сумму возможные промежуточные флаги	19, 22, 23, 27, 30, 31
Начало	Комбинации SIN+ACK, SIN+PUSH	26, 18
Середина	ACK, PUSH+ACK	16, 24
Конец	Любые комбинации с флагами FIN и RST без SIN	4, 17, 21, 25, 28, 29, 20

Для того, чтобы соединить все неполные сессии, необходимо:

1. Убрать из массива данных все полные TCP-сессии и потоки UDP.

2. Оставшиеся данные отсортировать по следующим 5 полям: src_ip, dst_ip, src_port, dst_port, first. Это обеспечит правильный порядок потоков и гарантирует, что данные не будут перемешаны между собой.

3. Для каждой следующей строки (i + 1) проверить условие: если параметры совпадают с текущей сессией (i), и она не закрыта, то в строке (i) изменяются параметры last, dpkts, doctets, Unix_time, tcp_flags. Иначе начинается новая сессия, а данные о текущей сохраняются без изменений или отбрасываются.

После того, как сессии были «склеены», необходимо добавить исключенные ранее данные о полных сессиях и отсортировать их по любому интересующему полю.

Заключение

Протокол Netflow является одним из самых популярных инструментов сбора трафика в сетях. Информация, собираемая с помощью Netflow, на первый взгляд дает лишь краткое представление о трафике, однако возможность экспорта собранных данных в табличном виде с содержанием множества полей делает протокол мощным инструментом сбора информации об исследуемой сети. Кроме того, простой алгоритм преобразования собранных данных, предложенный в статье, снимает ограничения на анализ сессий, что позволяет использовать Netflow в

качестве инструмента получения исходных данных для анализа природы трафика сети.

В дальнейшем планируется использовать Netflow для определения профилей трафика различных социальных групп и выделения общих и частных особенностей современного сетевого трафика.

Список используемых источников

1. Kassim M., Ismail M., Yusof M. I. Statistical Analisys and Modeling of Internet Traffic IP-Based Network for Tele-Traffic Engineering // ARPN Journal of Engineering and Applied Sciences. 2015. Vol. 10. № 3. PP. 1505–1512.

2. Kotz D., Essien K. Analysis of a Campus-wide Wireless Network Categories and Subject Descriptors // Science. 2002. Vol. 11. № September. PP. 115–133.

3. Гетьман А. И., Евстропов Е. Ф., Маркин Ю. В. Анализ сетевого трафика в режиме реального времени: обзор прикладных задач, подходов и решений. [Электронный ресурс] // Препринты ИСП РАН. URL: http://www.ispras.ru/preprints/docs/prep_28_2015.pdf (дата обращения 20.03.2016).

4. A Summary of Network Traffic Monitoring and Analysis Techniques / A. Cecil. – 9 p.

5. Сайт компании Cisco Systems [Электронный ресурс]. URL: http://www.cisco.com (дата обращения 02.02.2016).

6. RFC 3954. Cisco Systems NetFlow Services Export Version 9 [Электронный ресурс]. URL: https://www.ietf.org/rfc/rfc3954.txt (дата обращения 21.03.2016).

7. RFC 793. Transmission Control Protocol [Электронный ресурс]. URL: https://tools.ietf.org/html/rfc793 (дата обращения 20.02.2016).

Статья представлена научным руководителем, кандидатом технических наук В. Ю. Гойхманом.

УДК 621.391

МАТЕМАТИЧЕСКАЯ МОДЕЛЬ ОЦЕНКИ КОЭФФИЦИЕНТА УДЕЛЬНОЙ ХРОМАТИЧЕСКОЙ ДИСПЕРСИИ ОПТИЧЕСКИХ ВОЛОКОН

С. С. Мазепкин, Г. В. Матвейкин, Д. О. Федосеев

Военная академия связи им. Маршала Советского Союза С. М. Буденного

Оптический сигнал, распространяясь по волокну, искажается за счёт дисперсии различного рода. В статье рассмотрена математическая модель расчета удельного коэффициента хроматической дисперсии на основе трехчленного уравнения Селлмейера. Предложенный вариант расчета позволяет с высокой достоверностью определить коэффициент удельной хроматической дисперсии для оптического волокна с заданным химическим составом сердцевины и оболочки.

оптическое волокно, показатель преломления, длина волны, мода, хроматическая дисперсия, поляризационная модовая дисперсия.

При прохождении оптического сигнала по волокну происходит рассеяние во времени его спектральных или модовых составляющих. Это явление носит название дисперсии и обусловлено различием времени распространения различных мод в оптическом волокне (ОВ) и наличием частотной зависимости показателя преломления. При передаче импульсных сигналов изменяется не только их амплитуда, но и форма – импульсы уширяются [1]. При достаточно большом уширении импульсы начинают перекрываться, так что становится невозможным их выделение при приеме. Таким образом, актуальным представляется исследование дисперсионных характеристик различных оптических волокон в широком диапазоне длин волн.

В одномодовых (ОМ) волоконных световодах модовая дисперсия отсутствует, так как по такому волокну распространяется только одна мода или две моды в двух разных состояниях поляризации. Другими словами, уширение импульсов в ОМ ОВ определяется хроматической дисперсией в пределах низшей моды [2]. Коэффициент хроматической дисперсии в ОМ ОВ может быть представлен в общем виде выражением:

$$D(\lambda) = M(\lambda) + B(\lambda),$$

где $M(\lambda)$ – удельная материальная дисперсия, $B(\lambda)$ – удельная волноводная дисперсия.

Материальная дисперсия определяется дисперсионными характеристиками материалов, из которых изготовлена сердцевина оптического волокна – кварца и легирующих добавок. Спектральная зависимость показателя преломления материала сердцевины и оболочки достаточно часто описывается известным уравнением Селлмейера, которое имеет следующий вид [3]:

$$n(\lambda) = \sqrt{1 + \sum_{j=1}^{3} \frac{A_j \lambda^2}{\lambda^2 - B_j^2}},$$

где A_j и B_j – коэффициенты Селлмейера, соответствующие заданному типу материала, легирующей примеси и ее концентрации, λ – длина волны.

При определении показателя преломления основных компонентов волоконного световода, необходимо учитывать, что в качестве материала светоотражающей оболочки, как правило, применяется чистое кварцевое стекло (SiO_2), а для изготовления сердечника – легированный кварц.

В ходе данной работы был проведен аналитический расчет коэффициента хроматической дисперсии для оптического волокна, сердечник которого состоит из 7 % GeO_2 93 % SiO_2, а оболочка из чистого кварца SiO_2.

Коэффициенты Селлмейера для кремния составляют: A = 0,6961663; 0,4079426; 0,8974794, B = 0,0684043; 0,1162414; 9,896161, а для кремния, легированного германием: A = 0,68698290; 0,44479505; 0,790973512, B = 0,078087582; 0,1155184; 10,436628 [3].

Спектральная зависимость показателей преломления сердечника $n(\lambda)$ и оболочки $n_{об}(\lambda)$ в диапазоне 600–1565 нм приведены на рисунке 1.

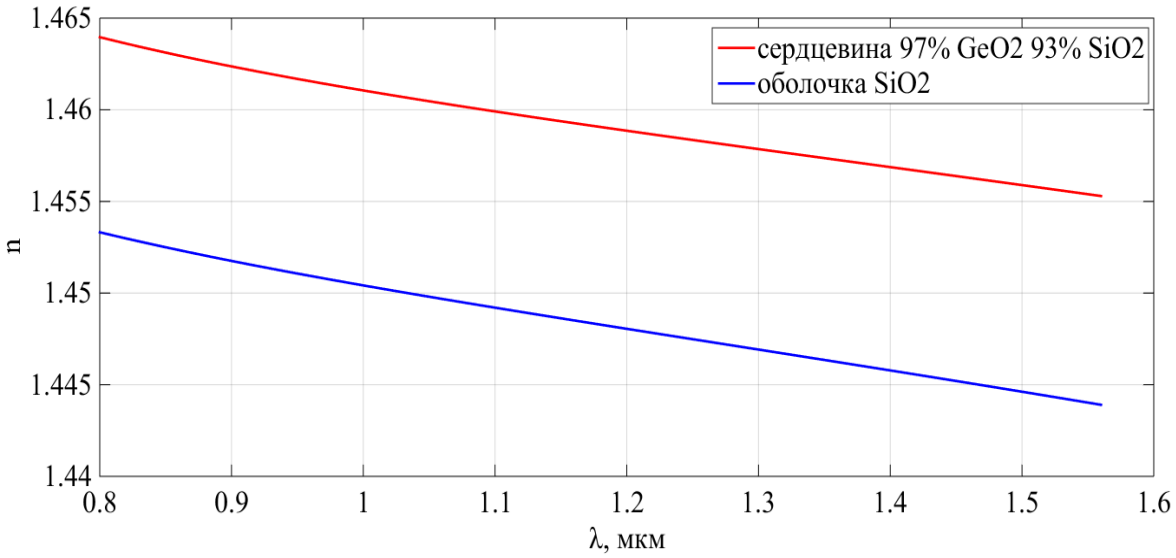


Рис. 1. Спектральная зависимость показателя преломления сердечника 97 % GeO_2 93 % SiO_2 и оболочки SiO_2

Материальная дисперсия характеризуется коэффициентом $M(\lambda)$, который определяется из соотношения [3]:

$$M(\lambda) = -\frac{\lambda}{c}\frac{\partial^2 n(\lambda)}{\partial \lambda^2},$$

где c = 2,998·10^8 м/с – скорость света.

Волноводная дисперсия характеризуется коэффициентом $B(\lambda)$, который определяется из соотношения [3]:

$$B(\lambda) = \frac{2n^2(\lambda)\cdot\Delta(\lambda)}{\lambda c},$$

где $\Delta(\lambda) = \dfrac{n^2(\lambda) - n_{об}^2(\lambda)}{2n^2(\lambda)}$ – относительная разность показателей преломления.

Результирующее значение коэффициента хроматической дисперсии $D(\lambda)$, который складывается из материальной и волноводной составляющих, изображено на рисунке 2.

Анализируя проведенные расчеты, установили, что коэффициент хроматической дисперсии для рассматриваемого волокна на длине волны

1550 нм составляет $D(1.550)$ = 17,89 пс/нм·км. Сравним полученное значение с параметрами одномодового волокна OFS SM 322, характеристики которого приведены в таблице 1.

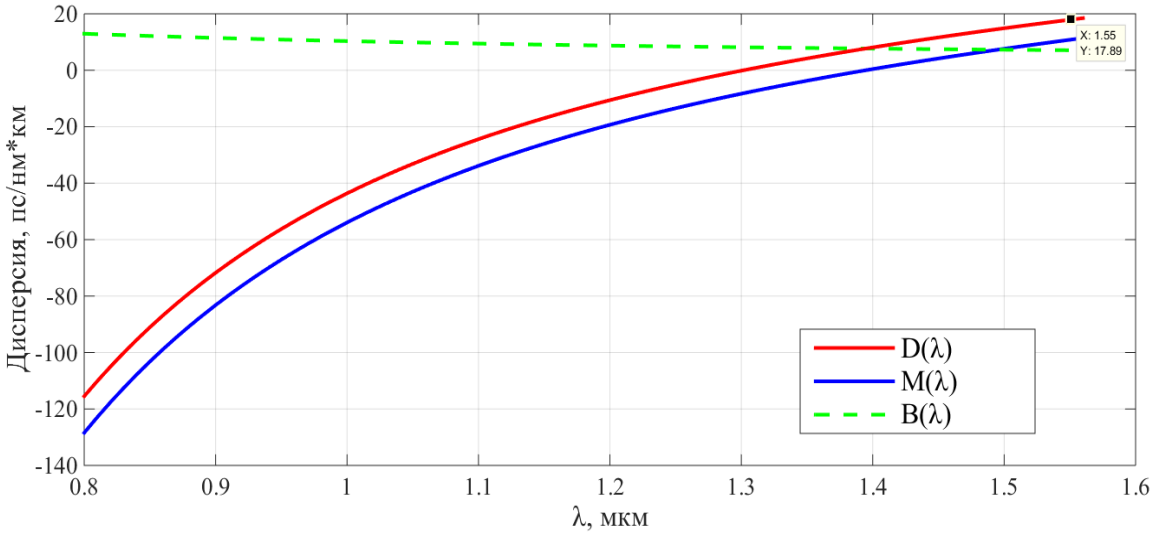


Рис. 2. Спектральная зависимость коэффициента материальной, волноводной и хроматической дисперсии рассматриваемого волокна

Данное волокно удовлетворяет требованиям ITU-T G.652.B. Оболочка ОВ кварцевая, а сердцевина легирована германием. Хотя его характеристики оптимизированы для эксплуатации в районе 1310 нм в области, где минимальна хроматическая дисперсия, его можно использовать и в районе 1550 нм, где минимально затухание [4].

ТАБЛИЦА 1. Характеристики оптического волокна OFS SM 322

Характеристика	Значение
Затухание	0,31–0,35 дБ/км на 1310 нм 0,21–0,25 дБ/км на 1550 нм
Длина волны нулевой дисперсии	$1300 \le \lambda_0 \le 1322$ нм
Наклон дисперсии (на λ_0)	$\le 0{,}092$ пс/нм^2·км
Дисперсия на 1550 нм	≤ 18 пс/нм·км
Коэффициент поляризационной модовой дисперсии (ПМД)	≤ 0.1 пс/км$^{1/2}$ на 1310 нм
Диаметр модового поля	9,2 ± 0,4 мкм на 1310 нм
Диаметр оболочки	125 ± 1 мкм
Эксцентриситет сердцевина/оболочка	$\le 0{,}5$ мкм
Длина волны отсечки в волокне (λ_C)	1150–1340 нм
Длина волны отсечки в кабеле (λ_{0C})	1260 нм

Сравнивая результаты расчетов с приведенными характеристиками, видим, что полученное значение соответствуем реальным данным (17,89 пс/нм·км < 18 пс/нм·км). Таким образом, предложенная модель расчета позволяет с высокой точностью определить коэффициент удельной хроматической дисперсии в широком спектральном диапазоне для оптических волокон с различным химическим составом материала сердечника и оболочки.

Список используемых источников

1. Гордиенко В. Н., Крухмалев В. В., Моченов А. Д., Шарафутдинов Р. М. Оптические телекоммуникационные системы : учебник для вузов / Под ред. профессора В. Н. Гордиенко. М. : Горячая линия – Телеком, 2011. – 368 с. ISBN 978-5-9912-0146-9.

2. Нойкин Ю. М., Махно П. В. Физические основы оптической связи [Электронный ресурс] : электронное учебное пособие. М-во образования и науки Российской Федерации Федеральное гос. автономное образовательное учреждение высшего проф. образования «Южный федеральный ун-т», Физический фак. Ростов-на-Дону : Южный федеральный ун-т, 2011. 1 электрон. опт. диск; 12 см. Загл. с титул. экрана : Радиоэлектроника – Электрическая связь – Оптическая связь – Теория. Исследования – Физические методы. ИЭР О 14-5/185.

3. Волоконно-оптические кабели и линии связи [Электронный ресурс] // Сайт. Банк лекций siblec.ru. URL: http://siblec.ru/index.php?dn=html&way=bW9kL2h0bWwvY29udGVudC84c2VtLzA2NS9tYWluLmh0bQ== (дата обращения 12.03.2016).

4. Листвин А. В., Листвин В. Н., Швырков Д. В. Оптические волокна для линий связи. М. : ЛЕСАРарт, 2003. 288 с.

УДК 001.891.572

МОДЕЛЬ ФОРМИРОВАНИЯ ОТКЛИКОВ СИГНАЛА НА ВОЗДЕЙСТВИЕ ХРОМАТИЧЕСКОЙ ДИСПЕРСИИ В ОПТИЧЕСКОМ ВОЛОКНЕ

А. Ю. Матюхин, М. А. Мельтенисов

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

Исследование влияния хроматической дисперсии является одной из актуальных задач в современных волоконно-оптических системах передачи. Особый интерес представляет аналитическое описание воздействия дисперсии во временной области. Одним из возможных вариантов описания является модель эхо-сигналов. В статье обосновывается возможность представления процесса распространения сигнала в оптическом волокне в виде последовательного появления новых пар эхо-сигналов.

модель, временная область, коэффициенты, оптическое волокно, хроматическая дисперсия, эхо-сигналы.

Хроматическая дисперсия – один из важнейших факторов, влияющих на распространение сигнала в оптическом волокне. Под её воздействием импульсы становятся шире и начинают перекрывать друг друга, как показано на рисунке 1. Этот эффект известен как межсимвольная интерференция. Одним из способов её описать является применение модели эхо-сигналов.

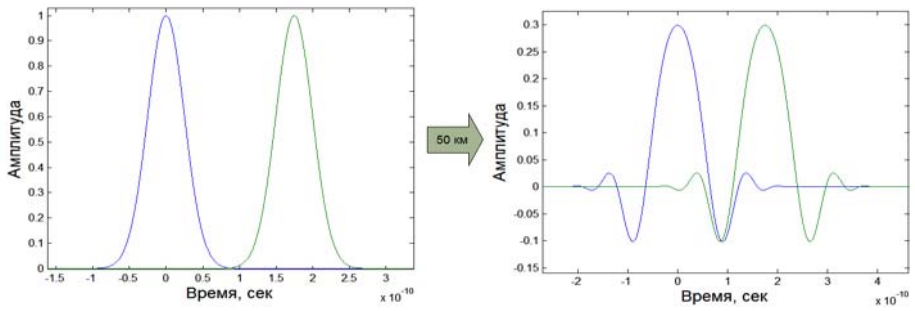


Рис. 1. Влияние хроматической дисперсии на распространение пары гауссовских импульсов на 50 км

Модель эхо-сигналов позволяет представить сигнал в точке z как сумму исходного сигнала и N пар эхо-сигналов: запаздывающих и опережающих на время $n\tau$. Причём каждое из слагаемых умножено на некоторый коэффициент a_n:

$$S(z,t) = a_0 S(0,t) + \sum_{n=1}^{N} a_n S(0,t+n\tau) + \sum_{n=1}^{N} a_{-n} S(0,t-n\tau).$$

Проверим, что модель эхо-сигналов действительно применима в волоконной оптике. Воспользуемся классическим методом представления сигнала в точке z суммой эхо-сигналов [1]. Для начала, необходимо получить передаточную характеристику оптического волокна в виде, подходящем для применения метода:

$$H(j\omega) = \left|H(j\omega)\right| \cdot e^{-jb(\omega)} = A(\omega) \cdot e^{-jb(\omega)},$$

где $A(\omega)$ – АЧХ, $b(\omega)$ – ФЧХ.

Распространение света в оптическом волокне описывается нелинейным уравнением Шрёдингера и не имеет аналитического решения в общем случае [2]. Однако, в контексте текущей задачи, нелинейные компоненты и постоянное затухание можно опустить. Таким образом, остаётся линейное дифференциальное уравнение первого порядка:

$$\frac{\partial \tilde{S}}{\partial z} = -j\beta(\omega)\tilde{S},$$

где $\tilde{S}(j\omega)$ – спектр передаваемого сигнала, β(ω) – постоянная распространения, зависящая от частоты.

Решением уравнения является:

$$\tilde{S}(z, j\omega) = \tilde{S}(0, j\omega) e^{-j\beta(\omega)z}.$$

Отсюда находим передаточную характеристику в искомом виде:

$$H(j\omega) = e^{-j\beta(\omega)z}.$$

Далее необходимо отделить линейную часть ФЧХ от нелинейной:

$$\beta(\omega) = \beta_л(\omega) + \beta_{нл}(\omega),$$

и убедиться, что $\beta_{нл} << \beta_л$. Как видно из рисунка 2, это действительно так. Влияние $\beta_л(\omega)$ моделируется постоянной групповой задержкой сигнала, поэтому нет необходимости в дальнейшем её рассматривать.

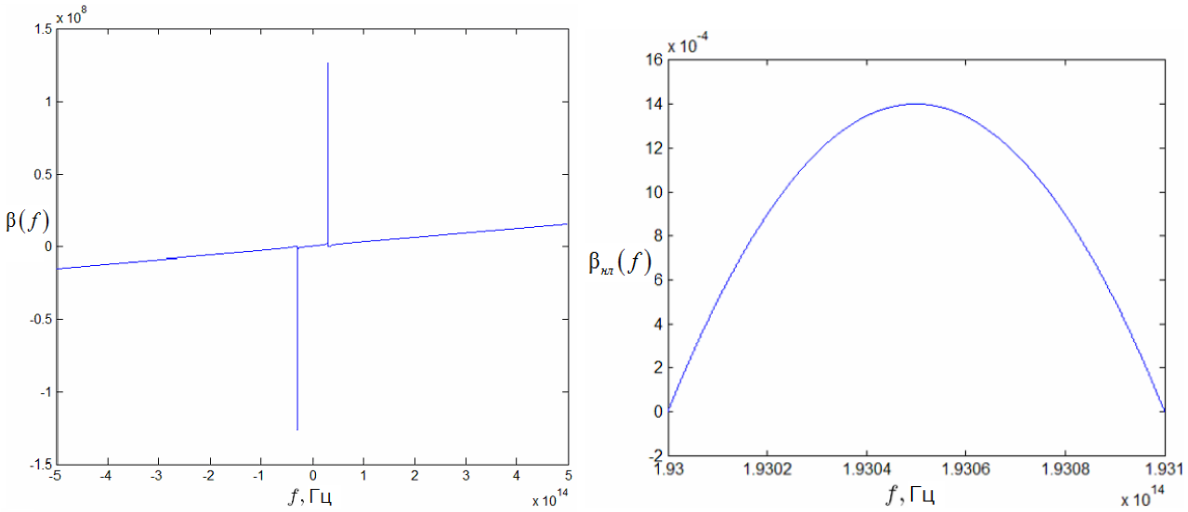


Рис. 2. Постоянная распространения (слева) и её нелинейная часть (справа)

Разложим $\beta_{нл}(\omega)$ в ряд Фурье:

$$\beta_{нл}(\omega) = \sum_n c_n \sin(n\tau\omega). \quad (1)$$

Теперь передаточная функция (если не рассматривать линейную часть ФЧХ) выглядит следующим образом:

$$H(j\omega) = e^{-j\sum_n c_n \sin(n\tau\omega)z}. \quad (2)$$

Метод эхо-сигналов подразумевает дальнейшее разложение (2) в ряд Тейлора, состоящего из двух первых его членов. Однако, из-за больших расстояний z степень экспоненты (2) много больше 1. Этот факт не позволяет

продолжать расчёты классическим способом. У данной проблемы есть два решения.

Первым из них является метод, описанный в [3]. Он основан на разложении в ряд Фурье непосредственно передаточной функции (без линейной составляющей ФЧХ), что позволяет пропустить шаг с разложением в ряд Тейлора.

Его недостатком является невысокая точность, связанная с необходимостью аппроксимировать $\beta_{нл}(\omega)$ квадратичной функцией, что приводит к существенному росту погрешности в рабочем диапазоне частот более 100 ГГц [3].

Альтернативным решением является метод с разбиением всей линии на равные участки-звенья, как показано на рисунке 3.

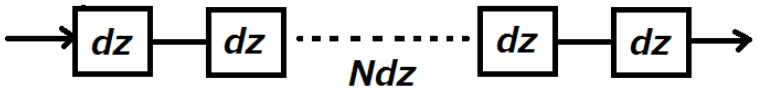


Рис. 3. Линия, разбитая на отдельные участки

Длина каждого участка *dz* должна быть подобрана так, чтобы его ФЧХ оказалась меньше 1. Тогда можно продолжить классический метод, и разложить (2) в ряд Тейлора. Кроме того, так как расстояние малое, можно ограничить ряд Фурье (1) одним членом:

$$e^{-j\sum_n c_n \sin(n\tau\omega)dz} \approx 1 - jc_1 \sin(\tau\omega)dz .$$

Применив формулу Эйлера, получим передаточную характеристику одного звена, у которого 3 слагаемых:

$$H_{dz}(j\omega) \approx 1 - \frac{c_1 dz}{2} e^{jn\tau\omega} + \frac{c_1 dz}{2} e^{-jn\tau\omega} = a_0 + a_{-1} e^{jn\tau\omega} + a_1 e^{-jn\tau\omega} . \quad (3)$$

Если умножить (3) на спектр исходного сигнала и сделать обратное преобразование Фурье, то получится выражение для сигнала, прошедшего через одно звено:

$$S(dz,t) = a_0 S(0,t) + a_1 S(0,t+\tau) + a_{-1} S(0,t-\tau) .$$

Каждое звено можно представить коротким КИХ-фильтром (рис. 4).

На вход каждого следующего звена будет подаваться сигнал с выхода предыдущего. Соответственно, прохождение сигнала через каждое звено будет порождать по одной новой паре откликов:

$$S([1]dz,t) = a_0 S([0]dz,t) + a_1 S([0]dz,t+\tau) + a_{-1} S([0]dz,t-\tau) .$$

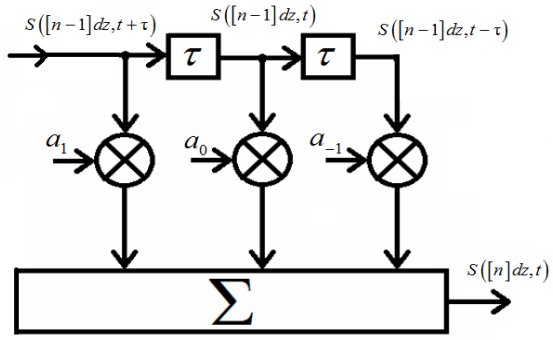


Рис. 4. Отдельное звено линии, представленное КИХ-фильтром

В итоге, в конце линии сигнал будет представлять собой сумму из пар эхо-сигналов, количеством равным числу звеньев:

$$S(Ndz,t)=\left[\sum_{k=0}^{K}(-1)^k c_{0k}a_0^{N-2k}a_1^{2k}\right]S(0,t)+$$

$$+\sum_{n=1}^{N}\left[\sum_{k=0}^{K}(-1)^k c_{nk}a_0^{N-(2k+n)}a_1^{2k+n}\right]S(0,t+n\tau)+$$

$$+\sum_{n=1}^{N}\left[\sum_{k=0}^{K}(-1)^k c_{nk}a_0^{N-(2k+n)}a_1^{2k+n}\right]S(0,t-n\tau). \qquad (4)$$

Коэффициенты при каждом эхо-сигнале можно получить по формуле:

$$c_{nk}=\frac{N!}{k!(k+n)!(N-2k-n)!},$$

где N – количество элементарных звеньев, n – номер отклика, k – номер слагаемого коэффициента при отклике и K – количество коэффициентов при отклике.

Таким образом, был получен метод представления модели эхо-сигналов в виде процесса формирования откликов на воздействие хроматической дисперсии в оптическом волокне. Его преимуществами, по сравнению с методом, описанном в [3], являются:

– Универсальность. Метод (4) можно использовать во всех случаях, в которых применима модель эхо-сигналов.

– Возможность применения в более широком диапазоне частот, поскольку нелинейная часть ФЧХ может быть аппроксимирована полиномом третей и большей степени.

Основным недостатком метода является накопление погрешности на каждом звене. Поэтому возникает необходимость её компенсации.

Список используемых источников

1. Баева Н. Н., Бобровская И. К., Брескин В. А., Якуб Ю. А. Основы многоканальной связи : учебник для вузов / Под ред. И. К. Бобровской. М. : Связь, 1975. 328 с.

2. Agrawal G.P. Nonlinear fiber optics (5th ed). Oxford; Waltham: Academic Press, 2013. 629 p. : ill. ISBN 978-0-12-397023-7.

3. Meltenisov M., Matukhin A. Analytical model of chromatic dispersion effect in the time domain // In: Proc. 18th International Conference on Advanced Communication Technology (ICACT). Phoenix Park, Republic of Korea, 2016. PP. 406–409.

УДК 681.3.066

ПОСТРОЕНИЕ ЭКРАНИРУЮЩЕГО МАРШРУТИЗАТОРА СООТВЕТСТВУЮЩЕГО ТРЕБОВАНИЯМ РУКОВОДЯЩЕГО ДОКУМЕНТА ФСТЭК РОСИИ

А. С. Мишин, Д. В. Юркин

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

В топологии любой крупной сети присутствует такой элемент, как маршрутизатор. Данное сетевое устройство выполняет такие задачи, как маршрутизация, фильтрация и фрагментация сетевых пакетов. Функциональные возможности современных маршрутизаторов очень высоки.

экранирующий маршрутизатор, UNIX, Netfilter, iptables.

ФСТЭК России – Федеральная Служба по Техническому и Экспортному Контролю. В её функции включен специальный контроль в некоторых областях. К сфере деятельности ФСТЭК относятся средства защиты информации без использования средств криптографии и не составляющих государственную тайну, т. е. обеспечение защиты информационной безопасности некриптографическими методами. В своем руководящем документе, ФСТЭК классифицирует экранирующие маршрутизаторы по пяти классам стойкости [1].

Устройства, соответствующие требованиям ФСТЭК имеют высокую стоимость, и потребитель не всегда может себе их позволить. Однако, построение экранирующего маршрутизатора, удовлетворяющего требованиям как минимум четвертого класса защищенности возможно и без значительных финансовых затрат.

Все, что требуется для создания данного устройства – персональный компьютер с установленной операционной системой (ОС) семейства UNIX. При этом для реализации не требуется дополнительное программное обеспечение. Вся настройка может быть выполнена исключительно штатными средствами UNIX.

Для маршрутизации пакетов в ОС UNIX используется набор утилит IPRoute2. Для фильтрации пакетов служит механизм Netfilter. Он включает

в себя ряд модулей, каждый из которых отвечает за определенный параметр фильтрации. Для удобства настройки, Netfilter имеет набор утилит. Так, за настройку модуля ip_tables отвечает утилита iptables, а за настройку модуля nf_conntrack утилита conntrack [2]. Полная схема механизма Netfilter представлена на (рис. 1).

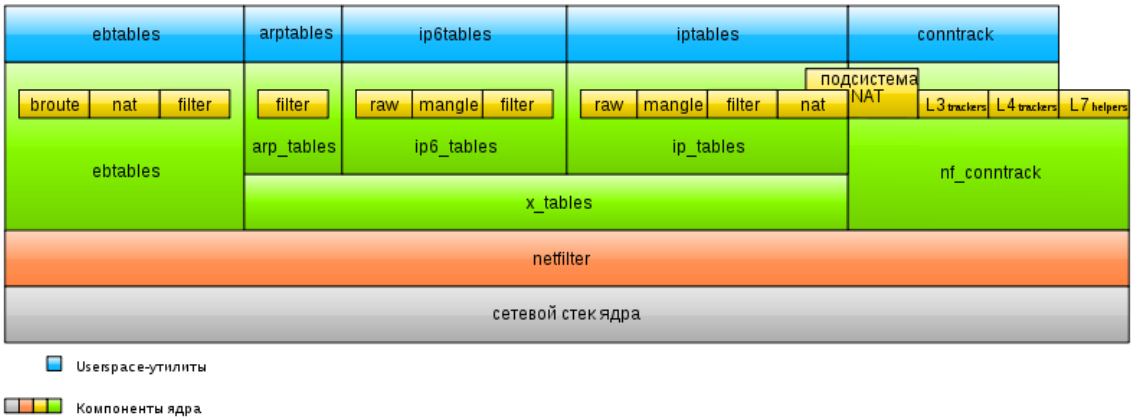


Рис. 1. Компоненты Netfilter

Требования ФСТЭК России к маршрутизаторам различных классов защищенности представлены в (табл.).

ТАБЛИЦА. Требования ФСТЭК к межсетевым экранам

Показатели защищенности	Классы защищенности				
	5	4	3	2	1
Управление доступом (фильтрация данных и трансляция адресов)	+	+	+	+	=
Идентификация и аутентификация	–	–	+	=	+
Регистрация	–	+	+	+	=
Администрирование: идентификация и аутентификация	+	=	+	+	+
Администрирование: регистрация	+	+	+	=	=
Администрирование: простота использования	–	–	+	=	+
Целостность	+	=	+	+	+
Восстановление	+	=	=	+	+
Тестирование	+	+	+	+	+
Руководство администратора защиты	+	=	=	=	=
Тестовая документация	+	+	+	+	+
Конструкторская (проектная) документация	+	=	+	=	+

Для построения экранирующего маршрутизатора 4 класса защищенности необходимо обеспечить фильтрацию на сетевом уровне. Это возможно реализовать инструментами iptables и conntrack. Созданный набор правил представлен на (рис. 2). По умолчанию, все входящие и проходящие транзитом пакеты отбрасываются. Разрешены лишь исходящие сетевые пакеты и те пакеты, которые соответствуют хотя бы одному из описанных правил. Если, пройдя по всей цепочке правил, сетевой пакет не был принят – он отбрасывается маршрутизатором. Таким образом, производится фильтрация сетевых пакетов по портам, по состоянию сетевого соединения, а также по входным интерфейсам.

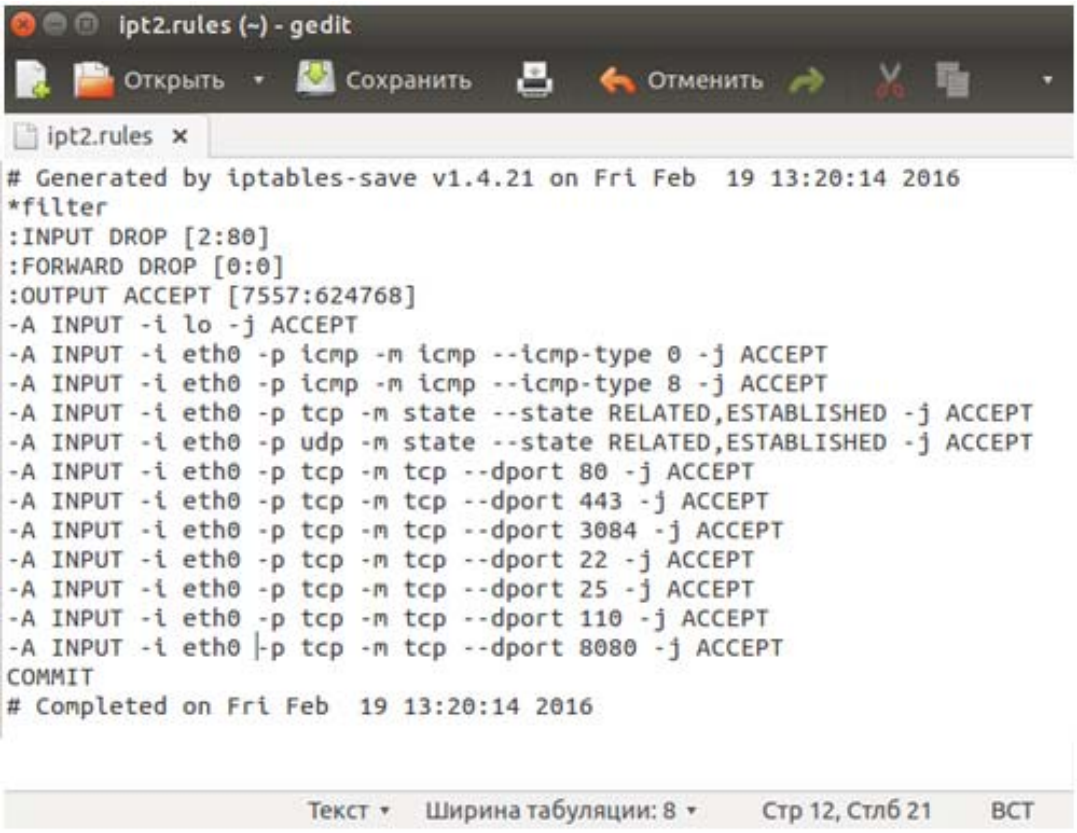


Рис. 2. Набор правил Iptables

Требования идентификации и аутентификации выполняются межсетевым экраном за счет системы доступа, позволяющей просматривать/редактировать настройки межсетевого экрана только администратору.

Регистрация действий осуществляется логированием. То есть автоматической записью любого действия системы в документ. Тонкая настройка механизма логирования доступна через утилиту iptables. Для соответствия требованиям ФСТЭК для четвертого класса защищенности достаточно включить логирование отброшенных пакетов командой: -A INPUT -i eth0 -j LOG --log-level debug --log-prefix «INPUT DROP:». Эта команда включает логирование событий в цепочке INPUT на интерфейсе eth0. Каждая запись

будет начинаться с префикса «INPUT DROP:» и содержать полную информацию об отброшенном пакете, включая адрес и время. Для цепочек правил FORWARD и OUTPUT необходимо включить логирование аналогичными командами, заменив название цепочки и префикс на FORWARD и OUTPUT соответственно.

Контроль целостности настроек экранирующего маршрутизатора возможен методом сравнения хэш-сумм системных файлов. Любое изменение в файле приведет к изменению его хэш-суммы. Таким образом, записанные значения хэш-сумм дают возможность в любой момент убедиться в целостности файлов. Команды «md5sum /etc/sysconfig/iptables» и «md5sum /etc/network/interfaces» выводят на экран контрольные суммы файлов iptables.rules и interfaces, которые, в свою очередь, хранят основные настройки маршрутизатора.

В случае несовпадения контрольных сумм системных файлов, восстановление свойств экранирующего маршрутизатора возможно благодаря команде «iptables-restore < /etc/sysconfig/iptables». Команда загружает настройки iptables из указанного файла. Сохранить все настройки в файл можно командой «iptables-save > /etc/sysconfig/iptables» (настройки будут сохранены в файл «iptables.rules», который будет располагаться в /etc/sysconfig/iptables).

Составление тестовой и конструкторской документации по построенному экранирующему маршрутизатору должно производиться лицом, выполнявшим настройку. Так как многие механизмы могут быть сконфигурированы под индивидуальные требования заказчика.

Тестирование построенного экранирующего маршрутизатора возможно так же, штатными средствами. Состояние портов позволяет контролировать утилита NMap. Информация обо всех отброшенных пакетах хранится в лог файле «Syslog», находящемся в каталоге /var/log. Процесс аутентификации администратора может быть протестирован при выполнении в терминале любой команды связанной с конфигурированием операционной системы. Все действия администратора записываются в файл «auth.log» находящийся в каталоге /var/log. Контролировать целостность позволяют хэш-суммы, получаемые командой «md5sum», а проследить за процедурой восстановления (при использовании «iptables-restore») можно при помощи команды просмотра правил iptables – «sudo iptables -L».

Таким образом, построение экранирующего маршрутизатора, соответствующего требованиям руководящего документа ФСТЭК России возможно штатными средствами операционной системы семейства UNIX. Для построения не требуется дополнительное программное обеспечение. Построенный маршрутизатор удовлетворяет требованиям 4 класса защищенности ФСТЭК России.

Список используемых источников

1. ФСТЭК России. «Средства вычислительной техники. Межсетевые экраны. Защита от несанкционированного доступа к информации. Показатели защищенности от несанкционированного доступа к информации.» Руководящий документ. Решение председателя Гостехкомиссии России от 25 июля 1997 г.

2. Andreasson O. Iptables Tutorial 1.1.19 [Электронный ресурс]; пер. с англ. : Андрей Киселев. 2001–2003. URL: http://www.opennet.ru/docs/RUS/iptables/ #STATEMACHINE (дата обращения 15.03.2016).

УДК 004.056

ИССЛЕДОВАНИЕ ВЕРОЯТНОСТНЫХ ХАРАКТЕРИСТИК КЛЮЧА, СФОРМИРОВАННОГО НА ОСНОВЕ КВАНТОВАНИЯ ВЫХОДА MIMO КАНАЛА

П. Д. Мыльников

Научно-исследовательский и проектно-конструкторский институт информатизации, автоматизации и связи на железнодорожном транспорте

Исследуются статистические характеристики ключа, полученного на основе оценивания случайных параметров коэффициентов передачи MIMO канала. На основе моделирования получены оценки коэффициента корреляции, найдены оценки энтропии Шеннона, энтропии Реньи, минимальной энтропии и статистического расстояния. Проведена оценка статистических характеристик ключа по графическим и оценочным тестам.

безопасность беспроводных сетей, MIMO каналы, распределение ключей, энтропия, статистические тесты, NIST STS.

В работах [1, 2] была исследована система формирования ключей, построенная на основе квантования фазы принимаемого сигнала на выходах MIMO канала. В данной работе проведено исследование статистических характеристик формируемого ключа.

Для исследования случайных последовательностей, применяются две группы тестов [3]:

1) Графические тесты – статистические свойства последовательностей отображаются в виде графических зависимостей, по виду которых делают выводы о свойствах исследуемой последовательности.

2) Оценочные тесты – статистические свойства последовательностей определяются числовыми характеристиками. На основе оценочных критериев делаются заключения о степени близости свойств анализируемой и истинно случайно последовательностей.

В дополнение к этим тестам представляет интерес исследование энтропии полученной последовательности и статистического расстояния по следующим формулам:

– энтропия Шеннона:

$$H(x) = -\sum_{i=1}^{n} p_i \log_2 p_i , \quad (1)$$

– энтропия Реньи:

$$H_2(x) = -\log_2 \sum_{i=1}^{n} p_i^2 , \quad (2)$$

– минимальная энтропия:

$$H_\infty(x) = -\log_2 \max_i p_i \quad (3)$$

– статистическое расстояние:

$$dif(P,Q) = 1/2 \sum_{i=1}^{n} |p_i - q_i| , \quad (4)$$

где p_i – распределение вероятностей для $i = 1, 2, \ldots, 2^N$ возможных комбинаций, $q_i = (½)^N$ – эталонное равномерное распределение.

Для исследования статистических характеристик последовательности, тестом «Проверка блоков» и по формулам (1)–(4), была сформирована бинарная последовательность длиной $1{,}6*10^6$ символов на основе системы формирования ключей со следующими параметрами: MIMO система 8 х 8, расстояние между антеннами в массиве – $\lambda/2$, скорость движения объекта – 100 км/ч, количество лучей – 8, частота несущей – 2,6 ГГц [1]. Результаты исследования представлены на рисунке 1 и в таблице 1.

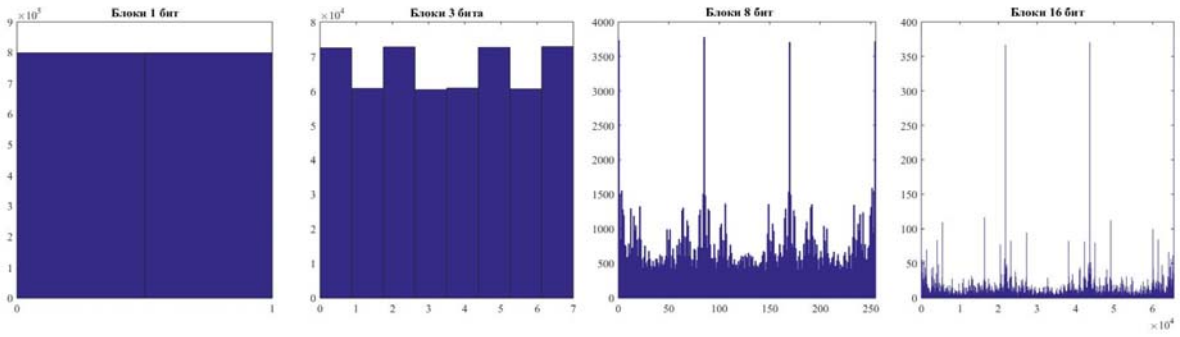


Рис. 1. Исследование статистических характеристик последовательности с помощью графического теста «Проверка блоков»

ТАБЛИЦА 1. Сводная таблица статистических оценок, полученных по сгенерированной последовательности до и после применения способа попарного объединения одинаковых разрядов, для разных блоков бит

	Статистические оценки до попарного объединения одинаковых разрядов				Статистические оценки после попарного объединения одинаковых разрядов			
	H	H_2	H_∞	*dif*	*H*	H_2	H_∞	*dif*
Блок 1 бит	1,00	1,00	1,00	6,10E-06	1,00	1,00	1,00	2,01E-05
Блок 2 бита	2,00	2,00	2,00	1,80E-04	2,00	2,00	2,00	5,71E-04
Блок 3 бита	2,99	2,99	2,88	4,29E-02	3,00	3,00	3,00	9,11E-04
Блок 4 бита	3,97	3,93	3,57	8,76E-02	4,00	4,00	3,97	6,79E-03
Блок 5 бит	4,97	4,94	4,39	6,40E-02	5,00	5,00	4,95	5,86E-03
Блок 6 бит	5,94	5,86	4,96	1,14E-01	6,00	6,00	5,89	8,78E-03
Блок 7 бит	6,94	6,86	5,57	8,27E-02	7,00	7,00	6,83	9,72E-03
Блок 8 бит	7,81	7,51	5,60	1,73E-01	8,00	7,99	7,56	2,51E-02
Блок 9 бит	8,91	8,72	6,53	1,11E-01	9,00	9,00	8,67	1,35E-02
Блок 10 бит	9,83	9,51	6,88	1,59E-01	10,00	10,00	9,53	1,74E-02
Блок 11 бит	10,86	10,53	7,37	1,32E-01	11,00	11,00	10,41	1,91E-02
Блок 12 бит	11,70	11,10	7,51	2,20E-01	12,00	11,99	11,05	2,83E-02
Блок 13 бит	12,81	12,29	8,22	1,57E-01	13,00	12,99	11,88	2,98E-02
Блок 14 бит	13,68	12,94	8,61	2,24E-01	13,99	13,98	12,60	4,12E-02
Блок 15 бит	14,74	14,01	9,14	1,91E-01	14,99	14,97	13,31	5,48E-02
Блок 16 бит	14,22	12,07	7,55	5,59E-01	15,95	15,88	12,61	9,04E-02

Как видно (рис. 1) в сформированной бинарной последовательности присутствуют закономерности, так, блоки длиной 3 и более символов не являются равномерно распределенными. В [4] предлагается несколько способов по устранению закономерностей в генерируемых последовательностях.

Первым способом является попарное объединение одинаковых разрядов нескольких случайных источников (рис. 2). Вторым способом для устранения неравномерного распределения является операция XOR нескольких битов последовательности друг с другом (рис. 3).

В результате статистических оценок до и после преобразования с помощью попарного объединения одинаковых разрядов можно увидеть улучшение статистических характеристик (табл. 1).

Анализ таблицы 1 показывает, что использование попарного объединения одинаковых разрядов для всех элементов MIMO массива оказывает влияние на статистические оценки, что особенно характерно для последовательностей, состоящих из блоков длиной 3 бита и более.

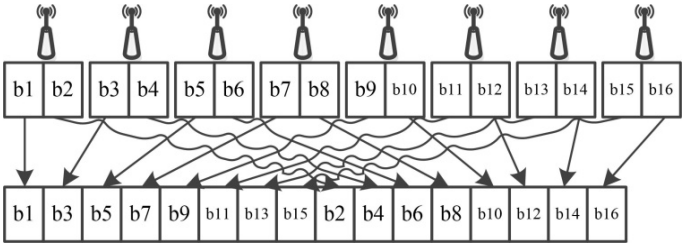


Рис. 2. Попарное объединение одинаковых разрядов для MIMO из восьми антенных элементов и $Q = 4$

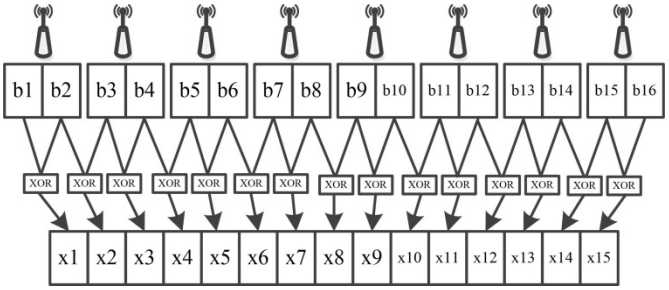


Рис. 3. Формирование последовательности путем попарного объединения одинаковых разрядов и операции XOR соседних разрядов

Дополнительно была проведена проверка оценки статистических характеристик на основе группы оценочных тестов NIST STS [5].

Пакет NIST STS включает в себя 15 статистических тестов, которые разработаны для проверки гипотезы о случайности бинарных последовательностей произвольной длины, порождаемых генераторами случайных чисел. Все тесты направлены на выявление различных дефектов случайности.

Основным принципом тестирования является проверка нулевой гипотезы H_0, заключающейся в том, что тестируемая последовательность является случайной. Альтернативной гипотезой H_a является гипотеза о том, что тестируемая последовательность не случайна. По результатам применения каждого теста нулевая гипотеза либо принимается, либо отвергается. Решение о том, что будут ли последовательности случайными или нет, принимается по совокупности результатов всех тестов.

Порядок тестирования отдельной бинарной последовательности S выглядит следующим образом:

1) Выдвигается гипотеза H_0 о том что последовательность S случайна.

2) По последовательности S вычисляется статистика теста $c(S)$.

3) С использованием специальной функции и статистики теста вычисляется значение вероятности $P = f(c(S))$, $P \in [0,1]$.

4) Значение вероятности P сравнивается с уровнем значимости α, $\alpha \in [0{,}001, 0{,}01]$. Если $P \geq \alpha$, то гипотеза H_0 принимается. В противном случае принимается гипотеза H_a.

Для исследования были сформированы 10 бинарных последовательностей, полученных как результат квантования фазы принимаемого сигнала, длиной 10^7 символов каждая. Результаты исследований представлены в таблице 2. В 3 и 4 столбцах указано количество последовательностей, которые успешно прошли тест после применения способов улучшения статистических характеристик.

ТАБЛИЦА 2. Результаты исследования случайных последовательностей, полученных в результате применения одного и двух способов улучшения статистических характеристик, с использованием группы оценочных тестов NIST STS

№	Наименование теста	Объединение разрядов	Объединение разрядов + XOR
1	Частотный тест	10/10	10/10
2	Частотный тест внутри блока	10/10	10/10
3	Проверка серий	9/10	10/10
4	Проверка максимальной длины серии в блоке	0/10	10/10
5	Проверка ранга двоичной матрицы	10/10	10/10
6	Спектральный тест	0/10	9/10
7	Проверка неперекрывающихся шаблонов	1/10	8/10
8	Проверка перекрывающихся шаблонов	0/10	10/10
9	Универсальный тест Маурера	10/10	10/10
10	Проверка линейной сложности	5/5	7/7
11	Последовательный тест	5/5	7/7
12	Энтропийный тест	0/10	10/10
13	Проверка накопленных сумм	3/10	10/10
14	Проверка случайных отклонений	1/10	10/10
15	Проверка случайных отклонений (вариант)	10/10	10/10

Из таблицы 2 следует, что только при использовании нескольких способов улучшения статистических характеристик последовательности, полученной в результате квантования фазы принимаемого сигнала на выходе MIMO антенны, можно сформировать истинно случайную последовательность, применимую для создания криптографического ключа.

Список используемых источников

1. Мыльников П. Д. Исследование характеристик системы формирования ключей для мобильных объектов железнодорожного транспорта на основе оценивания параметров MIMO канала // Известия Петербургского государственного университета путей сообщения. 2016. № 1. С. 31–39.
2. Яковлев В. А., Мыльников П. Д. Распределение ключей в беспроводных сетях с подвижными объектами на основе использования MIMO каналов с квантованием фазы сигнала // Проблемы информационно безопасности. Компьютерные системы. 2016. № 1. С. 102–113.
3. Иванов М. А., Чугунков И. В. Теория, применение и оценка качества генераторов псевдослучайных последовательностей. М. : КУДИЦ-ОБРАЗ, 2003. 240 с. ISBN 5-93378-056-1.
4. Шнайер Б. Прикладная криптография. М. : Триумф, 2002. 816 с. ISBN 5-89392-055-4.
5. A Statistical Test Suite for Random and Pseudorandom Number Generators for Cryptographic Applications. National Institute of Standards and Technology [Электронный ресурс]. URL: http://csrc.nist.gov/publications/nistpubs/800-22-rev1a/SP800-22rev1a.pdf (дата обращения 07.03.2016).

Статья представлена научным руководителем, доктором технических наук, профессором В. А. Яковлевым.

УДК 004.056

МЕТОДИКА ОПТИМИЗАЦИИ ПАРАМЕТРОВ СИСТЕМЫ ФОРМИРОВАНИЯ КЛЮЧА НА ОСНОВЕ КВАНТОВАНИЯ ФАЗЫ СИГНАЛОВ В MIMO КАНАЛЕ

П. Д. Мыльников[1], В. А. Яковлев[2]

[1]Научно-исследовательский и проектно-конструкторский институт информатизации, автоматизации и связи на железнодорожном транспорте
[2]Санкт-Петербургский государственный университет телекоммуникаций им. проф. М. А. Бонч-Бруевича

Исследуется способ распределения ключей в беспроводных сетях с подвижными объектами на основе использования MIMO каналов. Получены выражения для оценки вероятности правильного и ошибочного решения о фазе сигнала на выходе MIMO-антенны, при ее квантовании с защитным интервалом. Проведена оптимизация параметров системы, обеспечивающих наибольшую скорость формирования ключа при выполнении требований по вероятности совпадения ключей у двух корреспондентов.

безопасность беспроводных сетей, MIMO каналы, оптимизация, криптографический ключ.

Рассматривается MIMO-система с одинаковым числом передающих и приемных антенн N_A, с помощью которой выполняется обмен тест-сигналами между корреспондентами сети беспроводной связи. Оценки параметров канала, получаемые после тестирования, являются случайными величинами. Они могут быть использованы для формирования шифрключей [1].

Результаты исследования MIMO-системы связи мобильных объектов железнодорожного транспорта на основе оценивания параметров канала [2] показали возможность использования фазы принимаемого тест-сигнала для формирования шифрключей.

Фаза сигнала с выхода каждой MIMO-антенны, квантуется на Q уровней:

$$f_Q(\theta) = q, если: \theta \in \left[\left((q-1)\Omega + \gamma/2\right), \left(q\Omega - \gamma/2\right)\right], q = 1,...,Q,$$

где $\Omega = \dfrac{2\pi}{Q}$ – сектор квантования, $\gamma \in [0, \Omega)$ – защитный интервал.

В результате квантования принятый отсчет может оказаться в одной из трех областей принятия решения (рис. 1): *области правильного решения* ($\angle POM = D_0 \cup D_1' \cup D_1''$), *области стирания* ($\angle SOP = D_3$, $\angle MOF = D_2$) и *области ошибочного решения* (внешний угол $\angle SOF$).

В [3] получены формулы вероятностей попадания отсчета в области принятия решений (рис. 1) при квантовании фазы сигнала:

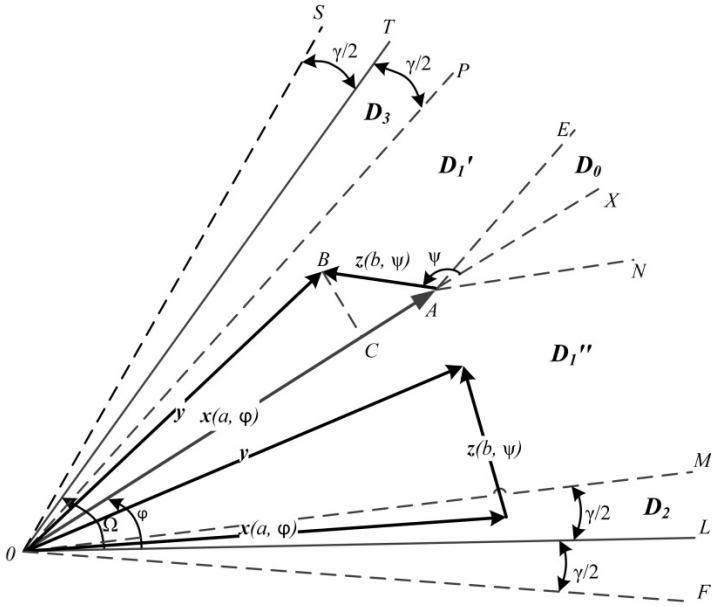


Рис. 1. Области принятия решения в секторе квантования Ω

$$P_{ош} = \frac{1}{2\pi\Omega}\int_0^{\Omega} d\varphi \int_{\varphi+\frac{\gamma}{2}}^{2\pi-\varphi-\frac{\gamma}{2}} d\psi \int_{\frac{\tan(\varphi+\frac{\gamma}{2})}{\sin\psi}}^{\infty} f(u)du,$$

$$P_{\text{пр}D_1} = \frac{1}{2\pi\Omega}\int_{\frac{\gamma}{2}}^{\Omega-\frac{\gamma}{2}} d\varphi \int_{\varphi-\frac{\gamma}{2}}^{2\pi-\varphi+\frac{\gamma}{2}} d\psi \int_{0}^{\frac{\tan(\varphi-\frac{\gamma}{2})}{\sin\psi}} f(u)du,$$

$$P_{\text{пр}D_2\cup D_3} = \frac{1}{2\pi\Omega}\int_{\Omega-\frac{\gamma}{2}}^{\Omega} d\varphi \int_{\varphi-\frac{\gamma}{2}}^{2\pi-\varphi+\frac{\gamma}{2}} d\psi \int_{\frac{\tan(\varphi-\Omega+\frac{\gamma}{2})}{\sin\psi}}^{\frac{\tan(\varphi-\frac{\gamma}{2})}{\sin\psi}} f(u)du,$$

$$P_{\text{пр}D_0} = \frac{1}{2\pi\Omega}\int_{\frac{\gamma}{2}}^{\Omega-\frac{\gamma}{2}} d\varphi \int_{0}^{\Omega-\gamma} d\psi \int_{0}^{\infty} f(u)du = \frac{(\Omega-\gamma)^2}{2\pi\Omega},$$

$$P_{\text{пр}D_2\to D_0} = \frac{1}{2\pi\Omega}\int_{0}^{\frac{\gamma}{2}} d\varphi \int_{\frac{\gamma}{2}}^{\Omega-\frac{\gamma}{2}} d\psi \int_{\frac{\tan(\frac{\gamma}{2}-\varphi)}{\sin\psi}}^{\infty} f(u)du,$$

$$P_{\text{пр}} = P_{\text{пр}D_1} + P_{\text{пр}D_2\cup D_3} + P_{\text{пр}D_0} + 2P_{\text{пр}D_2\to D_0},$$

$$P_{\text{ст}} = 1 - P_{\text{пр}} - P_{\text{ош}},$$

где $f(u) = \frac{2\delta^2 u}{(\delta^2+u^2)^2}$ – функция плотности вероятности распределения случайной величины *u*, являющаяся отношением двух релеевских распределений: шума и сигнала, $\sigma^2 = \frac{1}{h^2}$ – отношение шум/сигнал.

При попадании отсчета в область правильного решения или область ошибочного решения результат квантования фазы сигнала передается в мультиплексор, на выходе которого образуется поток двоичных отсчетов, из которых формируется ключ. При попадании отсчета в область стирания, результат квантования в мультиплексор не поступает. Номера стертых отсчетов для каждой антенны сохраняются до этапа согласования ключа. Для компенсации потери стертого отсчета передающая сторона передает дополнительный отсчет.

Вероятность успешного формирования ключа длиной n_0 двумя корреспондентами равна:

$$P(k) = (\tilde{P}_{\text{пр}}{}^2)^{\frac{n_0}{\log Q}}, \qquad (1)$$

где $\tilde{P}_{\text{пр}} = \frac{P_{\text{пр}}}{1-P_{\text{ст}}}$.

Эффективность системы формирования ключа будем определять скоростью его формирования, под которой будем понимать скорость потока отсчетов на выходе мультиплексора для системы из N_A антенн:

$$R = N_A \log Q(1 - P_{ст2}), \text{ [бит/обмен]} \qquad (2)$$

где $P_{ст2} = 2P_{ст} - P_{ст}^{\ 2}$ – вероятность стирания отсчета хотя бы одним корреспондентом.

Оптимизационной задачей для системы формирования ключей является нахождение максимальной скорости формирования ключа:

$$R \to \max$$

при выполнении требований на вероятность правильного формирования ключа $P(k) \geq P(k)_{треб}$ и его длину n_0.

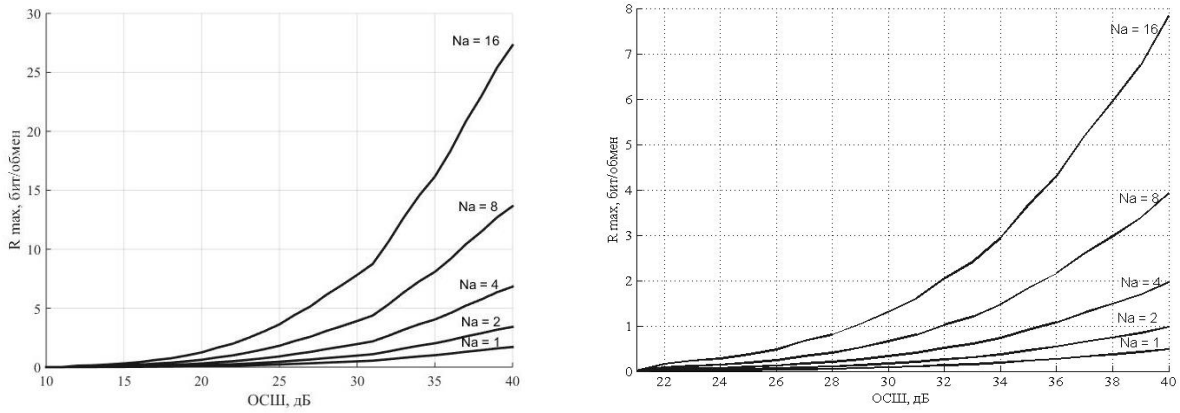
Величины $P(k)$ (1) и R (2) зависят от вероятностей $P_{пр} = f_1(\gamma, Q, h^2)$ и $P_{ст} = f_2(\gamma, Q, h^2)$, определяемых параметрами квантователя и характеристиками системы радиосвязи.

Тогда оптимизационная задача может быть записана так:

$$(\gamma^*, Q^*, N_A^*, h^{2*}) = \underset{\gamma, Q, h^2, N_A}{Arg} \max R,$$

при выполнении ограничений: $P(k) \geq P(k)_{треб}$; $0 \leq \gamma < 2\pi/Q$; $2 \leq Q \leq Q_{max}$; $1 \leq N_A \leq N_{Amax}$; $10 \leq h^2 \leq h^2_{max}$. Параметры Q_{max}, N_{Amax}, h^2_{max} определяются организационно-техническими требованиями к построению системы MIMO.

Задача (3) относится к задаче смешанной оптимизации: дискретной по N_A, Q и непрерывной по γ и h^2. Оптимизация проводилась на основе метода ветвей и границ. На рисунке 2 показаны зависимости R от отношения сигнал/шум (ОСШ) при формировании ключа длиной n_0 = 256 бит с $P(k)_{треб}$ = 0,9 и 0,99, для MIMO массивов из N_A = 1, 2, 4, 8, 16 антенн.



а) б)

Рис. 2. Скорость формирования ключа длиной 256 бит с: а) $P(k)_{треб}$= 0,9; б) $P(k)_{треб}$ = 0,99 и оптимальными параметрами системы

В таблице представлены оптимальные значения $\alpha^* = \frac{\gamma^*}{\Omega}$ и Q, при которых достигаются максимальные значения R для заданного значения ОСШ.

ТАБЛИЦА 1. Оптимальные параметры α* и Q^* для достижения максимального значения R при заданном значении ОСШ

		ОСШ, дБ										
$P(k)_{треб}$		12	16	20	22	26	30	32	34	36	38	40
0,9	Q^*	2	2	2	2	2	2	3	3	4	4	5
	α*	0,89	0,82	0,71	0,64	0,47	0,30	0,35	0,24	0,24	0,15	0,14
0,99	Q^*	–	–	–	2	2	2	2	2	2	2	2
	α*	–	–	–	0,89	0,82	0,71	0,64	0,57	0,48	0,39	0,30

Анализ графиков (рис. 2) показывает, что скорость формирования ключа возрастает с увеличением количества антенн в MIMO массиве. Естественно скорость формирования ключа возрастает с увеличением ОСШ, и для каждого значения ОСШ существуют оптимальные значения количества уровней квантования фазы Q и величины защитного интервала γ, при которых обеспечивается требуемая вероятность формирования ключа у обоих корреспондентов.

Список используемых источников

1. Jon W. Wallace, Rajesh K. Sharma. Automatic Secret Keys from Reciprocal MIMO Wireless Channels: Measurement and Analysis // IEEE Transactions on Information Forensics and Security. Vol. 5. No. 3. September 2010. PP. 381–391.

2. Мыльников П. Д. Исследование характеристик системы формирования ключей для мобильных объектов железнодорожного транспорта на основе оценивания параметров MIMO канала // Известия Петербургского государственного университета путей сообщения. 2016. № 1. С. 31–39.

3. Яковлев В. А., Мыльников П. Д. Распределение ключей в беспроводных сетях с подвижными объектами на основе использования MIMO каналов с квантованием фазы сигнала // Проблемы информационно безопасности. Компьютерные системы. 2016. № 1. С. 102–113.

УДК 004.021

ИССЛЕДОВАНИЕ МЕТОДОВ СТЕГОАНАЛИЗА ЦИФРОВЫХ ВИДЕОПОСЛЕДОВАТЕЛЬНОСТЕЙ

К. А. Небаева, Л. Г. Попов

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

В работе рассмотрены существующие методы стегоанализа цифровых видеопоследовательностей, основанные на различных подходах к обработке видеоданных, в которые было произведено вложение дополнительных бит информации. Представлен анализ данных методов обнаружения, возможность их практического применения в приложениях реального времени.

стеганография, стегоанализ, цифровая видеопоследовательность, линейная коллизия, временные корреляции, асимптотическое незапоминающее обнаружение, широкополосное вложение, мультипликативное вложение.

В настоящее время стеганография, используя сжатый видеопоток, может легко достигать большой ёмкости даже с низкими скоростями вложения. Поэтому всё большее внимание уделяется стегоанализу цифровых видеопоследовательностей.

Как правило, методы стегоанализа состоят из двух этапов:

– этап атаки на водяной знак, используемый для оценки исходного медиа;

– этап распознавания образов, используемый для обнаружения стеганографической активности.

Рассмотрим 5 различных методов стегоанализа цифровых видеопоследовательностей.

Стегоанализ цифрового видео, использующий статистическую видимость во временной области [1]

Оценка исходного видео происходит при помощи линейной коллизии, являющейся особым случаем коллизии, в котором оператор коллизии $\mathfrak{C}_P$ является средневзвешенной операцией над выбранными кадрами.

На рисунке 1 представлены основные этапы: атака коллизии $\mathfrak{C}_P$, разность между исходным (Y_k) и оценённым ($\widehat{U}_k$) кадрами, анализ остатка разности на присутствие вложения (классификатор образцов).

Интуитивно, линейная коллизия на последовательности видеокадров усиливает части фреймов, которые похожи и ослабляет компоненты, которые различны.

Для измерения качества оценки используется СКО (среднеквадратическая ошибка) – это вспомогательный сигнал архитектуры стегоанализа.

Считается, что более точная оценка водяного знака обычно будет иметь результатом более успешный стегоанализ в целом.

Атака линейной коллизии вычислительно проста, делая подход практически выполнимым для приложений реального времени.

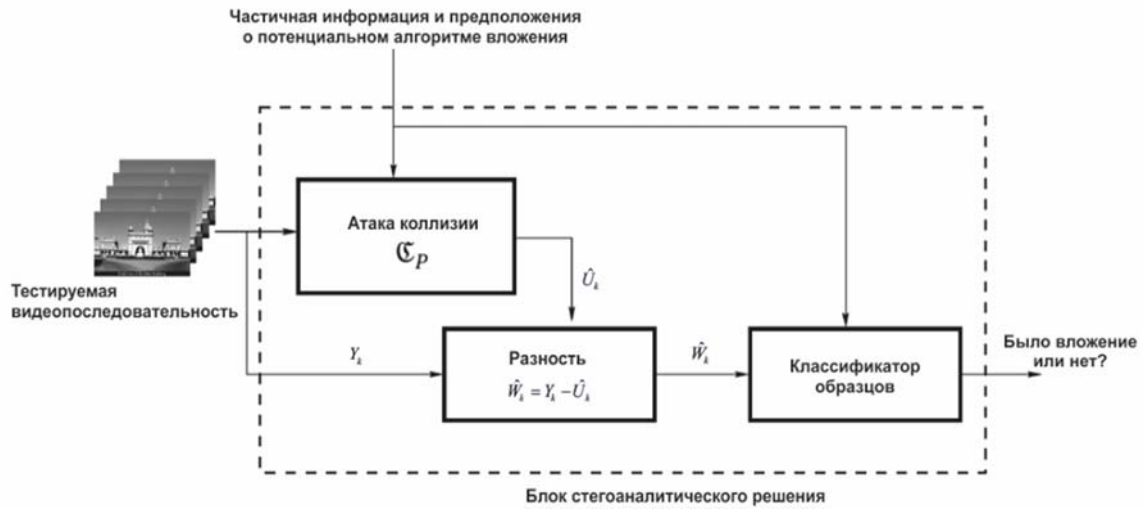


Рис. 1. Предлагаемый фреймворк для стегоанализа

Предполагается, что стеганография появляется при добавлении гауссовских водяных знаков, поэтому используются параметры, которые могут измерить уровень гауссовости в сигнале: эксцесс, энтропия и 25 процентиль [2].

Данный алгоритм стегоанализа использует преимущество временной избыточности, присутствующей в видео, что приводит к улучшенной эффективности, по сравнению с чисто пространственными методами.

Стегоанализ цифровых видео с использованием асимптотического незапоминающего обнаружения [3]

Общая схема стегоанализа изображена на рисунке 2.

Предполагается, что один из фреймов (F_n) оказывается потерянным из видео и нуждается в интерполяции. Использованием фреймов, расположенных в непосредственной близости, которые обозначаются как $F_n - 1$ и $F_n + 1$, восстанавливается оцениваемый фрейм $F_n^{\#}$. Метод оценки движения, который используется для сопоставления блоков – это техника суммы абсолютных разностей (САР – сумма абсолютных разностей). Этот метод простой концептуально, кроме того, даёт удовлетворительные результаты. После оценки получаем разность $\{Y\} = F_n - F_n^{\#}$, которая используется далее в детекторе.

Использование АОЭ (асимптотическая относительная эффективность) детектора требует знания нелинейности $g(x) = \sum_{i=0}^{M} \alpha_i \cdot x^i$. Эта нелинейность полиномиальная, где коэффициенты α_i могут быть получены,

как только эффективность η (мера производительности в тестах АОЭ) максимизирована.

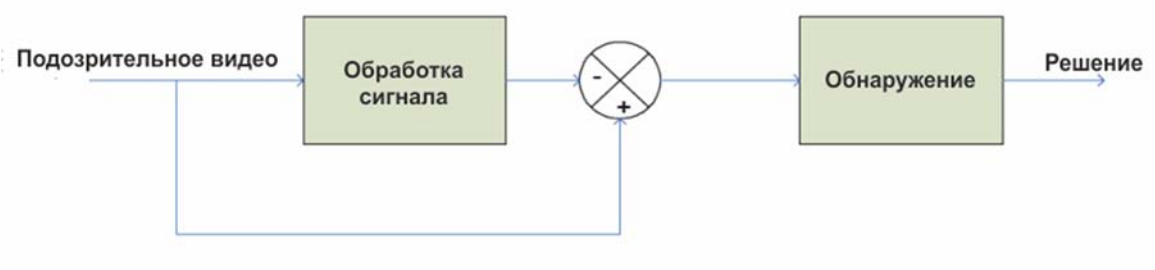


Рис. 2. Алгоритм стегоанализа

Особенность в том, что порог является изменяющимся в зависимости от характеристик: размер видео; стандартная девиация; его коэффициенты корреляции (см. рис. 3, где $H_0 : Y_i = N_i;\ H_1 : Y_1 = N_i + \theta \cdot S_i$, N_i и S_i – распределения шума и сигнала *i*-го фрейма (вложения), соответственно.)

Кроме того, учитывается количество кадров, которые должны быть проанализированы при каждом прохождении через детектор.

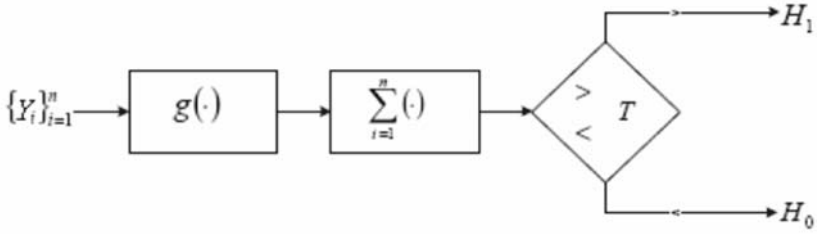


Рис. 3. Предлагаемый этап обнаружения

Видеостегоанализ, использующий параметры реверсии вектора движения [4]

Данный метод предназначен, для видеостеганографии, использующей вектора движения (*Motion Vectors* (MVs)). Представлен калибровочный подход, для осуществления динамического стегоанализа.

При декомпрессии стеговидео в пространственную область и сжатии его снова без вложения изменённые вектора движения возвращаются к своим предшествующим значениям. Поэтому MVs калиброванных видео имеют большинство макроскопических параметров, сходных с параметрами чистых видео.

Выполняется калибровка повторным сжатием, и основанные на реверсе параметры вектора движения получаются из разности между оригинальным и калиброванным видео.

При этом считается, что стеговидео будет иметь меньшую часть векторов движения с нулевым сдвигом и большую долю векторов движения с ненулевым сдвигом.

Улучшение видеостегоанализа путем использования временной корреляции [5]

Допускается идея о возможности адаптации существующих подходов слепого стегоанализа для неподвижных изображений к последовательности кадров, то есть к видео.

На рисунке 4 представлена схема основных этапов: предсказание скомпенсированного движения, чтобы получить PEFs (*prediction-error frames*); вычисление разности между PEFs и их пространственными предсказаниями; разложение результирующих фреймов с использованием 3-уровневого DWT (*discrete wavelet transform*); вычисление первых 3-х моментов характеристических функций (CFs – *characteristic functions*) в каждом поддиапазоне; использование полученных 39-размерных характеристических векторов для обучения классификатора образцов.

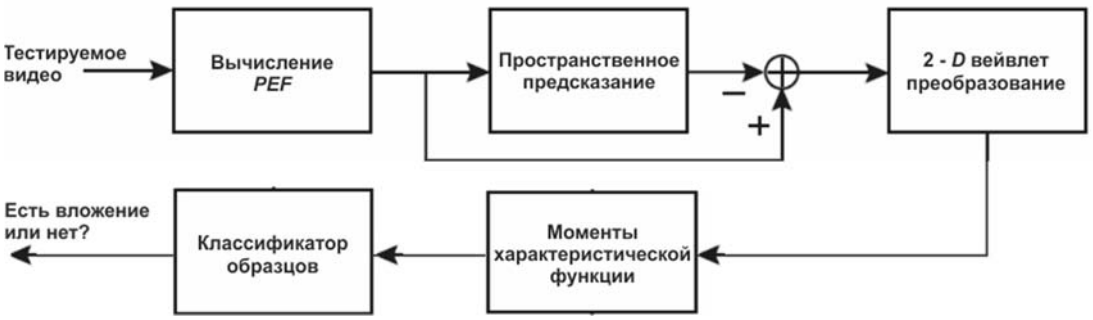


Рис. 4. Схема стегоанализа

Стегоанализ мультипликативной широкополосной стеганографии [6]

Предлагается метод видеостегоанализа по отношению к мультипликативному широкополосному вложению, так как он имеет большую устойчивость, чем аддитивное вложение.

Для оценки используются шумоподавление (а точнее стационарный вейвлет с мягким определением порога [7]) и межфреймовая оценка путём сопоставления блоков 8×8 (как в стандартах видеосжатия [8]).

После извлечения некоторых параметров (дисперсия остаточных значений, островершинность распределений и др.) из видеокадров и остаточной матрицы полученное видео классифицируется как «подозрительное» или «неподозрительное».

В случае «подозрительного» видео оценивается скрытое сообщение и глубина вложения, используемая на стороне вложения.

Используя оценённое скрытое сообщение и глубину вложения создаётся новая оценка видео, которая снова подаётся на вход системы (рис. 5). Следовательно, осуществляется повторная оценка покрывающего медиа, что приводит к более эффективному стегоанализу.

Рис. 5. Блок-схема предлагаемой системы стегоанализа

Таким образом, при стегоанализе видео применяются принципы, похожие на стегоанализ изображений, однако есть свои специфические особенности, связанные с областью (пространством), в которой приходится работать стегоаналитику.

Все рассмотренные методы подходят для практической реализации в обычных приложениях и показывают хорошие результаты обнаружения.

В будущем есть перспектива усовершенствовать методы для работы с быстро движущимися последовательностями и для применения к более широкому набору стеганографических подходов, т. е. повысить универсальность.

Список используемых источников

1. Budia U., Kundur D., Zourntos T. Digital Video Steganalysis Exploiting Statistical Visibility in the Temporal Domain // IEEE Transactions on Information Forensics and Security. 2006. Vol. 1, No. 4. PP. 502–516.

2. Papoulis Probability A. Random Variables and Stochastic Processes. 4th ed. New York : McGraw-Hill, 2002. 678 p.

3. Jainsky J. S., Kundur D., Halverson D. R. Towards Digital Video Steganalysis using Asymptotic Memoryless Detection // Proceedings of the 9th International Workshop on Multimedia and Security, Dallas, TX, USA, 2007. PP. 161–168.

4. Cao Y., Zhao X., Feng D. Video Steganalysis Exploiting Motion Vector Reversion-Based Features // IEEE Signal Processing Letters. 2012. Vol. 19. No. 1. PP. 35–38.

5. Pankajakshan V., Ho A. T. S. Improving Video Steganalysis using Temporal Correlation // Proceedings of the 3rd International Conference on Intelligent Information Hiding and Multimedia Signal Processing. 2007. Vol. 1. PP. 287–290.

6. Zarmehi N., Akhaee M. A. Video steganalysis of multiplicative spread spectrum steganography // Proc. 22th European Signal Processing conference. Lisbon. 2014. PP. 2440–2444.

7. Donoho D. L. De-noising by soft-thresholding // IEEE Trans. on Information Theory. 1995. Vol. 41, No. 3. PP. 613–627.

8. Yang J., Yin B., and Zhang N. A block-matching based intra frame prediction for h.264/avc // IEEE International Conference on Multimedia and Expo, July 2006. PP. 705–708.

УДК 654.173

СТЕГАНОГРАФИЯ В IP-ТЕЛЕФОНИИ И СЛОЖНОСТИ ЕЕ РЕАЛИЗАЦИИ

К. А. Небаева, С. А. Скородумов

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

В статье рассматривается возможность использования потоковых контейнеров для встраивания скрытой информации, а именно пакеты данных, передающихся в режиме реального времени по протоколу прикладного уровня RTP. Данный протокол рассматривается как основной стандарт для передачи голоса и видео в IP-сетях и совместно с кодеками.

цифровая стеганография, IP-телефония, RTP.

Методы стеганографии уже известны несколько веков, и благодаря развитию цифровых технологий, стал стремительно развиваться новый вид скрытой передачи данных – сетевая стеганография (рис. 1). Основой является вложение дополнительной информации в цифровые объекты. При этом происходит искажение конечного файла. Стоит отметить, что уровень данных искажений находится за чертой восприятия человека. Это не приводит к значительным изменениям объекта, что усложняет и затрудняет поиски, а также разоблачение [1].

Анализ последних исследований и публикаций показывает, что существующие стеганографические методы IP-телефонии были разработаны и внедрены из двух других, разных по происхождению исследований [2]. Во-первых, из традиционных графических и звуковых стеганографических контейнерах. Во-вторых, из скрытых каналов других сетевых протоколов (например, SIP-протокол, а также протоколы RTP и RTCP).

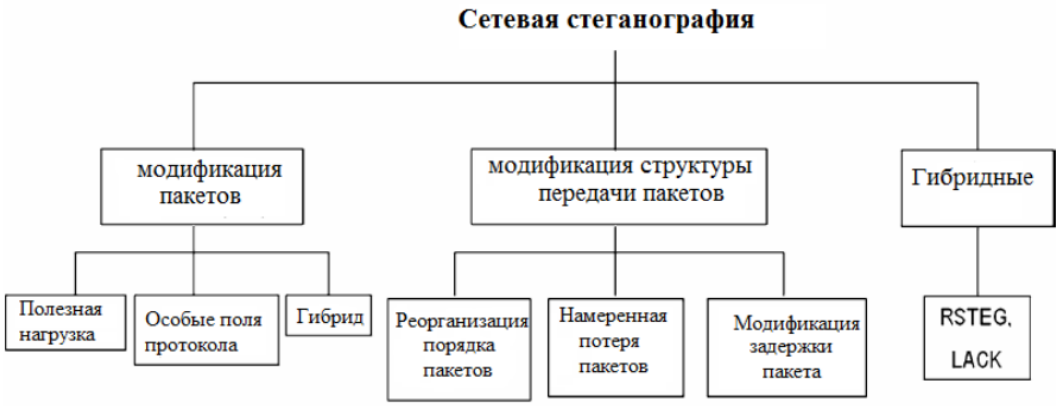


Рис. 1. Классификация методов сетевой стеганографии

Методы сетевой стеганографии можно разделить на три группы:

1) методы стеганографии, суть которых в изменении данных в полях заголовков сетевых протоколах и в полях полезной нагрузки пакетов (рис. 2);

2) методы стеганографии, в которых изменяется структура передачи пакетов, например, изменяются очередности передачи пакетов или преднамеренное введение потерь пакетов при их передаче;

3) смешанные (гибридные) методы стеганографии – при их применении изменяются содержимое пакетов, сроки доставки пакетов и порядок их передачи.

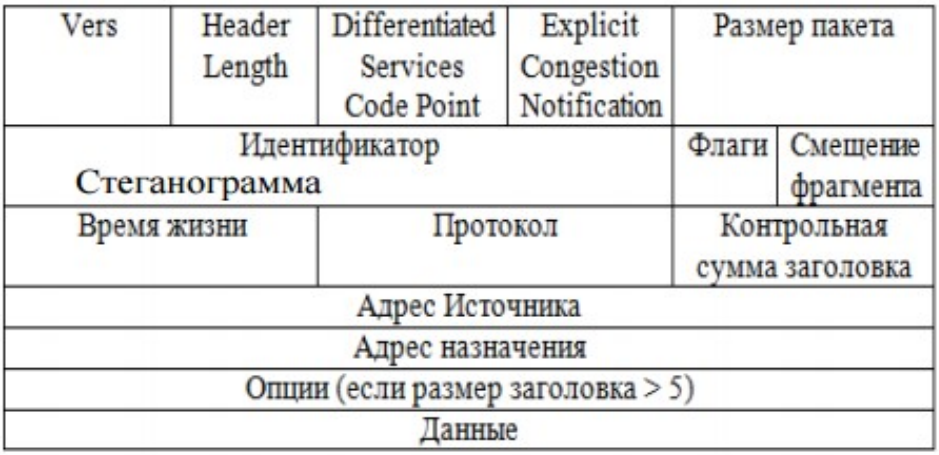


Рис. 2. Метод модификации полей IP-заголовка

Каждый из этих методов делится ещё на несколько групп; например, методы модификации пакетов включают в себя три разных метода:

1) методы изменения данных в полях заголовков протокола: они основаны на модификации полей заголовков IP, TCP, SCTP и так далее;

2) методы модификации полезной нагрузки пакета; в этом случае применяются всевозможные алгоритмы водяных знаков, речевых кодеков и прочих стеганографических техник по скрытию данных;

3) методы смешанных техник.

Методы модификации структуры передачи пакетов включают в себя три направления:

1) методы, в которых изменяется порядок последовательности пакетов;

2) методы, изменяющие задержку между пакетами;

3) методы, суть которых заключается во введении преднамеренной потери пакетов путём пропуска порядковых номеров у отправителя;

4) смешанные (гибридные) методы стеганографии используют два подхода: методы потери аудио пакетов (LACK) и ретрансляция пакетов (RSTEG);

5) методы сетевой стеганографии с модификацией пакетов.

Существует несколько решений/способов для возможности скрытой передачи данных внутри сети [1]:

1) Использование стеганографических методов в VoIP, которые используют голосовой поток как скрытый носитель информации. Метод называется SteganRTP [3] и заключается во встраивании стеганограмм, используя наименьший значащий бит кодека G.711. Позже было предложено так же использование младших битов, но уже кодека Speex;

2) Метод HICCUPS (*Hidden Communication system for CorrUPted networkS*) [2]. Этот метод использует несовершенства передачи данных в сетевом окружении, такие как помехи и шум в среде связи, а также обычную подверженность данных к искажению.

HICCUPS является стеганографической системой с распределением пропускной способности в общественной сетевой среде. Беспроводные сети более восприимчивы к искажению данных, чем проводные, поэтому использование помех и шума в среде связи выглядит очень заманчиво.

В частности, беспроводные сети используют воздушное соединение с переменной частотой ошибок в битах (BER), что создаёт возможность вводить искусственно поврежденные кадры. В целом, новшества HICCUPS следующие:

– использование безопасных сетевых телекоммуникаций с криптографическими механизмами для обеспечения работы системы стеганографии;

– предложение нового протокола с распределением пропускной способности для стеганографических целей, основанных на испорченных пакетах.

Этот метод обладает низкой полосой пропускания (зависит от сети), громоздкой реализацией, низкой стеганографической стоимостью и высокой сложностью обнаружения. Тем не менее, анализ кадров с неверной контрольной суммой может привести к обнаружению использования данного метода.

3) Система LACK [4]. Принцип функционирования выглядит следующим образом. Передающая сторона выбирает один из пакетов голосового потока, и его полезная нагрузка заменяется битами секретной информации, стеганограммой, которая затем встраивается в пакет. Затем выбранный пакет намеренно задерживается. Каждый раз, когда пакет чрезмерно задерживается, он отбрасывается получаемой стороной. Однако это в том случае, если получаемая сторона не знакома с стеганографической процедурой. Получатель знает об этом, поэтому вместо удаления полученных RTP пакетов, извлекает скрытую информацию. Пропускная способность данного метода позволяет производить вложение около 1,4 Мб данных примерно за 9 минут (это средняя продолжительность вызова в IP-телефонии) [1]. Соответственно, чем больше скрытой информации нужно положить в голосовой поток за тот же промежуток времени, тем больше вероятность обнаружения

сканированием потока данных или применением другого метода стегоанализа. Так же, при увеличении количества используемых пакетов, качество связи будет ухудшаться.

Лучшим выбором для LACK целей является кодек G.711. Он может поддерживать потери пакетов более 5 % и при этом обеспечить приемлемое качество голоса. Одновременно, на основе G.711 LACK обеспечивает наибольшие стеганографические пропускные способности. Например, при потере пакетов на уровне 1 % он обеспечивает около 590 бит/с. Такая производительность достигается тем, что размер полезной нагрузки каждого пакета RTP составляет 160 байт, что значительно больше, чем при использовании любого другого выбранного кодека. Сравнение скорости передачи стеганограммы различными кодеками, в зависимости от потери пакетов (рис. 3) [3].

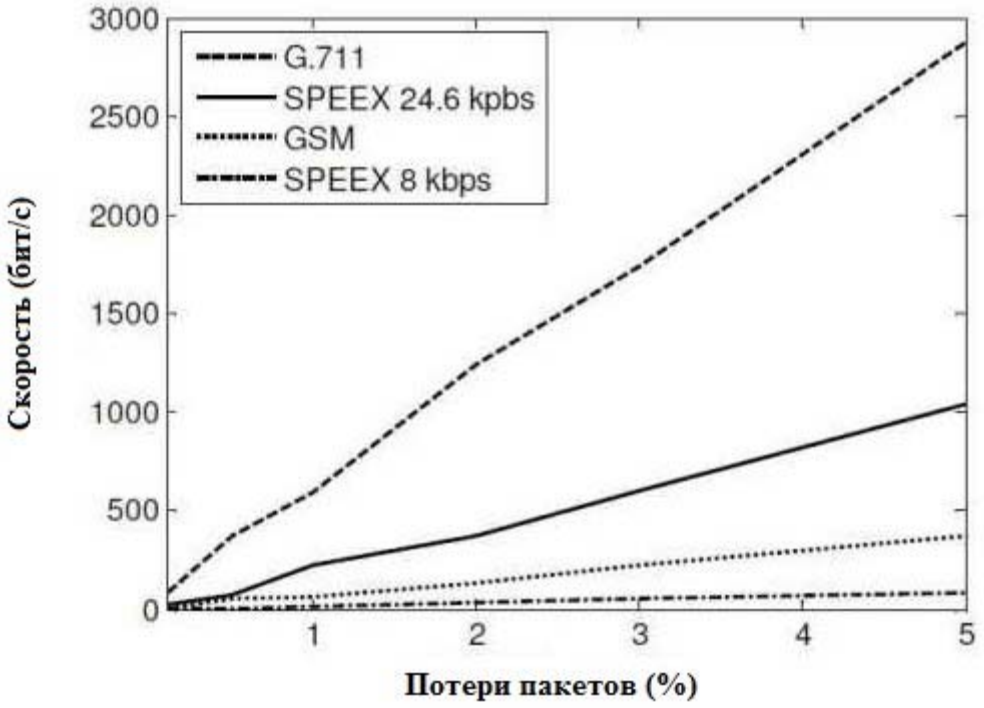


Рис. 3. Зависимость потери пакетов от скорости передачи и выбранном кодировании

В непрерывном потоке данных самая большая сложность для получателя – определить, когда начинается скрытое сообщение. При наличии в потоковом контейнере сигналов синхронизации или границ пакета, скрытое сообщение начинается сразу после одного из них. В свою очередь, для отправителя возможны проблемы, если он не уверен в том, что поток контейнера будет достаточно долгим для размещения целого тайного сообщения [5].

Производительность зависит от нескольких факторов:

– тип используемого кодека, в частности устойчивость к потере пакетов и качество голоса по умолчанию;

– размер полезной нагрузки RTP пактов и размер джиттер-буфера;

– сетевые факторы, связанные с задержкой пакетов и вероятностью потерь;

– LACK факторы, связанные с намеренно задержанными пакетами.

Стегоанализ LACK проблематичен. Это связано с тем, что потери пакетов в сети – это частое и обычное явление. Но потенциальные методы стегоанализа LACK должны включать в себя:

– статический анализ потерянных пакетов для звонков в подсети;

– статический анализ продолжительности VoIP вызовов;

– активное наблюдение и анализ всех протоколов RTP, которые были задержаны продолжительное время.

Сетевая стеганография позволяет скрывать секретные сообщения внутри трафика VoIP без серьезного ухудшения качества голосовой связи. Проведенные исследования показывают, что протокол RTP представляет для этих целей широкие возможности, как на уровне передачи RTP пакетов, так и на самой структуре пакета. В обоих случаях используются уязвимые места в данном протоколе. Полученные результаты могут быть использованы в качестве основы для разработки новых методов стеганографии и для защиты информации от утечек по скрытым каналам связи.

Список используемых источников

1. Коркач И. В., Пирогова Ю. И. Использование технологий IP-телефонии для скрытой передачи информации // Информационная безопасность человека, общества, государства. 2012. Т. 9. N 2. С. 124–128.

2. Пескова О. Ю., Халабурда Г. Ю. Применение сетевой стеганографии для защиты данных, передаваемых по открытым каналам Интернет [Электронный ресурс] // URL: http://www.gosbook.ru/system/files/documents/2013/03/19/57PeskovaKhalaburda.pdf (дата обращения 01.04.2016).

3. Pontón Loaiza M. M. Steganography using RTP packets [Электронный ресурс] // MSc. Ethical Hacking & Computer Security. 2014. URL: http://repositorio.educacionsuperior.gob.ec/bitstream/28000/1677/1/T-SENESCYT-00795.pdf (дата обращения 10.04.2016).

4. Mazurczyk W., Lubacz J. LACK – a VoIP steganographic method [Электронный ресурс] // Warsaw University of Technology. URL: http://cygnus.tele.pw.edu.pl/~wmazurczyk/art/LACK_journal_final.pdf (дата обращения 01.04.2016).

5. Генне О. В. Основные положения стеганографии [Электронный ресурс] // Защита информации. Конфидент. 2000. N 3. URL: http://www.citforum.ru/internet/securities/stegano.shtml (дата обращения 10.04.2016).

УДК 621.391.63
621.395.52

ВОПРОСЫ НОРМИРОВАНИЯ ОПТИЧЕСКОГО ТРАКТА С УСИЛИТЕЛЯМИ

Б. К. Никитин, А. Н. Сергеев, Г. М. Смирнов

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

В статье рассмотрены вопросы нормирования компонентов волоконно-оптической линии передачи с оптическими усилителями. Приведены основные требования к техническим характеристикам оптических сигналов в точках нормирования, к передающим и приёмным устройствам, а также к оптическому тракту. Рассмотренные вопросы востребованы при проектировании линий связи. Кроме того, знание норм необходимо при технической эксплуатации волоконно-оптических линий передачи, работающих с технологией синхронной цифровой иерархии уровней STM-4, 16, 64.

Нормирование ВОЛС, элементарный кабельный участок, ЭКУ, оптический тракт, потери, дисперсия, накопленная дисперсия, затухание, джиттер, MPI-S, MPI-R, ПМД, поляризационно-модовая дисперсия, оптический интерфейс, точка нормирования, код применения, отношение «сигнал-шум», шум-фактор, передающее устройство, приёмное устройство, коэффициент дисперсии, ВОЛС, ВОЛП, ВОЛТ.

Для увеличения скоростей передачи по ВОЛС независимо от ее протяженности в настоящее время применяются самые разные технологии. Эта задача решается одновременно с двух сторон, с одной –это увеличение скорости работы активных устройств, а с другой – оценка и снижение влияния факторов, ограничивающих время распространения сигнала вдоль среды передачи.

При проектировании современных волоконно-оптических линий передачи необходимо учитывать оба вышеуказанных ограничения.

Отсюда возникает необходимость нормирования состояния параметров оптического тракта по указанным критериям, которое задаёт пределы ухудшения его технических характеристик при проектировании, строительстве и последующей эксплуатации, соответствующие требованиям качества передачи различных видов информации.

Нормирование технических характеристик выполняется как для систем без применения оптических усилителей, так и для более сложных систем с оптическими усилителями разного типа и назначения или систем, работающих по технологии спектрального уплотнения.

В первом случае, в системах, где происходит относительно простая оценка технических характеристик элементарного кабельного участка (ЭКУ), основными критериями являются:

– общее затухание и коэффициент затухания в оптических волокнах соединённых каскадом;

– максимально допустимая дисперсия и дисперсия, накопленная при прохождении сигнала по оптическому волокну [1].

Задача поддержания технических характеристик в пределах нормы становится главной для качественной передачи цифровых потоков. Под качеством передачи понимается максимально допустимый коэффициент ошибок при приёме, который часто в волоконно-оптических системах SDH оценивается в виде BER (коэффициентов ошибок по битам) или BBER (коэффициент ошибок по блокам с фоновыми ошибками). При любых сочетаниях значений параметров оптических стыков для различных оптических интерфейсов коэффициент ошибок BER в тракте должен быть не более $1x10^{-12}$.

Нормирование характеристик таких участков выполняется для комбинации, включающей в себя одну из 2-х длин волн (1310 нм и 1550 нм), одно из 3-х типов одномодовых оптических волокон (стандартное волокно, волокно с нулевой смещённой дисперсией или волокно с затуханием, минимизированным на длине волны 1550 нм) и 5 длин элементарного кабельного участка (внутриобъектовая связь *I*, короткий участок *S*, длинный *L*, очень длинный *V* и сверхдлинный *U*).

Общие требования к построению линейного оптического тракта приведены в [2].

В соответствии с рисунком в линейном оптическом тракте существуют некоторые точки, в которых оценивается значение передаваемого сигнала. К этим точкам относятся *MPI-S, R′, S′* и *MPI-R*. Значения задаваемых параметров в этих точках указаны в таблицах 1 и 2.

Для оптических стыков волоконно-оптической системы передачи с оптическими усилителями по кодам *V* и *U* дополнительно определяются следующие параметры:

– отношение оптических сигнал/шум;

– поляризационно-модовая дисперсия на элементарном кабельном участке.

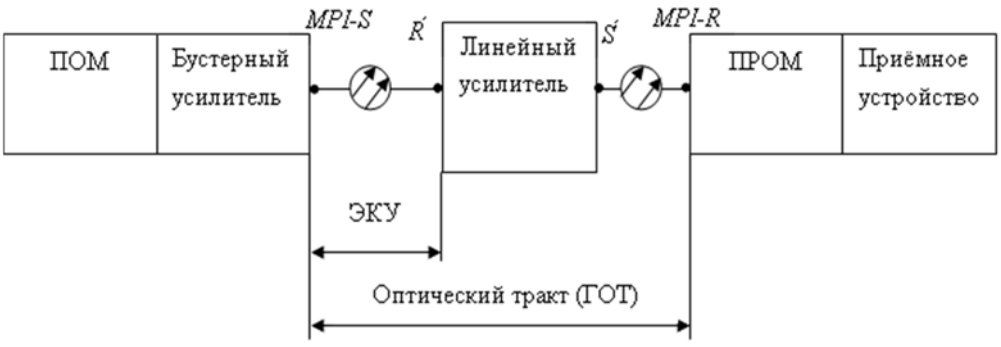


Рисунок. Схема волоконно-оптической линии передачи с одним оптическим усилителем

ТАБЛИЦА 1. Технические требования к параметрам оптических стыков в точках нормирования *MPI-S* и S′

Точка нормирования	*MPI-S*	*S′*
Наименование параметров	Значение параметров	
Уровень мощности на один оптический канал, не более, дБ	+20,0	+20,0
Отношение оптических сигнал/шум, не менее, дБ	20,0	20,0

ТАБЛИЦА 2. Технические требования к параметрам оптических стыков в точках нормирования *MPI-R* и *R′*

Точка нормирования	*MPI-R*	*R′*
Наименование параметров	Значение параметров	
Уровень мощности на один оптический канал, не более, дБ	–36,0÷–15,0	–36,0÷–15,0
Отношение оптических сигнал/шум, не менее, дБ	18,0	18,0

Первый параметр оценивается для следующих точек оптического тракта – в точке MPI-S и в точках S' на выходе каждого промежуточного оптического усилителя – по следующим формулам:

$$OSNR = 19 + x + 10\lg x \text{дБ}, \qquad \text{для точки } MPI - S$$

$$OSNR = 19 + x - k + 10\lg\frac{x}{k+1}, \text{дБ} \qquad \text{для точек } S'$$

В этих формулах k – порядковый номер промежуточного оптического усилителя, а x – максимальное число оптических усилителей в тракте [3]. Первым фактором, ограничивающим перекрываемое расстояние, служит дополнительный шум, вызванный работой оптических усилителей. Через несколько усилителей суммарное отношение сигнал/шум снизится до неприемлемого уровня.

Второй влияющий фактор – поляризационно-модовая дисперсия (ПМД) – действует при высоких скоростях передачи. Ввиду того, что ПМД имеет случайный характер, её величину оценивают максимально допустимыми накопленными значениями, которые приведены в таблице 3 [1].

ТАБЛИЦА 4. Величина накопленной ПМД для оптических интерфейсов

Оптический интерфейс	*V*-4.2, *V*-4.3, *U*-4.2, *U*-4.3	*V*-16.2, *V*-16.3, *U*-16.2, *U*-16.3	*S*-64.1,*S*-64.2,*S*-64.3, *L*-64.2*a*, *L*-64.2*b*
Максимальное значение ПМД, пс	160	40	10

Перекрываемое затухание между точками ГПд и ГПр для ВОСП без промежуточных оптических усилителей в зависимости от типа применения не должно превышать на один ЭКУ:

для кодов *L* – 22 дБ, для *V* – 33 дБ, для *U* – 44 дБ.

Перекрываемое затухание между точками MPI-S и *R′, S′ и R′, S′* и *MPI-R* для ВОСП с промежуточными оптическими усилителями в зависимости от типа применения не должно превышать (на один ЭКУ):

для кодов *L* – 22 дБ и для кодов *V* – 33 дБ.

Суммарная дисперсия между точками MPI-S и MPI-R, MPI-S и *R′, S′* и *R′, S′* и MPI-R в зависимости от типа применения не должна превышать (на один ЭКУ):

для кодов *L* – 1600 пс/нм, для кодов *V* – 2400 пс/нм, для кодов *U* – 3200 пс/нм.

Для уменьшения дисперсии в оптическом тракте с кодами *V*-64.2*a* и *L*-64.2*a* применяется пассивный компенсатор дисперсии (во втором коде может также использоваться принудительное смещение центральной частоты), а в тракте с кодами *V*-64.2*b* и *L*-64.2*b* – самомодуляция фазы.

После этого требуется произвести расчёт основных показателей сигнала в разных точках нормирования и сравнить полученные результаты с нормами, приводимыми в [2]. Если хотя бы один из них выходят за пределы, то необходимо внести изменения в проект будущей трассы (при проектировании) либо произвести ремонт (при эксплуатации).

Список используемых источников

1. Сергеев А. Н. Об особенностях расчёта и проектирования ВОЛС в одноканальных системах SDH // Международная конференция «Современные технологии проектирования, строительства и эксплуатации линейно-кабельных сооружений СТЛКС-2011», Санкт-Петербург, 2011.

2. ОСТ45.178-2001 Системы передачи с оптическими усилителями и спектральным уплотнением. Стыки оптические. Классификация и основные параметры. Введ. 2001-08-01.

3. Никитин Б. К., Смирнов Г. М., Глаголев С. Ф. Современные технологии строительства и эксплуатации ВОЛС. Федеральное агентство связи, Федеральное гос. бюджетное образовательное учреждение высш. проф. образования «Санкт-Петербургский гос. ун-т телекоммуникаций им. проф. М. А. Бонч-Бруевича». СПб. : СПбГУТ, 2012. 106 с. : ил.

УДК 621.39

ОЦЕНКА ПОМЕХОУСТОЙЧИВОСТИ КАНАЛОВ СВЯЗИ С ЗАМИРАНИЯМИ И РАЗНЕСЕННЫМ ПРИЕМОМ

О. А. Остроумов[1], Н. В. Савищенко[2]

[1]Военная академия связи им. Маршала Советского Союза С. М. Буденного
[2]Санкт-Петербургский государственный университет телекоммуникаций им. проф. М. А. Бонч-Бруевича

Статья посвящена методики оценки помехоустойчивости декаметровых каналов радиосвязи при разнесенном приеме многопозиционных сигналов. Получены точные выражения расчета вероятности ошибки в канале связи в условиях замираний Райса и Релея. Обосновывается использование различных видов разнесенного приема для улучшения качества связи.

замирания, разнесенный прием, вероятность ошибки, многопозиционные сигналы.

На надежность и качество связи в любом диапазоне волн существенное влияние оказывают помехи. Существует много способов защиты от помех [1]: предотвращение перегрузки приемников; компенсация радиопомех; различного рада селекцией сигналов; адаптацией; перестройкой радиочастоты; использование шумоподобных сигналов и т. д.

Одним из наиболее эффективных и часто используемых методов борьбы с помехами и замираниями радиоволн, средством повышения помехоустойчивости, достоверности и надежности связи является разнесенный прием. В случае если в канале связи замирания сигнала отсутствуют, помехоустойчивость при разнесенном приеме определяется степенью корреляции помехи в отдельных ветвях разнесения, также возникает дополнительная возможность повышения помехоустойчивости за счет слабой корреляции сигнала в отдельных ветвях разнесения [андронов].

В системах с разнесенным приемом обеспечивается параллельная передача одной и той же информации по нескольким ветвям разнесения. Выделяют шесть видов разнесенного приема: по пространству, по времени и частоте, по углу прихода лучей, по поляризации и по отдельным лучам при многолучевом распространении.

Лучше всего на качество связи влияет использование пространственного разнесенного приема и поляризационного разнесенного приема. В этом случае максимально эффективно используется мощность передатчика. Временной и частотный разнесенный прием уступает пространственному разнесению по устойчивости. При временном разнесении, неизменной скорости и мощности передатчика длительность элемента уменьшается в L раз, тот же результат при частотном разнесении, если для каждой ветви ис-

пользуется свой передатчик. При частотном разнесенном приеме, реализованном на одном передатчике, мощность передатчика используется хуже. Однако, почти всегда, использование разнесенного приема позволяет повысить качество связи, без увеличения мощности передатчика, либо снизить эту мощность за счет использования большего количества ветвей. Проведенные исследования [2, 3] показали. Что использование пространственного разнесенного приема дает выигрыш по помехоустойчивости почти в два раза, а с увеличением количества ветвей выигрыш имеется, но не такой значительный. В этом случае остается актуальным вопрос выбора необходимого количества ветвей разнесения, исходя из существующей обстановки (ограничений) по энергетическому, материальному и техническому обеспечению подразделений связи.

Выбор количества ветвей разнесения может определяться по различным критериям: минимальной стоимости, максимальной помехоустойчивости или помехозащищенности и т. д. В данной работе критерием выбора числа ветвей является минимум средней вероятности битовой ошибки: $\arg\min_{L} P_b(L, \gamma_{bc}^*)$, где вероятность ошибки в общем случае зависит от отношения сигнал/шум и от параметров, характеризующих замирания.

Существующие методики оценки помехоустойчивости систем с разнесенным приемом, представленные в [2, 3], не учитывают позиционность передаваемых многомерных сигналов и влияние помехи подобной, сигналу.

Для анализа помехоустойчивости сигнальных конструкций при разнесенном приеме воспользуемся следующими предположениями: в каждой ветви разнесения осуществляется однолучевой прием сигналов; число ветвей разнесения $L \geq 1$; величина γ_0 есть среднее отношение энергии сигнала к спектральной плотности шума (помехи), которое было бы, если бы тот же передатчик использовался для одиночного приема; для любой ветви разнесения помеха является аддитивным белым гауссовым шумом с односторонней спектральной плотностью мощности шума $N_0/2$ и коэффициентом передачи $\mu_l, l = \overline{1, L}$; сигналы во всех ветвях некоррелированны; в каждой ветви разнесения отношения сигнал/шум есть величина $\gamma_l = E_l / N_l$, $l = \overline{1, L}$; для разнесенного приема справедливо соотношение $\gamma_L^* = \gamma_0 / L^{\lambda}$, где γ_0 – среднее отношение сигнал/шум в одной отдельной ветви разнесения и $\lambda \in [0, 2]$ – коэффициент эффективности использования мощности передатчика при разнесенном приеме [3, 4].

Отношение сигнал/шум при оптимальном когерентном приеме и некоррелированной по отдельным ветвям помехи, равно сумме всех отношений каждой из ветвей [3, 4]:

$$\gamma_{\Sigma} = \sum_{l=1}^{L} \gamma_l = \gamma \sum_{l=1}^{L} \delta_l^2 = \gamma \Delta_L, \; 0 \leq \Delta_L \leq L,$$

где $\delta_l^2 = \frac{\gamma_l}{\gamma_1}$, $\gamma = \gamma_l$, тогда, предполагая упорядоченность по мощности, справедливо неравенство $\delta_1^2 \geq \delta_2^2 \geq ... \geq \delta_L^2$, $\delta_1^2 = 1$. Энергетический выигрыш при переходе от одиночного к разнесенному приему будет $\eta_\Sigma^2 = \frac{\gamma_\Sigma}{\gamma_0} = \frac{1}{L^\lambda}\sum_{l=1}^{L}\delta_l^2$.

Если в канале связи присутствуют замирания, то:

$$\gamma_{l,\mu} = \frac{\mu_l^2}{\overline{\mu_l^2}}\gamma_l,\ \overline{\mu_l^2} = m_{2,l} = \int_0^\infty \mu_l^2\,\omega(\mu_l)\,d\mu_l,\ l = \overline{1,L},$$

где $\omega(\mu_l)$ – плотность распределения вероятности коэффициента передачи μ_l для l-ой ветви.

В теории связи для описания замираний в канале связи наибольшее применение нашли плотности распределения вероятностей Релея, Райса и Накагами [3, 5, 6], поэтому для дальнейших исследований удобно рассмотреть обобщенное распределение Райса-Накагами $RN(p, \gamma, \beta)$ [4]:

$$\omega(\mu) = \frac{(\beta\mu)^p}{\gamma^{p-1}}\exp\left(-\frac{\gamma^2}{2\beta} - \frac{\beta}{2}\mu^2\right)I_{p-1}(\gamma\mu), \qquad (1)$$

включающее в себя, как частный случай плотности распределения Релея, Райса и Накагами. Введем понятие коэффициента глубины замираний для распределения Райса – Накагами $k^2 = \frac{\gamma^2}{2\beta}$. Плотность распределения Райса-Накагами определяется параметрами (p, γ, β, k^2):

– для распределения Релея – $p = 1$, $\gamma = 0$, $\beta = 1/\sigma^2$, $k^2 = 0$;

– для распределения Райса – $p = 1$, $\gamma = \mu_0/\sigma^2$, $\beta = 1/\sigma^2$, $k^2 = \frac{\mu_0^2}{2\sigma^2}$;

– для распределения Накагами $p = m$, $\gamma = 0$, $\beta = 2m/\overline{\mu^2} = 2m/\Omega$; $k^2 = 0$.

Полная вероятность ошибки в канале с разнесением и некоррелированными по ветвям замираниями (независимо от вида замираний) имеет вид [6]:

$$\overline{P}_{e|b} = \mathrm{E}P_{e|b} = \int_0^{+\infty}...\int_0^{+\infty} P_{e|b}\left(\gamma_{bc}\sum_{l=1}^{L}\delta_l^2\mu_l^2\Big/\overline{\mu_l^2}\right)\prod_{l=1}^{L}\omega(\mu_l)d\mu_1...d\mu_L, \qquad (2)$$

где $P_{e|b}$ – вероятность символьной (битовой) ошибки в канале с детерминированными параметрами и белым шумом; μ_l – коэффициент передачи в l ветви, $l = \overline{1,L}$.

Известно, что вероятность символьной (битовой) ошибки при когерентном приеме в канале с детерминированными параметрами и АБГШ может быть представлена в виде [6]:

$$P_{e|b}(\gamma_{bc}) = \sum_k a_k T\left(\alpha_k \sqrt{\gamma_{bc}}, \eta_k\right), \tag{3}$$

где $\alpha_k = 2g_k$.

Из (2) с учетом (3) следует, что для расчета полной вероятности ошибки в канале связи с разнесением необходимо вычислить интеграл:

$$J_L = \int_0^\infty \ldots \int_0^\infty T\left(\alpha\sqrt{\gamma_{bc}\sum_{l=1}^{L}\delta_l^2\frac{\mu_l^2}{\overline{\mu_l^2}}}, \eta\right)\prod_{l=1}^{L}\omega(\mu_l)d\mu_1 d\mu_2 \ldots d\mu_L =$$

$$= \frac{1}{2\pi}\int_0^\eta \frac{1}{1+x^2}\prod_{l=1}^{L}\left(\int_0^\infty e^{-\frac{\alpha^2\gamma_{bc}\delta_l^2\frac{\mu_l^2}{\overline{\mu_l^2}}(1+x^2)}{2}}\omega(\mu_l)d\mu_l\right)dx. \tag{4а}$$

Преобразовав формулу (4а) с учетом (1), получим выражение, по своей структуре похожее на *H*-функцию [6]:

$$J_L = H_p^{(L)}\left((z_l)_{l=1}^L, (b_l)_{l=1}^L, \eta\right) =$$

$$= \frac{1}{2\pi}\prod_{l=1}^{L}\left(1-b_l^2\right)^p \int_0^\eta \frac{1}{1+x^2}\frac{1}{\prod_{l=1}^{L}\left(1+b_l^2x^2\right)^p} e^{-\frac{1}{2}(1+x^2)\sum_{l=1}^{L}\frac{z_l^2}{1+b_l^2x^2}}\,dx, \tag{4б}$$

где $b_l^2 = \dfrac{\alpha^2\gamma_{bc}\delta_l^2}{\alpha^2\gamma_{bc}\delta_l^2 + \overline{\mu_l^2}\beta_l}$ и $z_l^2 = \dfrac{\gamma_l^2}{\beta_l}b_l^2$.

Если при разнесенном приеме каналы связи однородные, т. е. статические параметры одинаковы: $b_l^2 = b^2$, $z_l^2 = z^2$, $l = \overline{1,L}$, тогда:

$$H_p^{(L)}\left(z_{l=1}^L, b_{l=1}^L, \eta\right) = H_{pL}\left(z\sqrt{L}, b, \eta\right) \text{ и } H_p^{(1)}(z,b,\eta) = H_p(z,b,\eta),$$

где [6]:

$$H_\nu(z,b,\eta) = \frac{\left(1-b^2\right)^\nu}{2\pi}\int_0^\eta \frac{1}{1+x^2}\frac{1}{\left(1+b^2x^2\right)^\nu} e^{-\frac{z^2}{2}\frac{1+x^2}{1+b^2x^2}}dx,\ \nu \ge 0,\ 0 \le b^2 \le 1,\ \eta \ge 0. \tag{5}$$

При проведении численных расчетов (5) можно записать в виде:

$$H_\nu(z,b,\eta) = \frac{\left(1-b^2\right)^\nu}{2\pi}\int_0^{\operatorname{arctg}\eta} \frac{\cos^{2p}t}{\left(1-\left(1-b^2\right)\sin^2 t\right)^\nu} e^{-\frac{z^2}{2}\frac{1}{1-(1-b^2)\sin^2 t}}dt.$$

Полученные соотношения могут быть использованы для произвольных многомерных многопозиционных сигнальных конструкций, однако в дальнейшем ограничимся численными расчетами вероятности ошибки при передаче двумерных многопозиционных сигналов ФМ-*M* (фазовая модуляция) и КАМ-*M* (квадратурная амплитудная модуляция), широко применяемых в современных телекоммуникационных стандартах. Для других сигнальных конструкций расчеты могут быть проведены по формулам вероятностей ошибок [6].

Использованием пространственного разнесенного приема и поляризационного разнесенного приема всегда дает выигрыш по помехоустойчивости. При использовании временного (частотного, когда информация на каждой частоте излучается своим передатчиком) разнесенного приема с увеличением количества ветвей разнесения для фиксированной мощности сигнала величина вероятности ошибки стремится к значению вероятности ошибки в канале с аддитивным белым гауссовским шумом. При частотном разнесенном приеме, реализованном на одном передатчике, с увеличение количества ветвей разнесения значение вероятности ошибки в канале связи уменьшается до определенного минимального значения. При дальнейшем увеличении количества ветвей разнесения качество связи ухудшается. Поэтому в зависимости от вида разнесенного приема можно выбрать оптимальное (при частотном, реализованном на одном передатчике) или рациональное (временное) количество ветвей разнесения по критерию минимума вероятности ошибки.

При пространственном разнесенном приеме выбор количества ветвей может производиться в зависимости от тех требований, которые предъявляются к системе связи.

Список используемых источников

1. Игнатов В. В., Сахнин А. А. Развед- и помехозащищённость систем и средств военной связи. СПб. : ВУС, 2001. 212 с.

2. Андронов И. С., Финк Л. М. Передача дискретных сообщений по параллельным каналам. М. : Сов. радио, 1971. 408 с.

3. Кловский Д. Д. Передача дискретных сообщений по радиоканалам. М. : Радио и связь, 1982. 362 с.

4. Бураченко Д. Л., Савищенко Н. В. Геометрические модели сигнально-кодовых конструкций. СПб. : Военная академия связи, 2012. 388 с.

5. Simon K., Alouini M.-S. Digital Communication over Fading Channels: A Unified Approach to Performance Analysis. N. Y. : John Wiley&Sons, 2000. 544 p.

6. Савищенко Н. В. Специальные интегральные функции, применяемые в теории связи: монография. СПб. : Военная академия связи, 2012. 560 с.

УДК 004.738

ОБЗОР ТЕНДЕНЦИЙ РАЗВИТИЯ НАНОСЕТЕВЫХ ТЕХНОЛОГИЙ В МЕДИЦИНЕ

Р. Я. Пирмагомедов, И. В. Худоев

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

В статье рассматривается влияние телекоммуникационных технологий на систему здравоохранения. Особое внимание уделяется вопросам применения наносетей в медицине. Проанализированы возможные методы развертывания наносетей в различных контекстах окружающей среды, рассматриваются архитектуры наносетей для медицинских приложений. Выявляются проблемы стоящие на пути развития Интернета Нано-Вещей, как со стороны технологий, которые еще предстоит реализовать в будущем, так и со стороны современного интернета и телекоммуникационного оборудования.

Интернет Нано-Вещей, медицина, наносети.

Сегодня на систему здравоохранения оказывает влияние бурное развитие телекоммуникационных технологий, которые позволяют предоставлять услуги диагностики и мониторинга вне помещений медицинских учреждений. Концепция Интернета Вещей внедряемая в том числе и в сфере здравоохранения [1], расширяет возможности врачей по сбору и анализу данных о состоянии пациента [2]. Дальнейшее развитие медицинской составляющей в сфере телекоммуникаций связанно с Интернетом Нано-Вещей, с набором новых, сложно структурированных приложений, которые могут быть развернуты внутри человеческого тела [3]. В данной статье мы рассмотрим несколько наиболее интересных направлений развития наносетевых технологий в здравоохранение.

По состоянию на сегодняшний день, нательные сети (*body area networks*) могут режиме реального времени, осуществлять мониторинг состояния здоровья пациентов, для которых это жизненно важно [4]. Мобильные системы здравоохранения удобны для ношения и могут поддерживать предоставление медицинских услуг как через смартфоны, так и через другие мобильные устройства [5]. Датчики, расположенные в окружающей среде, оповещают о факторах, несущих вред здоровью.

Архитектура медицинских наносетевых приложений

Наносетевые технологии позволяют вывести здоровье и медицинские услуги на новый уровень. Дизайн этих сетей будет зависеть от примитивов, которые будут развернуты в различных контекстах: в окружающей человека среде, на и внутри тела человека. Такими примитивами являются сетевые

наноструктуры. Они расширят медицинские приложения за пределы только мониторинга состояния пациента [6].

Основной структурной единицей наносетевых технологий, являются наномашины или наноустройства, которые имеют микроскопические размеры. Наномашины могут проводить измерения и выполнять примитивные действия. Другие наноустройства, называемые наномаршрутизаторы, выступают в качестве промежуточных узлов, которые будут пересылать данные от одних наномашин к другим, а также из наносетей на микроустройства, смартфоны, или точки доступа. Сетевые наноструктуры могут быть комплексно развернуты внутри человеческого тела, для решения специализированных задач. Предполагается два основных способа обмена информацией между устройствами: молекулярный и электромагнитный. Архитектура наносетевых структур, интегрированных с интернетом, состоит из трех уровней (рис.) Первый уровень данной архитектуры состоит непосредственно из наносетей развернутых в различных контекстах, такие сети смогут создать, вокруг человека, единую экосистему. Следующем уровнем являются специальные шлюзы, которые обеспечат агрегирование и слияние данных для передачи их на удаленные сервера [2]. Удаленные сервера предназначенные для сложных вычислений, прогнозирования событий и распределения операций между наносетями, станут третьим уровнем таких систем [2, 7].

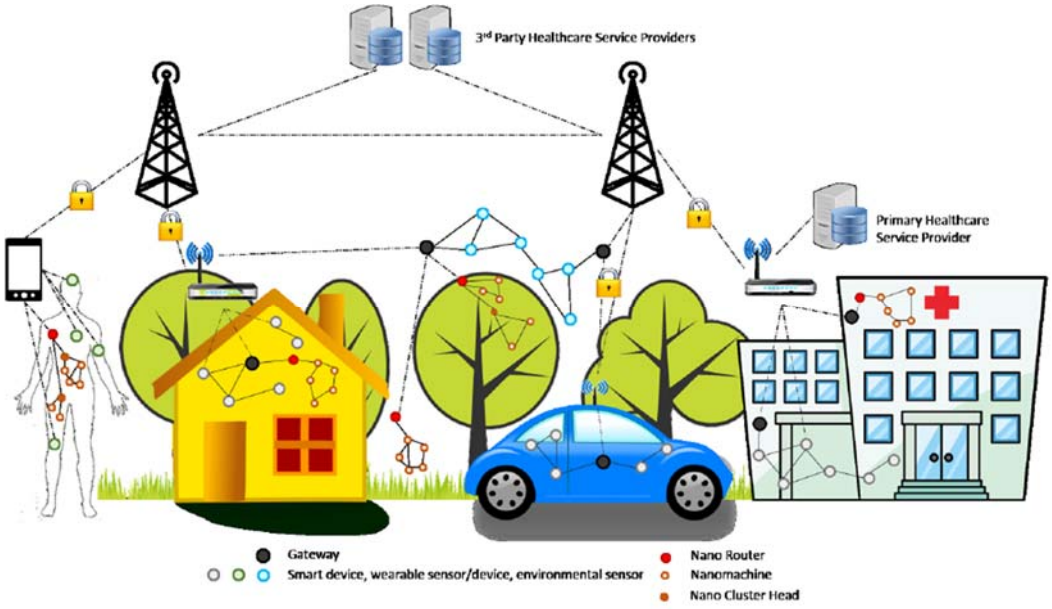


Рисунок. Архитектура наносети связанной с интернетом (*"Internet of Nano-Things Healthcare Applications: Requirements, Opportunities, and Challenges" Wireless and Mobile Computing, Networking and Communications* (WiMob), 2015 IEEE 11th International Conference, p. 11)

Рассмотрим три основных контекста, в которых будут разворачиваться наносети:

– в окружающей человека среде;
– на поверхности тела человека;
– внутри тела человека.

Дома, в машине, в больницах и других учреждениях предполагается развернуть наноструктуры, которые будут осуществлять контроль над окружающей средой и проводить ряд изменений. Для данных наноструктур предполагается использовать алгоритм отрицательного отбора искусственной иммунной системы – алгоритм, использующийся для классификации и распознавания проблемных областей, где модель строится на основе имеющихся знаний, а уже после происходит сравнение образцов с моделью. Наноструктуры, использующие такой алгоритм, могут быть использованы для очистки воздуха или воды, выступать в роли индикатора разлива нефти на водных объектах, являться индикатором наличия биологического или химического оружия [8].

Два других контекста, ориентированы на сбор информации о состоянии здоровья человека, что необходимо для медицинских приложений, рассмотрим их более подробно.

Наносетевые технологии в медицине

Сетевые наноструктуры могут быть развернуты на теле пациента или его одежде. Ряд предложенных систем уже позволяют развернуть наносенсоры на одежде [9, 10] или в мобильном телефоне [11]. Передовые проекты по развитию наносенсоров на текстильной основе (электрические / оптические волокна) включает датчики, передатчики сигнала и другие активные нанокомпоненты. Проекты призваны решить две основные задачи:

1) Создание новых сенсорных и функциональных волокон (волокна способные заменять существующие природные волокна и выполнять их функции), что позволит производить наблюдения за функциями организма, такие как электрокардиограмма мониторинг и биологическое виды в тела близости.

2) Создание прототипов и организацию производства таких тканей, предназначенных для здравоохранения, реабилитации и профилактики. Примером, демонстрирующим положительные стороны данных проектов, является электронное белье для людей с параличом нижних конечностей, которые страдают от пролежней.

Наиболее интригующим направлением развития наносетей представляют собой, структуры, которые можно развернуть непосредственно в теле человека. На сегодня примером такой системы является лекарство против рака – Bacteriobot, созданное командой Chonnam, Национального Университета Южной Кореи [12, 13]. Bacteriobot представляет из себя генетически модифицированную бактерию сальмонеллы, которая тянется к опухолям, используя вещества, выделяемые раковыми клетками. В бактерии находятся

микроскопические роботы, размером около 3 микрометров, которые автоматически выпускают капсулы, наполненные лекарствами, как только бактерия достигает опухоли. Такое лекарство более эффективно и наносит меньше вреда организму, чем традиционные методы лечения, например, химиотерапия.

Заключение

Бурное развитие наносетевых технологий является логическим продолжением развития Интернета Вещей, одним из ключевых критериев перехода Интернета Вещей (*Internet of Things*) в Интернет Всего (*Internet of Everythings*). Разработки наносетевых приложений в сфере здравоохранения, направлены на повышение доступности и качества медицинских услуг для граждан. С помощью нано структур можно будет диагностировать ранние стадии заболевания, производить поиск патогенных факторов, производить лечение. Огромный объем данных, который будет генерироваться наносетями безусловно окажет влияние на структуру и организацию интернет, предвосхищая изменения в области телекоммуникационной инфраструктуры, в связи с изменением структуры и объема трафика. Для широкого внедрения наносетевых приложений, нужно решить ряд ключевых вопросов, таких как: создание шлюза между нано структурами и интернетом, снабжение устройств энергией, создание устойчивого канала связи между нано структурами, разработка протоколов обмена данными между нано структурами и др. Однако уже сегодня, отдельные примеры наносетевых приложений реализованы и нашли применение.

Список используемых источников

1. Кучерявый А. Е., Прокопьев А. В., Кучерявый Е. А. Самоорганизующиеся сети. СПб. : Любавич, 2011. 311 с.

2. Пирмагомедов Р. Я., Глушаков Р. И., Киричёк Р. В., Кучерявый А. Е. Живые организмы в киберпространстве – проект Биодрайвер // Электросвязь. 2016. № 1. С. 47–52.

3. Пирмагомедов Р.Я. Киричёк Р. В., Кучерявый А. Е. Бактериальные наносети // Информационные технологии и телекоммуникации. 2015. № 2 (10). С. 5–10.

4. Seyedi M., Kibret B., Lai D. and Faulkner M. A Survey on Intrabody Communications for Body Area Network Applications / IEEE Transactions on Biomedical Engineering, 2013. Vol. 60, no. 8. PP. 2067–2079.

5. Kumar S., Nilsen W., Abernethy A., Atienza A., Patrick K., Pavel M., Riley W., Shar A., Spring B., Spruijt-Metz D., Hedeker D., Honavar V., Kravitz R., Lefebvre R., Mohr D., Murphy S., Quinn C., Shusterman V. and Swendem D. Mobile Health Technology Evaluation: The mHealth Evidence Workshop // American Journal of Preventive Medicine. 2013. Vol. 45, no. 2. PP. 228–236.

6. Atakan B., Akan O. and Balasubramaniam S. Body Area NanoNetworks with Molecular Communications in Nanomedicine // IEEE Communications Magazine. 2012. Vol. 50, no. 1. PP. 28–34.

7. Najah Abu Ali, Mervat Abu-Elkheir. Internet of Nano-Things Healthcare Applications: Requirements, Opportunities, and Challenges // Wireless and Mobile Computing, Networking and Communications (WiMob), 2015 IEEE 11th International Conference, 2015. PP. 9–14.

8. Prachi Raut, Nisha Sarwade. Designing and Performance Analysis of Nano Machines Network for Synthetic Immune System // Circuits, Systems, Communication and Information Technology Applications (CSCITA), 2014 International Conference on. PP. 144–149.

9. URL: http://sensing.xprize.org/

10. Shyamkumar P., Rai P., Oh S., Ramasamy M., Harbaugh R. and Varadan V. Wearable Wireless Cardiovascular Monitoring Using Textile-Based Nanosensor and Nanomaterial Systems // Electronics. 2014. Vol. 3, no. 3. PP. 504–520.

11. Ramasamy M., Oh S. and Varadan V. Wireless sleep monitoring headband to identify sleep and track fatigue / Proc. SPIE 9060, Nanosensors, Biosensors, and Info-Tech Sensors and Systems, 2014. Vol. 9060.

12. Gopinath S., Tang T.-H., Yeng Chen Y., Citartan M. and Lakshmipriya T. Bacterial detection: From microscope to smartphone // Biosensors and Bioelectronics. 2014. Vol. 60. PP. 332–342.

13. Sunghoon Cho, Sung Jun Park, Young Jin Choi, Han-earl Jung, Shaohui Zheng, Seong Young Ko, Jong-Oh Park* and Sukho Park. Biomedical Robotics and Biomechatronics / 5th IEEE RAS & EMBS International Conference, 2014. PP. 856–860.

УДК 004.67

СОНИФИКАЦИЯ РЕЗУЛЬТАТОВ ИНФОРМАЦИОННОГО АНАЛИЗА САЙТОВ

Д. А. Подольский, Г. Г. Рогозинский

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

В статье анализируются результаты информационного анализа (парсинга) четырёх популярных сайтов с целью их представления в виде акустических сигналов (сонификации). Сонификация расширяет возможности анализа сложной информации за счет использования слухового анализатора, что позволяет снизить нагрузку на оператора и быстрее обнаруживать характерные особенности в потоке данных.

Полученные на протяжении недели данные были преобразованы к виду, удобному для сонификации. Мощный аппарат языка музыкального программирования Csound позволил представить полученные данные в виде соответствующих тембральных классов.

сонификация данных, парсинг, Csound.

С увеличением объёма информации, которую получает человек в современном информационном обществе, всё более остро встаёт вопрос поиска алгоритмов и инструментов для оперативного анализа принятых данных: котировки акций и ценных бумаг, сводки прогноза погоды или цены

на продукты в ближайшем супермаркете. Учитывая преимущества слухового восприятия во временной, пространственной и частотных областях, становится возможным использование неречевого аудио для передачи информации, т.е. сонификации (англ. *Sonification*).

Как утверждал в 1998 г. Эдворти (*Edworthy*), появление *слуховых дисплеев* и аудио интерфейсов было неизбежно, учитывая простоту и экономическую выгоду, с которыми в настоящее время электронные устройства могут воспроизводить звук [1]. Сонификация, как часть информационной системы, обеспечивает связь между источником и адресатом сообщения.

За счет использования слухового анализатора сонификация расширяет возможности обработки больших массивов данных. Это позволяет уменьшить время на поиски закономерностей и выявление характерных особенностей в потоке информации.

Научно-технический прогресс имеет тенденцию затрагивать все области человеческой деятельности: на сегодняшний день, для того чтобы играть на рынке ценных бумаг или узнать температуру воздуха, скорость ветра и температуру воды, достаточно иметь любое устройство с доступом в Интернет. Однако, объём данных, который необходимо с высокой степенью точности анализировать человеку, значительно увеличивается с поступлением новой информации. Современные возможности в области звукового дизайна и вычислительной техники позволяют сонифицировать практически любой информационный поток, однако предметом исследования автора доклада стали данные, полученные в результате синтаксического разбора (парсинга) четырех веб-сайтов: популярный сервис «Яндекс.Погода» (https://pogoda.yandex.ru/), удобная платформа для отображения актуальной информации о курсах валют и стоимости нефти за баррель «Сберометр» (http://www.sberometer.ru/), сайт новостей фондового рынка и данных с ценами на акции ПАО «Газпром»«БКС экспресс» (http://bcs-express.ru/).

Обслуживание большого потока меняющихся данных не в силах обеспечить даже слаженная работа операторов, а информация на выбранных ресурсах меняется динамично. Поэтому не целесообразно использовать ручной режим обновления данных. Парсинг сайтов - это эффективное решение для автоматизации сбора и изменения информации. Используя стандартные средстваобъектно-ориентированногои интерпретируемого языка скриптов Python, была решена задача получения доступа из программы к объектам веб-ресурсов.

Многие алгоритмы в Python сводятся к обработке массивов данных и получению новых массивов данных в результате. Среди встроенных функций Python есть несколько для работы с последовательностями. Под последовательностью в Python понимается любой тип данных, который поддерживает интерфейс последовательности [2].

Для анализа файлов HTML/XML был выбран парсер Beautiful Soup [3], который способен преобразовать различные варианты разметки в дерево

синтаксического разбора. Парсер поддерживает простые и естественные способы навигации и поиска в HTML/XML коде веб-страницы, что существенно облегчает задачу сохранения данных с сайта необходимой платформы.

В период с 18.04.16 по 24.04.16 Python-скрипт парсил выбранные для исследования веб-сайты с интервалом обращения каждый час. В качестве источника информации на разных платформах были выбраны данные: температура воздуха, скорость ветра и температура воды (сервис «Яндекс.Погода»); стоимостьбаррели нефти, курс доллара и евро (платформы «Сберометр»); цена акции ПАО «Газпром» и стоимость акций в разделе «Котировки» (сайт новостей фондового рынка «БКС экспресс»).

Полученные данные записывались в текстовый документ, затем средствами прикладных пакетов проводилась обработка собранной информации. В данной статье автор ограничивается рассмотрением сонификации информации о скорости ветра, график которой представлен на рисунке 1.

Рис. 1. Изменение скорости ветра в Санкт-Петербурге с 18.04.16 по 24.04.16.

Изменение скорости ветра наблюдается относительно средней величины 4 м/с, при этом характер отклонения величины не зависит от времени суток. Очевидно, что чем больше полученное значение, тем сильнее порывы ветра, а нахождение на улице для человека становится некомфортным или опасным. Полученную информацию сонифицировать напрямую не представляется возможным: по оси абсцисс значения времени, которые будут увеличиваться с ростом частоты обращения парсера к веб-ресурсу, по оси ординат большая амплитуда флуктуации.

Для сонификации данных использовался мощный аппарат языка музыкального программирования Csound, в библиотеке которого имеются опкоды, позволяющие создать практически любой звуковой алгоритм. Структурная схема синтезатора «скорости ветра» представлена на рисунке 2.

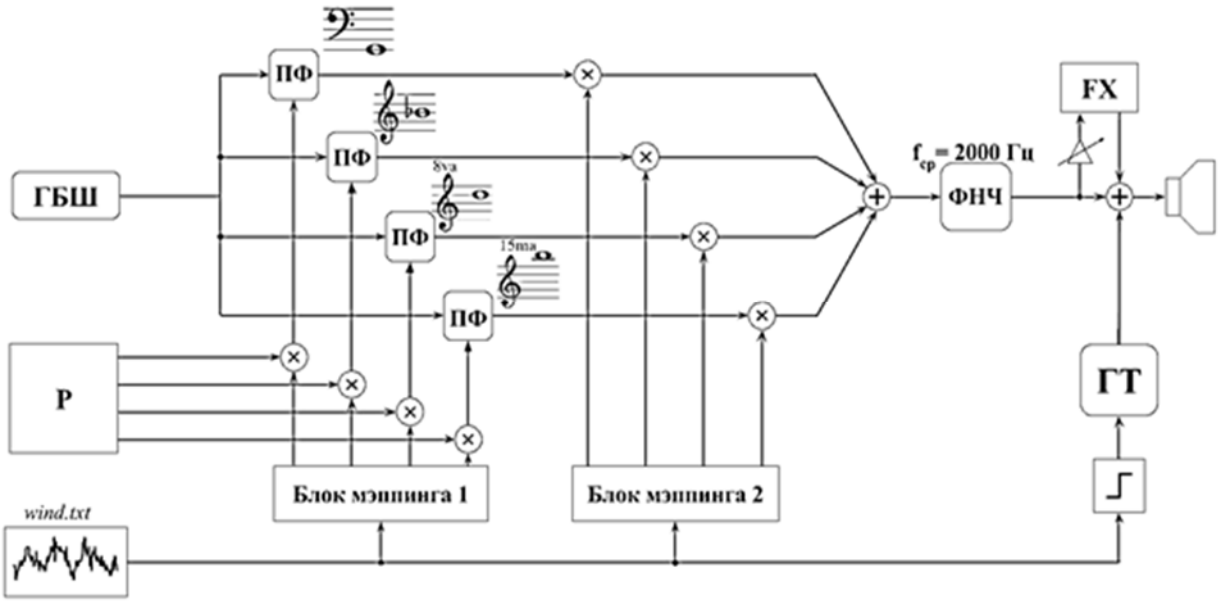


Рис. 2. Структурная схема «синтезатора ветра»

В качестве источника сигнала используется генератор белого шума ГБШ. Сигнал с блока ГБШ $X_ш(n)$ поступает на четыре полосовых фильтра ПФ, центральная частота и ширина полосы пропускания которых зависят от значения первой мэппинг-функции. Для создания более естественного звучания на выходе ПФ был введён блок рандомизации Р параметров фильтров. Данный блок реализован с помощью опкода jspline [4], который вносит расстройку центральной частоты среза полосовых фильтров в заданном диапазоне частот относительно нот, указанных на структурной схеме. Необходимо так же, чтобы поступающие значения о ветре влияли и на огибающую синтезируемого звука. Для обеспечения влияния поступающих параметров на динамические нюансы выходного звука, был введён второй блок мэппинга. Таким образом, сигнал на выходе каждого полосового фильтра описывается формулой (1).

$$S_i(n) = K_i(n) \times M_1(i) = f[X_{\text{ш}}(n), W_i(M_2)] \times M_1(i), \qquad (1)$$

где $X_{\text{ш}}(n)$ – сигнал на выходе ГБШ, $W_i(M_2)$ – значения второй мэппинг-функции, $M_1(i)$ – значение первой мэппинг-функции.

Для возможности ориентации в информационном потоке введён блок генератора тона ГТ, который срабатывает по сигналу компаратора. Компаратор сравнивает поступающее значение со значением 3,4 м/с. Именно такая скорость ветра соответствует границе между легким и слабым ветром по шкале Бофорта [5]. В зависимости от того, с области каких значений (бóльших или меньших) относительно выбранного порога поступающие данные пересекают 3,4 м/с, ГТ синтезирует две разные частоты $S_{\text{ГТ}}(n)$, в общем случае описываемые выражением (2). Сигнал на выходе сумматора

имеет вид (3). Для создания объёмного и естественного звучания используется блок реверберации *FX*.

$$S_{\text{ГТ}}(n) = \sin\left(500{,}1000, R(n)\right) \quad (2)$$

$$Y(n) = \sum_{i=1}^{4} S_i(n) + S_{\text{ГТ}}(n) \quad (3)$$

Результатом сонификации данных скорости ветра стал аудиофайл длительностью 100 секунд, который даёт представление о силе ветра в течение недели. С помощью введённых тональных меток, слушатель легко ориентируется в анализируемой информации. Это позволяет быстрее обрабатывать поступающий массив данных и выявлять характерные особенности в потоке цифр.

Список используемых источников

1. Thomas Hermann, Andy Hunt, John G. Neuhoff (Eds.). The Sonification Handbook. Logos Verlag, Berlin, Germany, 2011. 566 p.

2. Сузи Р. А. Язык программирования Python. М. : Национальный открытый Университет «ИНТУИТ», 2016. 350 с.

3. Beautiful Soup Documentation. URL: https://www.crummy.com/software/BeautifulSoup/bs4/doc/ (дота обращения 14.04.2016).

4. Ed. by Richard Boulanger. The Csound Book. MIT Press, 2000. 782 p.

5. Шкала Бофорта // Портал Гидрометцентра России. URL: http://meteoinfo.ru/bofort (дата обращения 19.04.2016).

УДК 535.317

РАСЧЕТ ОПТИЧЕСКОЙ СИСТЕМЫ МЕТОДОМ МАТРИЧНОЙ ОПТИКИ

Е. В. Полякова

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

Решение задачи о прохождении света через идеальную центрированную оптическую систему возможно различными способами. Наряду с традиционным расчетом существует матричный метод, позволяющий установить соотношения между входными и выходными параметрами системы. Методы матричной оптики актуальны при расчете оптических систем, построенных на основе использования оптического микрокомпонента.

волоконный микрокомпонент, линзовый микрокомпонент, специализированные волокна, матрица передачи.

Волоконные микрокомпоненты успешно применяются уже много лет. Микрокомпоненты различных форм и размеров позволяют изменять форму диаграммы излучения на входе или выходе оптического волокна. Чаще всего концы волокна требуемой формы получают путем обработки оптического материала исходного волокна. Процесс обработки может быть, как механическим, так и термическим, в последнем случае чаще всего применяется лазерная обработка. Поскольку профилированные концы формируются непосредственно из материала самого волокна, стык между волокном и профилированным концом отсутствует. Следовательно, не возникает переходного затухания между микрокомпонентом и волокном. Это снижает оптические потери и существенно повышает механическую прочность и долговечность устройства. Среди большого разнообразия существующих волоконных микрокомпонентов можно выделить основную категорию – линзы. Волоконные микрокомпоненты могут изготавливаться в виде вогнутых, выпуклых и сферических линз [1].

Расчет линзового микрокомпонента возможен с применением уравнения стандартной тонкой линзы (рис. 1). В случае формирования сферической линзы на конце волокна необходимо определить радиус линзы:

$$\frac{1}{a}+\frac{1}{a'}=(n_2-n_1)\left(\frac{1}{R_1}-\frac{1}{R_2}\right), \quad (1)$$

где a, a' – сопряженные расстояния, R_1, R_2 – радиусы поверхностей линзы, n_1, n_2 – показатели преломления сред.

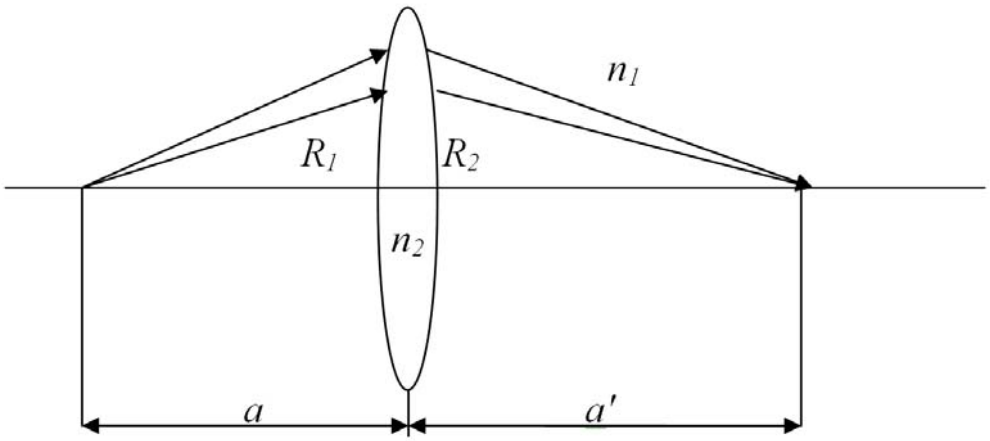


Рис. 1. Иллюстрация к уравнению тонкой линзы

В случае, когда необходимо собрать коллимированный свет от источника и ввести его в оптическое волокно (рис. 2), линза должна иметь плоско-выпуклую структуру. В этой ситуации параметры a и R_2 равны бесконечности и при предположении $n_1 = 1$ (воздух), уравнение тонкой линзы упрощается к виду:

$$\frac{1}{a'}=\frac{n_2-1}{R_1}. \quad (2)$$

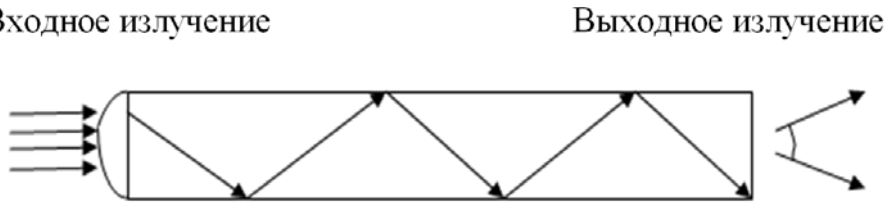


Рис. 2. Волоконный микрокомпонент в виде положительной выпуклой линзы с $NA_{вх} < NA_{вых}$

Поскольку числовая апертура волокна $NA_{вых}$ и показатель преломления сердцевины n_2 известны, то расстояние a' может быть получено из определения числовой апертуры:

$$a' = \frac{h}{NA_{вых}}, \quad (3)$$

где h – радиус входного пучка.

Подставляя a' (3) и n_2 в упрощенное уравнение тонкой линзы (2), можно рассчитать радиус сферической поверхности линзы R_1.

В настоящее время разработаны специализированные оптические волокна для различных биомедицинских приложений. Интерес представляет кварцевое волокно с низким уровнем OH, диаметром сердцевины порядка 200 мкм с линзовым плоско-выпуклым микрокомпонентом для фокусировки излучения гольмиевого (Ho:YAG) лазера в оптический волновод.

При условии, что волоконный световод выполнен из кварцевого стекла с показателем преломления равным 1,51, радиус поверхности линзового микрокомпонента составляет 2,5 см, предмет высотой 5 см расположен в воздухе на оси на расстоянии 10 см от крайней точки этой поверхности (рис. 3) можно определить размер изображения и его положение.

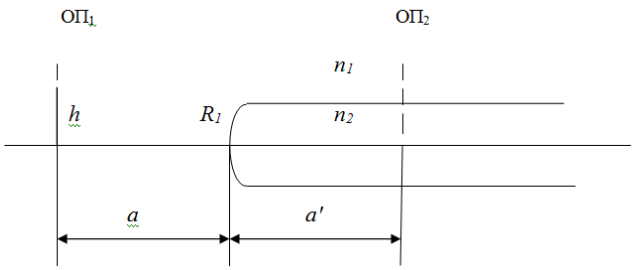


Рис. 3. Расположение предмета и параметры конструкции

Матрица передачи оптического луча (M), состоит из матриц передачи (T) и матрицы преломления (R) для данной конструкции [2]. R – матрица преломления оптической поверхности имеет вид:

$$R = \begin{bmatrix} 1 & 0 \\ -\frac{n_2 - n_1}{R_1} & 1 \end{bmatrix}. \quad (4)$$

Пространство от предмета до преломляющей поверхности определяется матрицей передачи T_1:

$$T_1 = \begin{bmatrix} 1 & \frac{a}{n_1} \\ 0 & 1 \end{bmatrix}. \quad (5)$$

Если изображение находится на расстоянии a' справа от вершины преломляющей поверхности, то T_2 – матрица передачи, определяющая пространство от преломляющей поверхности до изображения, имеет вид:

$$T_2 = \begin{bmatrix} 1 & \frac{a'}{n_2} \\ 0 & 1 \end{bmatrix}. \quad (6)$$

Матрица передачи оптического луча M представляет собой результат перемножения матриц передачи (5, 6) и матрицы преломления (4) в направлении от изображения к предмету:

$$M = \begin{bmatrix} 1 & \frac{a'}{n_2} \\ 0 & 1 \end{bmatrix} \begin{bmatrix} 1 & 0 \\ -\frac{n_2 - n_1}{R_1} & 1 \end{bmatrix} \begin{bmatrix} 1 & \frac{a}{n_1} \\ 0 & 1 \end{bmatrix} =$$

$$= \begin{bmatrix} 1 & \frac{a'}{1{,}51} \\ 0 & 1 \end{bmatrix} \begin{bmatrix} 1 & 0 \\ -0{,}204 & 1 \end{bmatrix} \begin{bmatrix} 1 & 10 \\ 0 & 1 \end{bmatrix} =$$

$$= \begin{bmatrix} 1 - 0{,}135a' & 10 - 0{,}688a' \\ -0{,}204 & -1{,}04 \end{bmatrix}.$$

Чтобы выполнялось соотношение, связывающее предмет с его изображением, верхний правый элемент B лучевой матрицы должен быть равен нулю [2]:

$$10 - 0{,}688a' = 0,$$

$$a' = 14{,}53 \text{ см}.$$

Таким образом, изображение находится внутри стержня на расстоянии 14,53 см от вершины сферической поверхности. Поперечное увеличение задается либо элементом матрицы A, либо величиной обратной элементу матрицы D и равно –0,96. Следовательно, изображение обратное и равно 4,8 см.

Аналогично рассчитываются оптические системы с вогнутыми или сферическими микрокомпонентами.

Список используемых источников

1. Мендез А., Морзе. Т. Ф. Справочник по специализированным оптическим волокнам : пер. с англ. М. : Техносфера, 2012. 727 с. ISBN 978-5-94836-320-2.

2. Джеррард А., Бёрч Дж. М. Введение в матричную оптику : пер. с англ. М. : Мир, 1978. 341 с.

УДК 004.896+75

ПРИМЕНЕНИЕ МЕТОДОВ СОНИФИКАЦИИ ПОТОКОВ ДАННЫХ И СЕНСОРНЫХ СЕТЕЙ В СИСТЕМЕ РАСПРЕДЕЛЕННОЙ ГЕНЕРАЦИИ ЗВУКОВЫХ ОБРАЗОВ

Г. Г. Рогозинский[1], А. В. Щекочихин[2]

[1]Санкт-Петербургский государственный университет телекоммуникаций им. проф. М. А. Бонч-Бруевича
[2]Санкт-Петербургский государственный институт кино и телевидения

Исследования авторов посвящены автоматизации процесса генерации звуковых образов. В качестве среды работы системы автоматической генерации предлагается использовать компьютерную сеть, а в качестве алгоритма музыкальной композиции – генетический алгоритм. Данная работа посвящена обзору методов сонификации и их применения к данным в сеносорных сетях.

алгоритмическая композиция, сонификация данных, сенсорные сети.

На данный момент работы над проектом уже создана модель системы распределённой генерации аудио контента при помощи генетического алгоритма. Модель системы была реализована в среде MAX/MSP и представлена в [1]. С подробными рассуждениями о структуре построения таких систем и процессов построения баз знаний в них можно ознакомиться в [2]. В [3] рассмотрены возможности применения генетических алгоритмов в качестве основы композиционной модели системы, авторами определён критерий корректности работы генетического алгоритма в такой системе. В [4] и [5] предложено применение технологий Интернета вещей в рамках работы системы. Рассматриваемая система обладает фундаментальным характеристикам Интернета вещей, представленными в [6]. Кроме того, в [5] авторами разработан механизм кластеризации сети, для работы с данными структурного аудио в системе дополненной акустической реальности.

Однако, возникает задача, близкая всем системам автоматической генерации звуковых образов – проблема взаимодействия среды и агентов системы. В случае композиции музыки или звуковых образов человеком он интерпретирует окружающую среду, эмоциональное состояние или техническое задание в виде слуховых образов. Законы интерпретации задаются жанром или техническим заданием предполагаемого контента.

В случае автоматической композиции предлагается рассматривать процесс композиции как задачу управления звуковым синтезатором. В зависимости от желаемых характеристик звукового образа управляющим функциям присваивается набор атрибутов и делается логический вывод о возможности использования данных из сети в качестве этих управляющих

функций. В качестве атрибутов могут быть использованы частотные характеристики, динамический диапазон или другие характеристики звуковых образов. Выбор атрибутов является отдельной темой исследования.

Авторами предлагается использовать данные сенсорных сетей для управления процессом генерации звуковых образов. С одной стороны, такой подход может предоставить необходимую разнообразную популяцию потенциальных решений для корректной работы генетического алгоритма (согласно условию корректности, определенному в [3]).

С другой стороны, сенсорные сети можно рассматривать как аналог системы органов чувств композитора, воздействие на которую влияет на процесс композиции. Кроме того, разрабатываемую авторами систему можно использовать для сонификации данных сенсорной сети.

Сонификация – процесс представления данных в виде звуковых образов, с целью улучшения процесса их восприятия. Сонификация – это акустический аналог визуализации. Несмотря на то, что визуализация данных приобрела большую популярность, сонификация также является функциональным инструментом представления информации [14].

С целью поиска методов сонификации сенсорной сети был произведен анализ существующих подходов к сонификации данных и их применения, представленных в [7, 8, 9, 10, 11, 12, 13]. На основе анализа выделены следующие техники сонификации.

Самой ранней техникой сонификации является аудификация. В ней любой одномерный сигнал интерпретируется как временная зависимость амплитуды аудио сигнала. Примером может служить подача на динамик напрямую данных наблюдения за любой физической величиной. Основным минусом данного способа является непредсказуемый характер звукового образа, а, следовательно, его сложная интерпретация. Однако данный способ нашел свое применение, в частности, в авангардном искусстве еще в начале XX века.

Другой техникой сонификации является сопоставление событиям в реальном или виртуальном мире специфических звуковых образов. Данный способ активно применяется для удобства работы в проводниках операционных систем. Определенные звуковые фрагменты соответствуют открытию папок и удалению документов. Не смотря на простоту, данный способ существенно изменяет восприятие взаимодействия пользователя и операционной системы.

Возможно применение и динамических звуковых ярлыков, например, для модельной задачи балансировки виртуального шара на подвижной плоскости. Генерация в реальном времени звука соответствующего движению шара позволяет испытуемому сбалансировать его быстрее, нежели если бы он только применял визуальный контроль. Развитие такой техники можно применять в хирургических операциях или задачах навигации для достижения наилучшего контроля [14].

Наиболее функциональной является техника мэппинга параметров потока данных к параметрам генерируемого аудио потока. В таком случае создается модель сопоставления параметров потока данных, которые необходимо наблюдать, наиболее характерным и заметным изменениям звукового образа.

Данная техника уже нашла модельное применение для мониторинга трафика в компьютерной сети [11]. В данной программе в качестве управляющих параметров выбраны количества отправленных и полученных битов и пакетов за 1 секунду. Каждый параметр управляет громкостью соответствующей звукового лупа и характеристикой частотного фильтра. При резком скачке одного из управляющих параметров соответствующий звуковой луп становится громче и ярче (рис. 1).

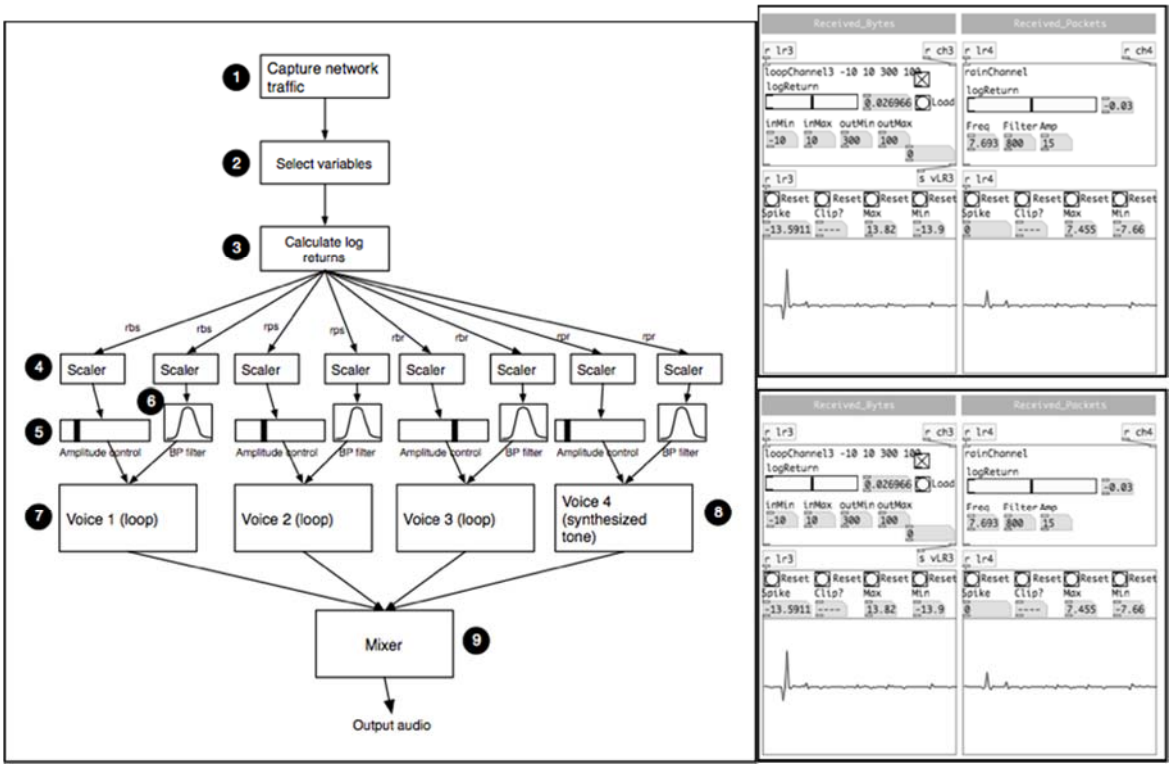


Рис. 1. Графический код программы для сонификации данных в сети, с целью мониторинга трафика и обнаружения DDoS атак [11]

Авторы предлагают использовать технику мэппинга данных для сонификации сенсорной сети. В качестве датчиков предлагается использовать датчики освещенности и температуры (рис. 2). Сценарий использования системы в данной ситуации следующий:

– ставится задача по мониторингу освещенности и температуры в двухмерном пространстве, в котором развернута сенсорная сеть, с известными пространственными координатами (горизонтальной и глубинной) Оператором формализуется задача мониторинга: задаются целевые критические значения освещенности и температуры;

– алгоритм поиска отбирает из сенсорной сети узел, показания которого наиболее близки к целевым, и отправляет их на сервер сонификации;

– в качестве сонификатора используется синтезатор гармонических последовательностей (монофонический синтезатор с арпеджиатором), в котором температура управляет скоростью смены нот в гармонической последовательности (низкая температура – медленно, высокая температура – быстро), а освещенность гармонией (наименьшая освещенность соответствует минорной гармонии, наибольшая – мажорной, между – цепочка гармонических аккордов);

– горизонтальная координата расположения сенсора в реальном пространстве мониторинга управляет расположением звукового образа в стереопанораме;

– глубинная локализация датчика в пространстве управляет уровняем реверберации звукового образа, располагая его соответственно дальше или ближе в звуковом фрагменте.

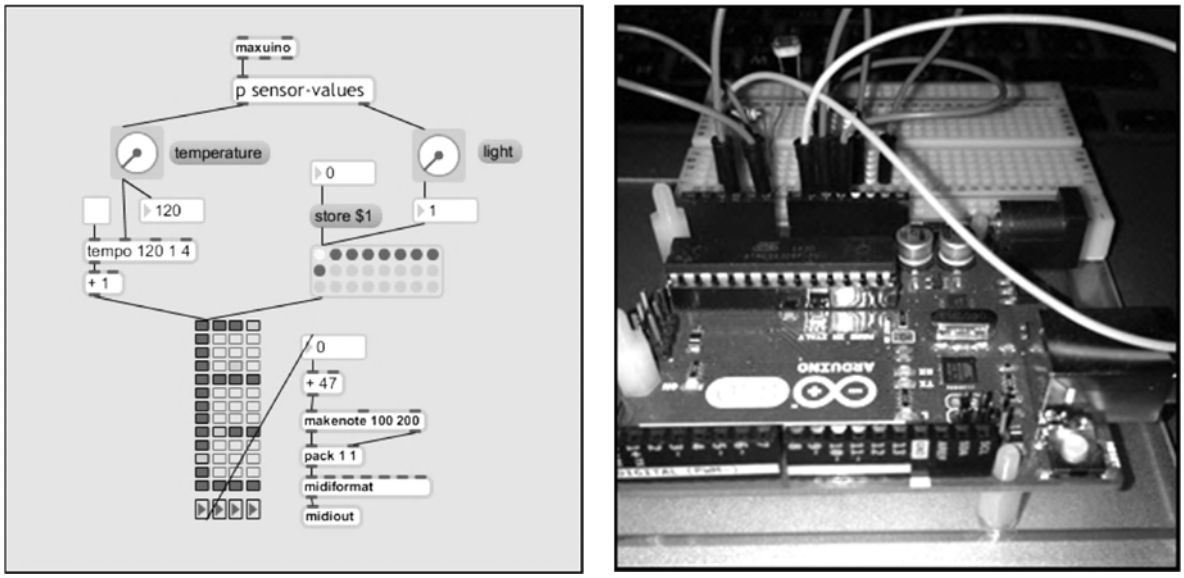


Рис. 2. Графический код узла сонификации в среде Max/MSP
и модельный сенсорный узел на базе Arduino

На данном этапе авторами проводятся лабораторные исследования, с целью усовершенствования алгоритма мэппинга параметров сонификации.

В заключение, стоит отметить потенциально широкий спектр областей возможного применения разрабатываемой системы по данному сценарию. В силу независимости рассматриваемых методов от природы сенсорной сети и задачи поиска, система может применяться как для мониторинга движения наблюдаемых объектов, так и для наблюдения параметров сенсорной наносети внутри пациента для медицинских исследований. Для изменения

области применения достаточно будет адаптировать мэппинг параметров для конкретной сенсорной сети и задачи поиска.

Список используемых источников

1. Рогозинский Г. Г., Щекочихин А. В. Модель распределенной системы генерации аудиоконтента на основе эволюционных алгоритмов // Информационные технологии и телекоммуникации. 2014. № 2. С. 20–26.

2. Cherny E., Rogozinsky G. The Internet of Machines – Technological Synergy and Computer Music // 16th Conference of Open Innovations Association Proc. 2014.

3. Рогозинский Г. Г., Щекочихин А. В. Особенности использования и корректность работы генетического алгоритма для распределенной генерации компьютерной музыки // Системы управления и информационные технологии. 2015. № 1 (59). С. 80–84.

4. Рогозинский Г. Г., Черный Е. В., Уолш Р., Щекочихин А. В. Распределенная генерация компьютерной музыки в Интернете вещей // Научно-технический вестник информационных технологий, механики и оптики. 2015. Т. 15. № 4. С. 654–660.

5. Рогозинский Г. Г., Чесноков М. А., Щекочихин А. В., Черный Е. В., Смирнов И. Н. Особенности представления и обработки данных в сети дополненной акустической реальности // Системы управления и информационные технологии. 2015. № 3 (61). С. 89–93.

6. Бондарик В. Н., Кучерявый А. Е. Прогнозирование развития Интернета Вещей на горизонте планирования до 2030 года // Радиотехника и телекоммуникации, труды МФТИ, 2013. С. 92–96.

7. Hans G. Kaper, Sever Tipei, Jeff M. Wright. Disco: An Object-Oriented System for Music Composition and Sound Design // Proc. Int'l Computer Music Conference, Berlin, 2000.

8. Hans G. Kaper, Sever Tipei, Elizabeth Wiebel. Data Sonification and Sound Visualization // Computing in Science and Engineering, Vol.1 No 4, July-August 1999. PP. 48–58.

9. Paul Vickers, B. Hogg. Sonification Abstraite / Sonification Concrete: an Aesthetic Perspective Space for Classifying Auditory Displays in the Ars Musica Domain // Proc. 12th Int'l Conf. on Auditory Display, London, UK June 20–23, 2006.

10. Vickers P. Haptic Input + Auditory Display = Musical Instrument? // Of Lecture Notes in Computer Science, vol. 4129/2006. Springer-Verlag, 2006. PP. 56–67.

11. Vickers P., Laing C., Fairfax T. Sonification of Network's Self-Organized Criticality // Pre-print arXiv: 1407.4705. June 2014.

12. Vickers P., Laing C., Debashi M., Fairfax T. Sonifcation Aesthetics and Listening for Network Situational Awareness // Conf. On Sonifiacation of Health and Environmental Data, York, UK, 2015.

13. Mascetti S., Gerino A., Picinali L., Ahmetovic D., Bernareggi C. // Pre-print arXiv: 1506.07272, June 2015.

14. Hermann T., Hunt A., Neuhoff J. Sonification Handbook. Berlin : Logos Publishing House, 2011. 586 p. ISBN 978-3-8325-2819-5.

УДК 004.49

ПРОБЛЕМЫ ОРГАНИЗАЦИИ ДОВЕРЕННОЙ ЦИФРОВОЙ СЕТИ СВЯЗИ С ИНТЕГРАЦИЕЙ УСЛУГ МЧС РОССИИ В НЕДОВЕРЕННОЙ ТЕЛЕКОММУНИКАЦИОННОЙ СРЕДЕ

С. С. Сердюк

Национальный центр управления в кризисных ситуациях МЧС России

Среди множества проблем организации доверенной сети МЧС России в недоверенной телекоммуникационной среде выделены основные – это проблемы топологии, балансировки нагрузки и безопасного масштабирования. Приведены конкретные примеры известных решений. Актуализирована научно-техническая задача синтеза комплекса механизмов безопасного масштабирования телекоммуникационной сети МЧС России.

доверенная телекоммуникационная сеть, недоверенная среда, топология, балансировка нагрузки, безопасное масштабирование, комплекс механизмов.

Для выполнения своего целевого предназначения МЧС России требуется надежная и высокотехнологичная телекоммуникационная сеть. На сегодняшний день эта миссия возлагается на цифровую сеть связи с интеграцией услуг (далее – ЦССИУ), которая является одним из основных компонентов системы управления МЧС России. За время своего становления и развития она постоянно масштабировалась и к настоящему времени охватывает территорию всей страны; при этом ее построение организовывалось в различных телекоммуникационных средах и по различным технологиям. Эволюционно обусловленное отсутствие единого высокоуровневого плана построения ЦССИУ породило множество плохо согласующихся между собой частных сегментированных сетевых решений в виде «конгломератов» технических и программных средств, и как следствие, поставило вопрос доверия к процедурам и результатам обработки и защиты информации. В этих условиях организация доверенной ЦССИУ в недоверенной телекоммуникационной среде приобретает актуальность. Анализ публикаций по вопросам информационной безопасности и устойчивости телекоммуникационных сетей позволил выделить среди множества ряд основных, рассмотренных ниже, проблем организации доверенной ЦССИУ МЧС России в недоверенной телекоммуникационной среде – это проблемы топологии, балансировки нагрузки и безопасного масштабирования. Хотя перечисленные проблемы и являются достаточно «классическими» для телекоммуникационных сетей [1], но порождающие их противоречивые факторы для ЦССИУ МЧС России имеет определенную специфику происхождения, что предполагает поиски оригинальных подходов и решений.

Проблема топологии

Проблема топологии ЦССИУ МЧС России обусловлена, во-первых, отсутствием единой концепции ее проектирования. Изначально некоторые сегменты сети создавались, как автономные. Подключение их в общую структуру ЦССИУ требовало изменения топологии этого сегмента. Во-вторых, ЦССИУ МЧС России является достаточно сложной системой. Она строится по иерархическому, многоуровневому принципу, как организационно, так и технологически: более высокие уровни управляют и обеспечивают взаимодействие более низких в иерархии уровней; уровни организационной иерархии строятся в соответствии со структурой МЧС России; уровни технологической иерархии представляют собой наложенные сети, использующие различные технологии. Подходы, используемые для решения задач проектирования, применялись для каждого из уровней отдельно, без учета взаимосвязи и взаимозависимости между уровнями. В результате, конфигурация ЦССИУ МЧС России не являться оптимальной. Одним из важных условий для решения проблемы топологии ЦССИУ является построение иерархической структуры, но при этом такой, что при выходе из строя промежуточных узлов обеспечивается выборочная доступность нижестоящих узлов или сегментов в целом. Применение комбинированных решений при построении маршрутов, использование различных протоколов маршрутизации и асимметричных маршрутов может привести топологию ЦССИУ МЧС России к более оптимальной структуре [2, 3, 4].

Проблема балансировки нагрузки

Стабильная работа ЦССИУ очень важна для решения задач, стоящих перед МЧС России. Необходимо, чтобы была связь не только между силами и средствами МЧС России, но и с местом возникновения чрезвычайной ситуации. В ЦССИУ МЧС России уже внедряются механизмы обеспечения качества обслуживания, осуществляется резервирование каналов связи, применяются различные технологии кластеризации и аварийной замены. Однако качество обслуживания обеспечивается далеко не на всех уровнях иерархии, резервирование каналов связи реализовано только для конкретных узлов, а не сегмента сети в целом, кластеризация и аварийная замена в основном применяется на крупных участках ЦССИУ МЧС России. Описанная проблема представляется актуальными задачами: возможностью эффективно использовать имеющиеся ресурсы, разработкой динамической балансировки буферных и канальных ресурсов, экономией финансовых затрат. Также остается актуальным вопрос реализации многопутевой маршрутизации для балансировки нагрузки, так как балансировка нагрузки по путям с разной метрикой (стоимостью) осуществляется в рамках известных протоколов маршрутизации преимущественно вручную, что делает этот

процесс очень чувствительным к уровню опыта и квалификации администратора сети на разных уровнях иерархии ЦССИУ МЧС России.

Проблему балансировки нагрузки ЦССИУ МЧС России также можно описать противоречием между обеспечением отказоустойчивости сети и экономией затрат, и его разрешение сводится к решению соответствующих оптимизационных задач, например, определения необходимого количества устройств для распределения заданий между ними с целью оптимизации использования ресурсов или сокращения времени обслуживания запросов. Решение задачи подобного рода для сетей описано, в частности, в [5, 6].

Проблема безопасного масштабирования

Проблема безопасного масштабирования ЦССИУ МЧС России порождается потребностями ее роста как «по вертикали», так и «по горизонтали». Масштабирование по вертикали – это наращивание «мощности» конкретных компонентов сети с целью повышения общей производительности и пропускной способности. Замена или модернизация существующих компонентов на более мощные и быстрые в условии экономии финансовых ресурсов ограниченно возможна за счет оптимального перераспределения имеющегося оборудования. Масштабирование по горизонтали происходит за счет увеличения количества рабочих станций, серверов и прочего оконечного оборудования. При этом можно наблюдать картину, когда расширение по горизонтали приводит к выделению более низшего уровня по вертикали; для вновь выделенного сегмента также становятся актуальными выше рассматриваемые проблемы. Проблема безопасного масштабирования обусловлена тем фактом, что при расширении ведомственной сети используются недоверенные телекоммуникационной среды [7]. Так, все чаще для построения каналов связи используется сеть Интернет, что с одной стороны упрощает подключение новых узлов или сегментов к сети, но с другой стороны значительно увеличивает количество угроз информационной безопасности. Некоторые решения проблемы, в том числе стандартными сетевыми средствами, приведены в [8, 9].

В то же время существует достаточная специфика масштабирования ЦССИУ МЧС России, установленная в силу опыта решения подобных задач. Во-первых, для ЦССИУ характерны большая территориальная протяженность, многоуровневость, многозвенность и многопродуктовость. Во-вторых, обеспечение мультисервисности, гетерогенности и безопасности (при доминанте последней) при сопряжении с ЦССИУ других министерств и ведомств. В-третьих, учет роли и места ЦССИУ в общей иерархии метасистемы – взаимоувязанной сети связи РФ в целом. В-четвертых, итерационный характер решения задач, возникающих при масштабировании.

И в-пятых, отсутствие научно-обоснованных и хорошо регламентированных требований по безопасному масштабированию ЦССИУ, что делает этот процесс практически не управляемым.

Эта специфика приводит, в частности, к необходимости научно-технической разработки комплекса механизмов безопасного масштабирования ЦССИУ МЧС России в недоверенной телекоммуникационной среде.

Заключение

Для первых двух из рассмотренных выше проблем организации, доверенной ЦССИУ МЧС России в недоверенной телекоммуникационной среде имеются определенные научные наработки, доведенные до технических (и технологических) решений. На путях успешного решения последней из рассмотренных проблем существует ряд специфических противоречий, связанных с отсутствием эффективного комплекса механизмов безопасного масштабирования.

На настоящий момент для разрешения указанных противоречий определен ряд научных задач. Во-первых, это формирование пула вариантов масштабирования с анализом угроз, связанных с изменениями ЦССИУ, а также возможных контрмер. Во-вторых, определение критериев и системы показателей безопасного масштабирования ЦССИУ. В-третьих, синтез специфических механизмов масштабирования ЦССИУ и их комплексирование с традиционными механизмами организации доверенной телекоммуникационной среды. В-четвертых, моделирование вариантов безопасного масштабирования ЦССИУ с оценкой их эффективности по требованиям безопасности информации. И в-пятых, выработка научно-обоснованных рекомендаций по безопасному масштабированию ЦССИУ МЧС России в недоверенной телекоммуникационной среде.

Список используемых источников

1. Буйневич М. В., Владыко А. Г., Доценко С. М., Симонина О. А. Организационно-техническое обеспечение устойчивости функционирования и безопасности сети связи общего пользования. СПб.: СПбГУТ, 2013. 144 с. ISBN 978-5-89160-087-4.

2. Агеев Д. В. Проектирование современных телекоммуникационных систем с использованием многоуровневых графов // Восточно-Европейский журнал передовых технологий. 2010. Т. 4. № 2 (46). С. 75–77.

3. Цветков К. Ю., Макаренко С. И., Михайлов Р. Л. Формирование резервных путей на основе алгоритма Дейкстры в целях повышения устойчивости информационно-телекоммуникационных сетей // Информационно-управляющие системы. 2014. № 2 (69). С. 71–78.

4. Буйневич М. В., Тиамийу О. А. Программная архитектура системы управления доверенной маршрутизацией в глобальных телекоммуникационных сетях // Информатизация и связь. 2014. № 3. С. 35–38.

5. Болодурина И. П., Парфёнов Д. И. Моделирование распределения ресурсов и динамической балансировки нагрузки в информационной системе дистанционной поддержки образовательного процесса // Параллельные вычисления и задачи управления (PACO'2012): материалы IV Междунар. конф., Москва, 24–26 окт. 2012 г. М.: ИПУ РАН, 2012. С. 173–182.

6. Лемешко А. В., Вавенко Т. В. Усовершенствование потоковой модели многопутевой маршрутизации на основе балансировки нагрузки [Электронный русурс] // Проблемы телекоммуникаций. 2012. № 1(6). С. 12-29. URL: http://pt.journal.kh.ua/2012/1/1/121_ lemeshko_multipath.pdf (дата обращения 01.03.2016).

7. 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.

8. Буйневич М. В., Магон А. Е., Ширяев Д. М. Анализ возможности безопасного масштабирования телекоммуникационной структуры АСУ путем принудительной маршрутизации трафика стандартными средствами // Вопросы современной науки и практики. Университет им. В. И. Вернадского. 2008. № 3 (13). Т. 2. С. 161–164.

9. Буйневич М. В., Иншаков О. Ю., Плаксицкий А. Б. Безопасное масштабирование конкретного варианта организации информационно-технического взаимодействия в автоматизированной системе оперативного управления пожарной охраной // Вестник Воронежского государственного технического университета. 2011. Т. 7. № 7. С. 227–228.

Статья представлена научным руководителем, доктором технических наук, профессором М. В. Буйневичем.

УДК 654.021

МОДЕЛИ КАЧЕСТВА ОБСЛУЖИВАНИЯ В СЕТЯХ IoT

О. А. Симонина, Е. А. Умиров

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

В статье вводится классификация трафика IoT на основании разделения на два базовых класса: ориентированного на восприятие человеком и на создание среды (Ambient User Experience). Анализируются модели для расчета параметров трафика с учетом пропускной способности сети и требований к QoS.

IoT, QoS.

Современный пользователь имеет наборы приложений, обеспечивающих его взаимодействие со средой. Можно сказать, что сейчас акцент делается на культуре приложений. При этом количество приложений, использующих IoT, будет расти в силу расширения области охвата Интернетом вещей.

Согласно четырехуровневой модели из рекомендации Y.2060 на нижних уровнях используется ограниченное количество технологий, отличающихся по основным параметрам: типы устройств IoT, пропускная способность, задержки, возможность построения сложных топологий (древовидных, кластеров). Однако, современный пользователь больше ориентируется на приложение, организующее его взаимодействие со средой IoT и сервисами IoT, а не технические особенности построения IoT-среды. За этот уровень отвечают технологии приложений. Средние уровни выполняют роль сопрягающих между технологиями нижних уровней, довольно разнообразных, и приложениями, задающими требования нижним уровням. Таким образом, одним из важных аспектов является обеспечение QoS для IoT, что является весьма критичным вследствие гетерогенности сети.

В таблице 1 проводится классификация по типу трафика согласно допустимому значению межконцевой задержки и допустимого уровня потерь на основе рекомендаций ITU-T Y.1541 [1], ITU-T Y.2060 [2], а также ITU-T FG M2M [3]. Такое разделение происходит из-за разнообразностей требований QoS в зависимости от предоставляемой услуги, в целях необходимости соблюдений качества информации, уложений в требуемых временных ограничениях и удовлетворений потребностей пользователей. Если рассмотреть IoT на примере сервисов здравоохранения, где необходимо наблюдение за показателями пациента, то в данном случае время является основным фактором для своевременного оказания помощи, а минимизация потерь трафика позволит избежать перезапросов и, как следствие, увеличения задержки. Таким образом, трафик можно подразделить в 1 группу из представленной таблице 1.

ТАБЛИЦА 1. Требования к трафику IoT

Тип трафика	Допустимое значение межконцевой задержки, мс	Допустимый уровень потерь, %
Интерактивный: управление и создание среды	< 50	< 0,5
Реального времени: виртуальная реальность, мониторинг	50–150	< 1
Реального времени: мультимедия	150–250	< 2
Потоковый, неэластичный: мультимедия, данные	250–400	< 3
Эластичный	Не нормировано	Не нормировано

Интернет Вещей требует новых моделей оценки качества услуг, так как появляются новые требования к сервисам и новый подход к предоставлению услуг. Проведем анализ существующих моделей QoS с целью определения механизмов, подходящих для поддержки QoS IoT.

Анализ моделей оценки QoS

Существующие модели оценки качества можно разделить на два класса: учитывающие гетерогенность сети и ориентированные на наборы приложений (табл. 2).

ТАБЛИЦА 2. Модели оценки QoS

Ориентированные на наборы приложений	Учитывающие гетерогенность сетей IoT
QoX [4]	Servilla middleware [6]
EuQoS [5]	QoS Manager (OpenIoT) [7]

Модель QoX – определение новой структуры QoS, которая будет способствовать развитию тенденции, определяющей QoS/QoE измерения в различных сетях [4]. Ключевым моментом этой модели является включение в интегрированную оценку качества услуги фактора восприятия конечным пользователем, что должно облегчить сохранение требуемого качества соединения и стабильности сети для заданного спектра услуг. Данная модель хорошо подходит для учета особенностей мультимедийных услуг.

Основная цель проекта EuQoS – это определить и реализовать архитектурную модель сети, способную гарантировать QoS точка-точка для заданных типов услуг поверх гетерогенных сетей [5]. Абоненты EuQoS должны быть способны использовать как зарегистрированные, так и существующие отдельно приложения и предоставлять сервисы с гарантированным QoS. Идея технологии заключается в проведении виртуализации на нижних уровнях сетевой архитектуры, позволяющую организовать однородность сетевой среды.

Основная идея модели QoS Manager, поддерживаемой проектом OpenIoT – создание сегментов сетей IoT, реализованных на разных технологиях, и объединение их через QoS-брокер [6]. Таким образом, получем гетерогенную сеть, объединенную в единое пространство обеспечения QoS через систему специализированных брокеров и сетевых агентов.

Servilla middleware предлагает поддержку энергоэффективности, которая рассматривается как еще один показатель качества [7]. Для решения вопроса создания единой среды поверх гетерогенной сети предлагается создание сервисной платформы на более низких уровнях, т. е. каждая сетевая технология должна обладать сервисной платформой, отвечающей на набор услуг и типы данных.

QoS Manager и Servilla middleware ориентированы на создание дополнительных элементов на нижних уровнях, позволяющих объединить разнородные технологии нижних уровней. QoS Manager – создает набор QoS-брокеров и объединяет их единой системой управления. Servilla middleware

создает единую сервисную платформу, к которой подключаются гетерогенные сети, управление качеством услуг осуществляется централизовано.

Таким образом, можно сформулировать показатели, которые необходимо учитывать для поддержки QoS в сетях IoT:

- модель организации гетерогенной сети IoT;
- тип трафика IoT;
- набор параметров QoS, ориентированный на приложения;
- тип технологии, по которой построена сеть IoT.

Модель организации гетерогенной сети показывает, нужно ли учитывать сервисную платформу или QoS-брокер и вносимые ими задержки и, возможно, потери и ограничения ресурсов. Тип трафика задает требования к показателям QoS и их набору. Набор параметров QoS позволяет определить, какие из них важны для предоставления данного сервиса. Тип технологии накладывает ограничения на функционал: возможность обратной связи, пропускная способность, количество промежуточных узлов и пр.

Расчет основных параметров QoS

Для расчета задержек в сквозном соединении воспользуемся выражением:

$$T_{e2e} = T_{PAN} + T_{br} + T_{br-appl},$$

где T_{e2e} – задержка в сквозном соединении в одном направлении, T_{PAN} – задержка в сети PAN, T_{br} – задержка на QoS-брокере или сервисной платформе, $T_{br-appl}$ – задержка в соединении брокер-приложение, которая может включать в себя и транспортные сегменты. Сеть PAN – *(Personal Area Network)* – это сеть, построенная «вокруг» человека. Данные сети призваны объединять все персональные устройства пользователя (телефоны, смартфоны, карманные персональные компьютеры, ноутбуки, гарнитуры и др.). Применительно к IoT такая сеть строится «вокруг» устройства («вещи»).

В силу использования технологий беспроводного доступа в сетях IoT, для расчета потерь можно использовать модель Келли, которая позволяет оценить уровень потерь на основании доступной пропускной способности [8]:

$$r_0 = 1 - AT,$$

где AT – занятый канальный ресурс в байтах и определяется как:

$$AT = \sum_k a_k b_k \left(1 - \pi_k\right),$$

откуда

$$\pi_k = \sum_{i=v-b_k+1}^{v} p(i),$$

где, b_k – число единиц ресурса, необходимое для обслуживания одного кадра, k – количество источников трафика, v – требуемый канальный ресурс, i – количество единиц ресурса, используемого всеми участниками:

$$i = \sum_n i_n b_n .$$

Тогда вероятность нахождения кадра на обслуживании:

$$P(i) = \sum_i p(i_1, i_2, \ldots, i_n), i = 0,1,\ldots(n+m).$$

Данные соотношения позволяют оценить потери доступе сети IoT для беспроводных технологий с поддержкой пакетной передачи исходя только из свободного канального ресурса.

Выводы и дальнейшие работы

В данной статье предложены классификация трафика IoT исходя из основных показателей QoS с учетом существующих рекомендаций и стандартов, классификация существующих моделей поддержки QoS в гетерогенных сетях IoT. Для расчета основных показателей QoS с учетом особенностей построения сетей IoT предлагается опираться на теорию телетрафика и модель Келли.

Актуальность рассматриваемого вопроса позволяет судить о необходимости работы в данном направлении. Таким образом можно сформулировать возможные направления дальнейших исследований:

– расширение классификации трафика IoT с учетом новых специфических показателей QoS: энергосбережения и стабильности узлов;

– расширение модели расчета показателей QoS с учетом энергосбережения и стабильности узлов.

Список используемых источников

1. Network performance objectives for IP-based services [Electronic resource] // ITU-T Rec. Y.1541 – 2011. URL: https://www.itu.int/rec/T-REC-Y.1541-201112-I/en (дата обращения 10.04.2016).

2. Overview of the Internet of things [Electronic resource] // ITU-T Recommendation Y.2060 – 2012. URL: https://www.itu.int/rec/T-REC-Y.2060-201206-I (дата обращения 10.04.2016).

3. M2M enabled ecosystems: e-health [Electronic resource] // ITU-T FG M2M. – 2014. URL: https://www.itu.int/pub/T-FG-M2M-2014-D1.1 (дата обращения 10.04.2016).

4. Ibarrola E., Saiz E., Zabala L., Cristobo L., Xiao J. et al. QoXphere: A New QoS Framework for Future Networks // ITU Kaleidoscope: Building Sustainable Communities (K-2013). 2013. PP. 1–7.

5. Masip-Bruin X., Yannuzzi M., Serral-Gràcia R., Domingo-Pascual J., Enríquez-Gabeiras J., Callejo M., Diaz M., Racaru F., Stea G., Mingozzi E., Beben A., Burakowski W., Monteiro E., Cordeiro L. et al. The EuQoS System: A Solution for QoS Routing in Heterogeneous Networks // IEEE Communications Magazine. 2007. PP. 96–103.

6. Marjanovic M., Skorin-Kapov L. et al. D4.6. Quality of Service (QoS) for IoT services [Electronic resource] // Open source blueprint for large scale self-organizing cloud environments for IoT applications. 2014. URL: http://www.openiot.eu /?page_id=20 (дата обращения 10.04.2016).

7. Fok C. L. et al. Challenges of satisfying multiple stakeholders: quality of service in the internet of things // Proceedings of the 2nd Workshop on Software Engineering for Sensor Network Applications. ACM, 2011. PP. 55–60.

8. Lavrukhin V., Simonina O., Volodin E. An experimental study of the key QoS parameters in public Wi-Fi networks // Ultra Modern Telecommunications and Control Systems and Workshops (ICUMT), 2014 6th International Congress on. IEEE, 2014. PP. 198–203.

УДК № 004.056.55:003.26

ИССЛЕДОВАНИЕ ПРАКТИЧЕСКОЙ ВОЗМОЖНОСТИ ВЗЛОМА ПО ЦЕПЯМ ЭЛЕКТРОПИТАНИЯ АППАРАТНО РЕАЛИЗОВАННЫХ ШИФРОВ НА ПРИМЕРЕ ГОСТ 28147-89

С. В. Тихонов

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

Рассматриваются особенности и сложности практической реализации взлома блокового шифра (в частности ГОСТ 28147-89), выполняющегося на микроконтроллере Atmel, с применением побочной атаки измерения потребляемой мощности в цепи питания. Описывается комплекс технических средств, позволяющих реализовать атаку с минимальными финансовыми затратами. Определяются операции, приводящие к наибольшей утечке секретной информации по цепи питания. Даются предложения по повышению эффективности реализации атаки.

секретный ключ, алгоритм DES, атаки DPA, SPA, S-box, атака по питанию, атака по побочным каналам, дифференциальный анализ мощности.

Современные блоковые шифры (такие как 3DES, AES, ГОСТ 28147-89) устойчивы к любым известным методам аналитического криптоанализа. Но шифр является лишь математическим алгоритмом, он, в свою очередь, реализуется на интегральных чипах. Чип (ввиду своих конструктивных особенностей) может являться источником «утечки» информации о секретных параметрах шифра, иногда её удаётся использовать для взлома, выполняющегося на чипе шифра. Атаки такого типа называют атаками по побочным каналам, наиболее известная из них – DPA (дифференциальный анализ мощности), в её основе лежит базовое допущение, что энергопотребление чипа, зависит от обрабатываемых им данных.

Выполнение DPA можно условно разделить на три этапа:

1. Снятие данных об энергопотреблении чипа.
2. Анализ и предварительная обработка полученных данных.
3. Восстановление секретного ключа, с использованием статистических алгоритмов, описанных в работах [1, 2, 3].

Реализация каждого из этих этапов (в особенности первых двух) сопряжена с необходимостью решения ряда проблем, в основном технического характера, которые в изученной литературе оставались практически нераскрытыми. Это приводит к тому что даже детально изучив соответствующую литературу повторить атаку оказывается сложно. Поэтому автор, в рамках лабораторного эксперимента, попытался раскрыть сложности именно практической реализации DPA.

Для выполнения первого этапа DPA было необходимо найти недорогой, но эффективный способ измерения энергопотребления чипа, а для этого определить требования к характеристикам измерительного оборудования. Базовыми элементами современных интегральных чипов являются логические вентили (ЛВ), они выполняют элементарную логическую операцию и представляют собой связку нескольких полевых транзисторов. Сочетанием ЛВ получают узлы большей агрегации, вплоть до АЛУ, ОЗУ, ПЗУ. Подавляющая доля энергопотребления ЛВ приходится на моменты их переключения т. е. когда к примеру, в ячейку ОЗУ на место логического «0» записывается «1» (или наоборот) – энергопотребление будет высоким, в противном случае оно будет ничтожно малым. Данное свойство энергопотребления ЛВ распространяется практически на все современные интегральные чипы. Поэтому в качестве анализируемого чипа был выбран вполне типовой микроконтроллер Atmel ATmega16L-8AU смонтированный на макетную плату по принципу минимальной достаточности (монтировались исключительно необходимые периферийные компоненты, таким образом и в таком качестве, чтобы обеспечить максимально стабильную работу чипа). Его тактирование осуществлялось от кварцевого генератора с частотой 2 МГц, питание – от стабилизированного источника Robiton SN1000S, перед контактами питания чипа также были смонтированы два конденсаторных фильтра, а в промежутке между ними установлен стабилизатор напряжения LM7805CV (для защиты даже от минимальных просадок напряжения в случае нестабильной работы бытовой сети). Отдельные конденсаторные фильтры и стабилизаторы напряжения были установлены перед контактами питания кварцевого генератора тактового сигнала и преобразователя уровней сигнала RS232 ↔ UART (необходимого для согласования интерфейса RS232 ПК и интерфейса UART приёмопередатчика микроконтроллера). В разрыв контакта земли чипа был установлен металлопленочный SMD резистор номиналом 10 Ом. Согласно [2, 3] переключение каждого простейшего ЛВ типа «НЕ» обуславливает всплеск

тока в 10–20 мкА, что по закону Ома повлечёт скачок напряжения на резисторе в пределах 100–200 мкВ. Что касается полосы пропускания, то при тактировании чипа от кварцевого генератора на 4–8 МГц теоретически [2, 3] должно хватить полосы в районе 50–80 МГц.

Задача измерения столь малых сигналов, к тому же изменяющихся на весьма большой частоте, является крайне специфичной. Самым простым способом кажется использование осциллографа, однако подавляющее их большинство в своей основе имеет 8-ми разрядный АЦП, что ограничивает чувствительность по напряжению «стандартными» 2 мВ/Дел. Для достижения большей чувствительности (до 200мкВ/Дел и даже выше) зарубежные исследователи используют активные дифференциальные пробники (со встроенным усилителем). Однако их стоимость высока ($5–10 тыс.), да и подходят они лишь к весьма дорогим осциллографам (за $10–15 тыс.). Поэтому в настоящем эксперименте было принято решение использовать АЦП AD9652 фирмы Analog Devices, разрядностью 16 уровней квантования в динамическом диапазоне –1,8 ÷ 1,8 В (теоретически, разрешение по напряжению составит 54,9 мкВ). АЦП был приобретён в составе оценочной платы (AD9652-310EBZ Evaluation Board, стоимостью $420), и дополнительной платы сопряжения с ПК (HSC-ADC-EVALCZ FPGA-Based Data Capture Kit, стоимостью $620), имеющей буферную память на 64'536 отсчётов, реализацию функции триггера и интерфейс связи с ПК (USB), в комплекте с программным обеспечением VisualAnalog. Для тактирования АЦП, вместо рекомендуемого производителем высокостабильного генератора Rohde Schwarz SMA 100 (стоимостью $25 тыс.) был использован кварцевый генератор EPSON за $20, с частотой 100 МГц, что позволяет оцифровывать сигнал с частотными составляющими до 50 МГц.

С использованием блока АЦП, ПК и платы с микроконтроллером была собрана измерительная установка (рис. 1), позволяющая анализировать малейшие колебания энергопотребления микроконтроллера при выполнении любых операций.

Рис. 1. Упрощённая блок-схема измерительной установки

На втором этапе были проанализированы, снятые при помощи измерительной установки, данные об энергопотреблении микроконтроллера – вначале при выполнении «пустых» команд «nop» (рис. 2*а*).

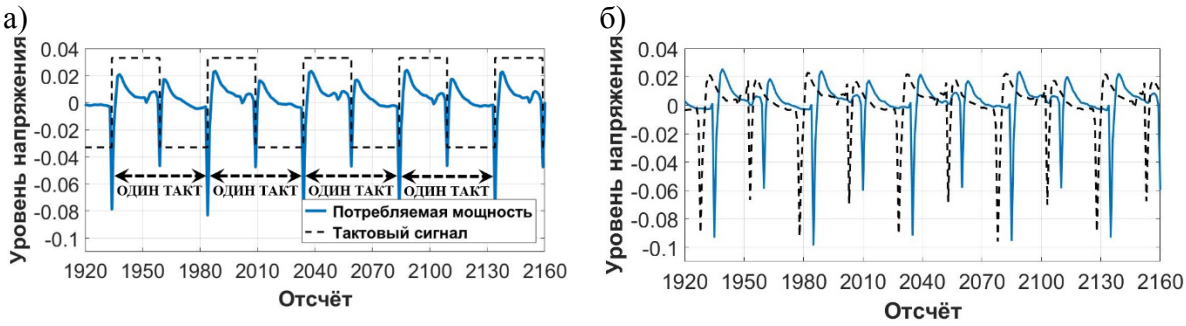


Рис. 2. Участок формы сигнала, полученной при выполнении команды «nop»: а) привыполнении «пустых» команд; б) при повторении эксперимента

На снятой форме сигнала отчётливо видны всплески потребляемой мощности с периодом кратным тактовой частоте чипа. Однако, за счёт нестабильности генераторов, тактирующих микроконтроллер и АЦП, при повторении эксперимента, рассматриваемые всплески смещаются по временной шкале (рис. 2*б*). Данный эффект серьёзно затрудняет реализацию атаки, поэтому было создано ПО, выравнивающее формы сигнала.

Затем, учитывая, что шифры реализуются на чипах путём последовательного выполнения ряда простых команд, автором была детально исследована зависимость энергопотребления чипа от данных, обрабатываемых на множестве разных операций. Экспериментально было подтверждено предположение о существовании зависимости энергопотребления чипа от обрабатываемых им данных (в частности от их веса Хэмминга). Более того была обнаружена очень существенная зависимость энергопотребления от выполняемой чипом операции, к примеру, при пересылке байта данных из рабочего регистра в ОЗУ (выполнении операций XOR, арифметического сложения или перемещения данных между рабочими регистрами) энергопотребление на соответствующих тактах может возрастать до 20 мВ (в зависимости от веса Хэмминга обрабатываемой комбинации – рис. 3), а при чтении байта данных из ОЗУ/ПЗУ в рабочий регистр всплеск энергопотребления не будет превышать 2–3 мВ.

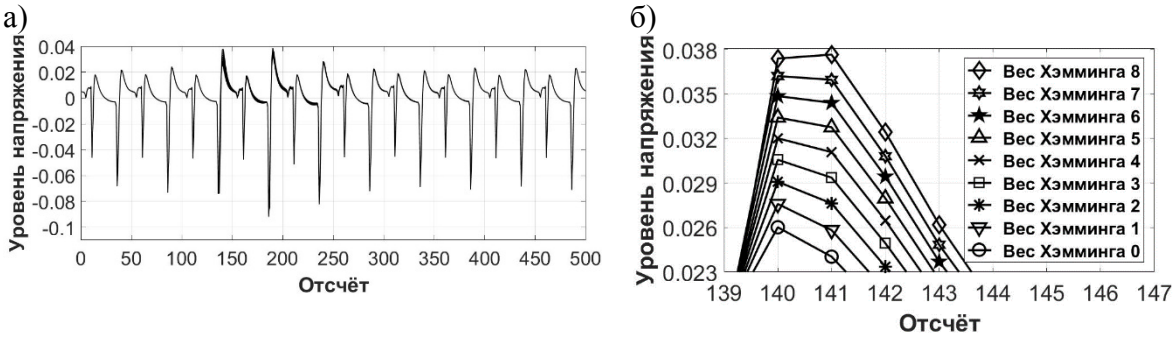


Рис. 3. Девять усреднённых (для минимизации шума) форм сигнала, полученных при пересылке в ОЗУ байт с различным весом Хэмминга: а) полная форма сигнал; б) увеличенный участок с максимальным всплеском

Также был обнаружен ряд особенностей снимаемых форм сигнала, не описанных в изученных автором в источниках. Наиболее интересная из них заключается в том, что энергопотребление чипа зависит от обрабатываемых данных не только на тех тактах на которых команда выполнялась, но и на 3–5 последующих тактах (постепенно затухая). Этот эффект безусловно осложнит реализацию атаки на полноценные алгоритмы шифрования – там команды выполняются последовательно друг за другом, поэтому скачки энергопотребления на любом такте окажутся зашумлены наложением «остаточных» всплесков энергопотребления от предыдущих тактов.

На третьем этапе эксперимента, выявленное явление зависимости энергопотребления чипа от обрабатываемых им данных, было использовано для восстановления секретного ключа шифра. Для этого на анализируемом микроконтроллере был реализован шифр ГОСТ 28147-89. Вначале был собран массив из 5-ти тыс. форм сигнала, характеризующих энергопотребление чипа при шифровании случайных сообщений. Затем как это было описано в [1, 2, 3] начиная с первого раунда шифра производился перебор небольших блоков раундового ключа, на каждом варианте которого, для массива зашифрованных сообщений рассчитывался выход соответствующего S-box. После этого вычислялись корреляционные функции, характеризующие зависимость между весом Хэмминга выхода S-box, полученного на предполагаемом подключе, и отсчётами всех форм сигнала. Корреляционная функция, соответствующая истинному подключу должна иметь наибольшие всплески, что полностью подтвердил наш эксперимент (рис. 4).

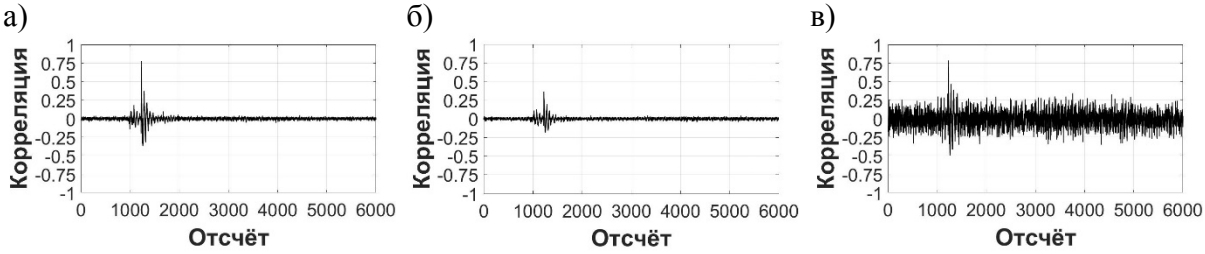


Рис. 4. Корреляционные функции для 8-го S-box ГОСТ 28147-89 первого раунда, полученные с использованием 5-ти тыс. форм сигнала на: а) истинном подключе; б) наихудшем ложном подключе; в) на истинном подключе с использованием 50-ти форм сигнала

Анализ полученных результатов позволяет сделать вывод, что даже несмотря на явление остаточной корреляции, успешная реализация DPA в отношении полноценных шифров весьма возможна, при этом не требуется детальных знаний о чипе и особенностях реализации на нём шифра. Также, подтвердился тот факт, что любую шумовую компоненту, присутствующую на снятых формах сигнала, можно исключить увеличением количества

обрабатываемых форм сигнала (рис. 4*в*). Но накопление больших выборок может и не потребоваться – используемая измерительная установка позволяла однозначно определить истинный подключ даже после накопления всего 50-ти форм сигнала. Восстановление одного раундового ключа шифра ГОСТ 28147-89 на имеющейся измерительной установке (в случае использования 5-ти тыс. форм сигнала) заняло у автора порядка 3-х часов, при этом по одному часу потребовалось на: сбор форм сигнала, их выравнивание и восстановление секретного ключа. По итогу можно утверждать, что реализация DPA вполне возможна с использованием оборудования стоимостью менее $2 тыс., что делает эту атаку принципиально доступной широкому кругу лиц, более того атака достаточно просто автоматизируется.

Автор выражает благодарность проф. Коржику В. И. за полезное обсуждение результатов работы.

Список используемых источников

1. Коржик В. И., Тихонов С. В. О возможности взлома аппаратной реализации шифра ГОСТ // Проблемы информационной безопасности. Компьютерные системы. 2012. № 3. С. 53–62.

2. Peeters E. Advanced DPA Theory and Practice: Towards the Security Limits of Secure Embedded Circuits. Springer. 2013.

3. Mangard S., Oswald E., Popp T. Power Analysis Attaks: Revealing the Secrers of Smart Card. Springer. 2007.

Статья представлена научным руководителем, доктором технических наук, профессором В. И. Коржиком.

УДК 654.9, 681.5

ИМИТАЦИОННАЯ МОДЕЛЬ СИСТЕМЫ DPI НА ОСНОВЕ ПРОГРАММНОГО ОБЕСПЕЧЕНИЯ GPSS WORLD

В. В. Фицов

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

В данной статье рассмотрены вопросы разработки и использования имитационной модели системы DPI. В качестве среды моделирования применяется ПО GPSS World. При построении имитационной модели учитывается общая архитектура системы DPI. Приведены алгоритмы модели. Произведена попытка оценки параметров производительности системы за счет изменения величины входящего потока трафика.

DPI, сигнатура, QoS, GPSS, система массового обслуживания (СМО), сеть массового обслуживания (СеМО).

Система DPI (Deep Packet Inspection, глубокого анализа пакетов) выявляет принадлежность потока пакетов к конкретному приложению, а затем, при необходимости, блокирует или ограничивает его скорость передачи в соответствии с индивидуальными политиками безопасности (тарифными планами). Для этого проводится точная классификация, применяются механизмы обеспечения QoS (Quality of Service, качества обслуживания) на сети, ведется всеобъемлющая статистика по передаваемому трафику.

В России DPI стали применять с 2004 г., и сейчас эту технологию используют ТрансТелеКом, Ростелеком, Мегафон, МТС, Билайн [1], Yota [2], МГТС [3]. Благодаря таким мерам удалось отказаться от постоянного расширения внешних каналов связи, повысить емкость сети, и снизить капитальные затраты [2].

Проблема существующих систем DPI заключается в том, что в погоне за большей точностью анализа и производительностью, в частности, для нужд обеспечения QoS, возникает и обратный процесс дополнительного снижения QoS, который безусловно необходимо уменьшить. Применение имитационной модели сетевой конфигурации DPI системы позволит определить необходимые аппаратные характеристики системы наилучшим образом подходящие под существующую пользовательскую нагрузку.

Представление архитектуры системы DPI в качестве сети массового обслуживания (СеМО)

Имитационная модель должна отражать архитектуру системы DPI. Однако, архитектура системы отличается в зависимости от вендора и области применения: для фиксированных или сотовых сетей связи [4, 5, 6, 7]. Поэтому для построения модели следует выделить основные элементы системы в качестве обобщенной архитектуры, изображенной на рисунке 1.

Каждый из серверов DPI, показанный на рисунке 1, выполняет свои задачи, и активно взаимодействует с остальными:

Bypass – в случае отказа системы DPI, переводит поступающий на фильтр трафик в сеть;

Front-End – проводит глубокий анализ пакетов потоков трафика;

Аппаратный фильтр – применяет политики (блокировка, ограничение, пропуск) и ведет статистику;

Back-End – хранит методы исполнения политики, статистику и сигнатуры;

PCRF (*Policy and Charging Rules Function*) – принимает решения о применении политики и возвращает ее номер.

Каждый из серверов DPI с точки зрения телетрафика является СМО (системой массового обслуживания), а система DPI может быть

представлена как сеть массового обслуживания (CeMO), состоящая из Bypass, аппаратного фильтра, Front-End, PCRF и Back-End.

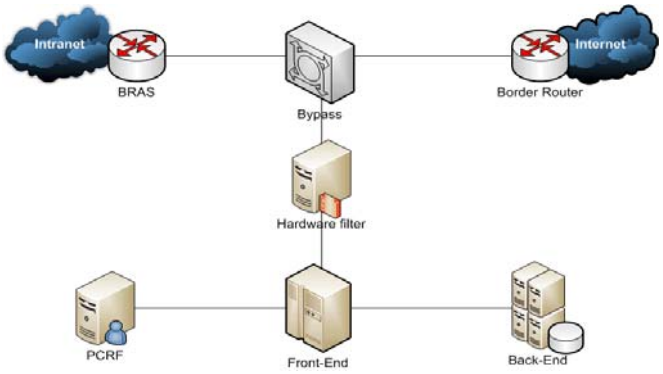


Рис. 1. Обобщенная архитектура системы DPI

На основе обобщенной архитектуры системы DPI, показанной на рисунке 1, можно построить функциональную модель. Функциональное взаимодействие между СМО определит направление потока заявок в имитационной модели между СМО. В функциональной модели в качестве СМО1 выступает аппаратный фильтр совместно с Bypass, который можно определить, как часть аппаратного фильтра. Связано это с тем, что в случае отказа системы DPI, Bypass инициирует поток не фильтруемого и не анализируемого трафика – поток необработанных заявок системы. СМО1-3 соответствуют Front-End, PCRF и Back-End.

Универсальная система моделирования GPSS World

При расчете параметров инфокоммуникационных систем и сетей успешно применяют методы программного моделирования (ПО network simulator-2 (ns-2), ns-3, OpNet simulator, AnyLogic, GPSS World).

Для построения имитационной модели на основе CeMO был выбран классический симулятор GPSS (*General Purpose Systems Simulator*, Универсальная система моделирования) систем массового обслуживания. В основе алгоритмов GPSS лежит дискретно-событийный подход и имеется большой набор законов распределения для законов поступления и обработки трафика [8]. Модели GPSS состоят из сети «Блоков», представляющие действия или задержки, через которые проходит набор «Транзактов» [9]. Весь процесс моделирования и есть последовательность одного Транзакта, перемещающегося по Блокам. Написание имитационной модели системы DPI, требует получить набор Блоков для обеспечения поведения Транзактов в соответствии с реальной системой. Исходя из того, что система DPI представлена как CeMO из четырех СМО, имитационная модель должна содержать четыре устройства, описанных набором блоков очередей и обработки, и их функционального взаимодействия, представленного блоками переходов между устройствами.

В результате симуляции GPSS World выдает информацию о работе устройства (СМО), очередей и значения отслеживаемых переменных. Отчет о работе устройства включает количество транзактов, прошедших через устройство (ENTRIES), среднее время обработки одного транзакта устройством (AVE. TIME). Отчет по статистике в очередях содержит: максимальную длину очереди (MAX), общее количество входов транзактов (ENTRY), среднюю длину очереди (AVE. CONT.), среднее время пребывания транзактов в очереди (AVE. TIME).

Имитационная модель позволит определить влияние алгоритмов обработки заявок серверов DPI на задержку определения потоков трафика.

Имитационная модель

На языке описания имитационной модели GPSS были определены основные функции серверов системы DPI – аппаратного фильтра, Front-End, PCRF, Back-End. Например, блоки определяющие устройство PCRF: QUEUE, SEIZE, DEPART – определяют работу очереди PCRF, ADVANCE – время обработки транзактов, RELEASE, TRANSFER – вероятность положительного или отрицательного ответа от PCRF к Front-End. Алгоритм работы имитационной модели DPI показан на рисунке 2.

В фильтре описывается поступление заявки, распределение с заданной вероятностью на уже известные потоки и требующие анализа. Получение инструкций от Front-End, обработка новых заявок и направление заявок в сеть, имеют различное время обработки.

Front-End анализирует пакеты, обрабатывает ответы от PCRF и Back-End, отправляет инструкции на фильтр. С заданной вероятностью в ходе анализа заявка считается определенной, и отправляет инструкции на фильтр, либо запрашивается номер политики на PCRF сервере. Ответ от PCRF с номером политики, с заданной вероятностью сообщает, что политика известна, либо необходимо запросить подробности на Back-End.

Первичные результаты работы имитационной модели

В модель были поданы потоки от 1 до 1 млн транзактов. В первую очередь отслеживалось время необходимое для их обработки системой и количество транзактов поступившее на каждое из устройств, что показано в таблице. Заметно, что на аппаратный фильтр поступают не только заявки на обработку, но и правила применения политик. Всего на аппаратный фильтр поступает приблизительно 120 % от изначального числа заявок. Исключение составляет имитация с 1 млн транзактов, в ходе которой произошла перегрузка системы DPI. Front-End обычно оказывается загружен 35 % транзактами от изначального числа, PCRF – 12 %, а Back-End – 3 %. Такое распределение заявок по СМО в имитационной модели, подтверждает функциональную модель, с заданными в ней вероятностями.

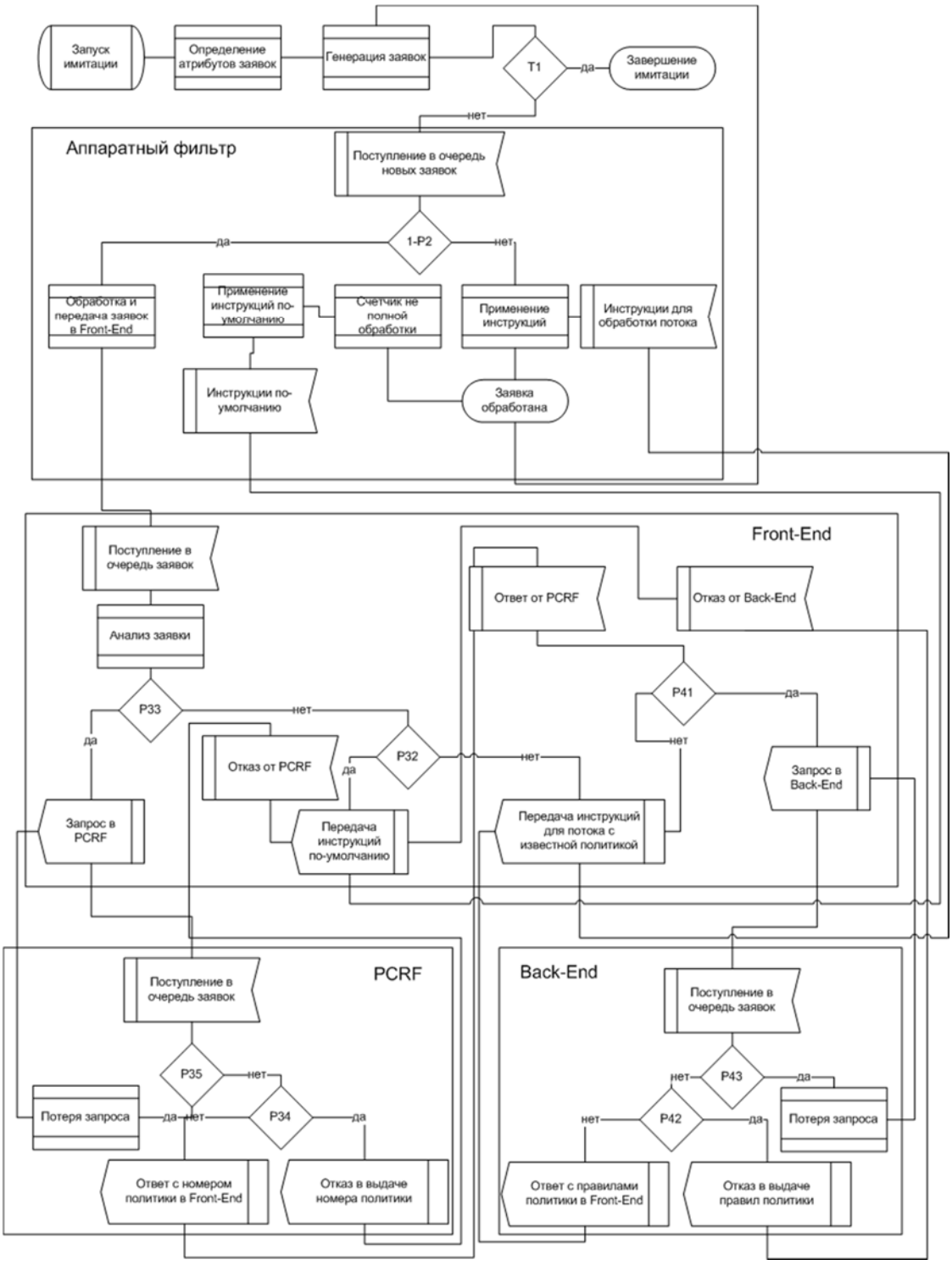


Рис. 2. Упрощенный алгоритм имитационной модели серверов DPI

Кроме того, в таблице показано среднее число транзактов в очереди поступившее на каждое из устройств и среднее время обработки транзакта устройством. Величины средней очереди устройств показывают одинаковую загрузку количеством транзактов аппаратного фильтра и Front-

End, и низкую загрузку PCRF, а шанс появления запросов на Back-End в ходе имитации возникает только после 100 000 транзактов.

Данные наглядно демонстрируют возможность более эффективного использования PCRF и Back-End способных обрабатывать большую нагрузку от нескольких серверов Front-End. Этот вывод подтверждается средним временем обработки транзактов в PCRF и Back-End, которые практически не создают задержки. С другой стороны, видно, что значительное время для обработки требуются Front-End, который не справляется при потоке транзактов в 1 млн (28 часов на обработку).

ТАБЛИЦА. Характеристики производительности устройств

Поток транзактов	Время, мс	фильтр			Front-End			PCRF			Back-End		
		транзактов, шт	ср. оч., шт	ср. вр. обр., с	транзактов, шт	ср. оч., шт	ср. вр. обр., с	транзактов, шт	ср. оч., шт	ср. вр. обр., с	транзактов, шт	ср. оч., шт	ср. вр. обр., с
1	0	1	0	0	0	0	0	0	0	0	0	0	0
10	1	11	0,14	0	1	0	0	0	0	0	0	0	0
100	5	117	7,5	0	25	5,4	0	7	0,01	0	1	0	0
1 к	49	1,2 к	96	0	333	94	0,01	114	0,03	0	25	0	0
10 к	510	12 к	1024	0,04	3,6 к	1 к	0,14	1,3 к	0,03	0	307	0	0
100 к	5 к	120 к	10,1 к	0,4	35 к	10 к	1,4	12 к	0,03	0	2,9 к	0	0
1 М	50 к	200 к	100 к	101 к	351 к	141 к	101 к	122 к	100к	0,03	29 к	28 к	0

Разработанная имитационная модель системы DPI в симуляторе GPSS World позволяет задать необходимые параметры системы, и получить данные о загрузки серверов СеМО. Результаты имитации могут быть использованы для более эффективного распределения аппаратных ресурсов между серверами системы DPI. Что позволит определить баланс между количеством серверов, затратами на аппаратные ресурсы и достигаемыми параметрами QoS.

Список используемых источников

1. Солдатов А., Бороган И. Интернет-фильтрация в России: еще и слежка [Электронный ресурс] // Forbes, 11.2012. URL: http://www.forbes.ru/tehno/194198-internet-filtratsiya-v-rossii-eshche-islezhka (дата обращения 17.02.2016).

2. Yota и компания «Инфосистемы Джет» внедрили комплекс по управлению трафиком в сети оператора [Электронный ресурс] // Инфосистемы Джет, 06.2014. URL: http://www.jet.msk.su/press_center/news/detail.php?ID=3820&post=-32711743_1565 (дата обращения 17.02.2016).

3. Аршан Л. DPI против сетевой нейтральности: МГТС заставит абонентов платить больше? [Электронный ресурс] // Информационный проект Telekomza, 08.2014. URL: http://telekomza.ru/2014/08/29/dpi-protiv-setevoj-nejtralnosti-mgts-zastavit-abonentov-platit-bolshe/ (дата обращения 17.02.2016).

4. Сибгатулин М. DPI [Электронный ресурс] // Информационно-аналитический портал NAG.ru, 08.2012. Код доступа: http://nag.ru/articles/article/22432/dpi.html/ (дата обращения 17.02.2016).

5. Trammell B., Boschi E., Procissi G. Identifying skype traffic in a large-scale flow data repository // III International Workshop "Traffic Monitoring and Analysis", Berlin: Springer. 2011, PP. 72–85.

6. Сенченко Ю. Х. Система DPI: генератор добавленной стоимости седьмого уровня // Мобильные телекоммуникации. 2012. № 8. С. 4–6.

7. Сенченко Ю. Х. НТЦ «Протей»: подходы к тарификации пакетного трафика в сетях мобильного широкополосного доступа // Мобильные телекоммуникации. 2012. № 9–10. С. 8–9.

8. Бронов С. А. Имитационное моделирование : учебное пособие. Красноярск : ФГОУ ВПО «Сибирский федеральный университет», 2007. 82 с.

9. GPSS World Tutorial Manual. Copyright Minuteman Software. Holly Springs, NC, U.S.A. Fifth Edition 2009 (пер. ИТМО, 2013, 390 с.).

Статья представлена заведующим кафедрой, доктором технических наук, профессором Б. С. Гольдштейном.

УДК 654.739

КОРРЕЛЯЦИОННЫЙ И ЭВРИСТИЧЕСКИЙ АНАЛИЗ ДЕЙСТВИЙ САМОМОДИФИЦИРУЮЩЕГОСЯ КОДА ДЛЯ ЗАЩИТЫ ИНФОРМАЦИИ В ИСПОЛНИМЫХ ФАЙЛАХ

С. И. Штеренберг

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

В статье рассматривается способы представления элементов самомодифицирующегося кода в исполнимых файлах для адаптивных систем. Исходя из представленных способов, следует вывести корреляционный и эвристический анализ действия самомодифицирующегося кода с целью выведения технических

характеристик работы программного обеспечения. Данный самомодифицирующийся код предназначен для защиты программного обеспечения от нарушения целостности.

саморазвивающийся код, исполнимый файл, защита информации, программное обеспечение, адаптивная система.

В работе [1] рассматривались способы представления элементов стеговложения информации в исполнимые файлы на основе самомодифицирующегося код для адаптивных систем работающий в закрытых локальных вычислительных сетях для надежной защиты информации. В результате теоретического анализа и приведенной там методики было выявлено, что имеющееся антивирусное ПО удовлетворяет лишь малой части требований. Создание и внедрение надежной системы защиты от быстро распространяющихся вирусов требует соблюдения всех перечисленных требований. Рассмотрен пример самомодификации файлов и дополнительного скрытого внедрения в код. Важно отметить, что должны сохраняться, прежде всего, целостность и неизменяемость информации при ее передаче.

Применение средств стеганографии адаптивных систем имеет достаточно многообещающие перспективы в силу ряда причин. Во-первых, сокрытие информации в исполняемых файлах имеет высокий уровень секретности – в большинстве случаев исходный и модифицированный файл будет иметь одинаковый размер и функционал. Во-вторых, стегоанализ данного контейнера и атаки на него являются затруднительными в силу особенностей вложения информации в исполняемый файл.

Экспериментальный анализ в работе [1, 2] показали, что комплекс методик решить следующие задачи:

1. Скрытность передаваемых сообщений.
2. Реализацию адаптивных функций окружного ПО.
3. Улучшение производительности и скорости обработки информации, не обращая внимания на системы защиты информации, которые в свою очередь тратят минимум объема контейнеров.

Вышеперечисленные свойства достигаются за счет исследования S – величины количества вложенной информации в битах и Z – объёма вкладываемой информации. Исследования в работах [3] и [4] показывают, что методика семантических замен эквивалентных операторов справедлива по формулам:

– для инструкций add и sub:

$$imm2 = (not\ imm1 + 1) \bmod 2^{size},$$

– для инструкций ror и rol:

$$imm2 = (size - imm1) \bmod size.$$

В обоих выражениях *imm*1 и *imm*2 – непосредственные значения для обратных инструкций, *size* – размер регистра, над которым производится операция [3]. Значения обратных инструкций важно синхронизировать с множеством *N* – количеством инструкций исполняемого кода. Множество справедливо по формуле:

$$N = (n_1 + n_2 + \ldots + n_\infty),$$

где *n* – количество определенных операторов. Если анализировать n как частицу самомодифицирующегося кода, в которой есть непосредственные значения для обратных инструкций *imm*1 и *imm*2, то ей подойдет выражение, связанное по формуле:

$$W = \frac{V * X}{t},$$

где *W* – неизменно коэффициент эффективности набранных решений самомодифицирующегося кода, а *V*, *X* – вектора скорости и координат частицы, *t* – номер итерации. Параметр *size* можно определить как *S* – величина количества вложенной информации в битах. Отсюда следует, что для того, чтобы учитывать количество вложенной информации, необходимо иметь экспоненциальную функцию, определенную через ряд Тейлора:

$$e^n = \sum_{n=1}^{\infty} \left(\frac{S^n}{n!}\right).$$

Имея показательную функцию, можно сформировать график зависимости (рис.) количества имеющихся различных типов операторов и величины *S*. Для этого следует представить приблизительную таблицу, рассмотренную в работе [3] и [4], в которой был рассчитан объём информации, который можно вложить в исполняемый код. Размер рассматриваемого исполняемого кода составлял 37 141 байт. Отношение объема вкладываемой информации справедливо по формуле:

$$Z = \frac{1}{S^n}.$$

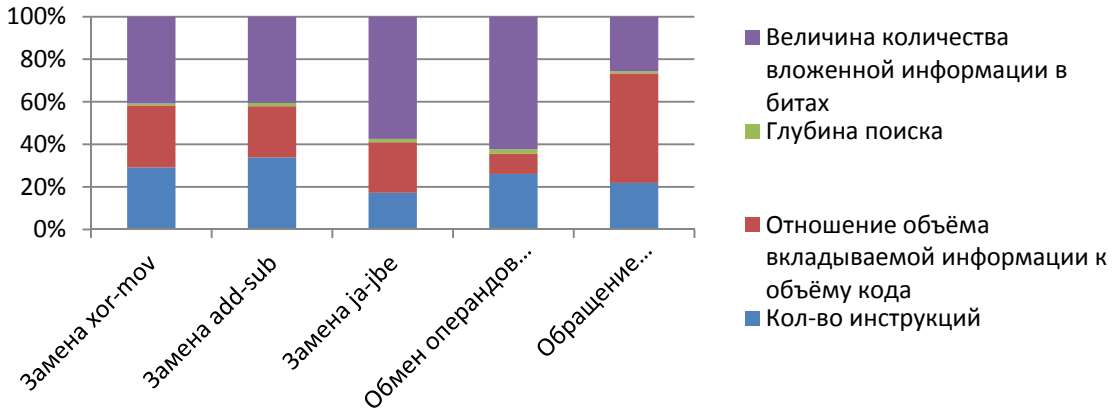
Соответственно, исследование в работах [3] и [5] показывает, что благодаря выявлению зависимости *Z* от *S* можно понимать, что под числом пересекающихся элементов понимается количество стеганографированных сообщений, размеры которых попали в оба интервала (т. е. для них невозможно однозначно определить – это двоичные инструкции программы или псевдослучайная последовательность) [6]. Для этого предварительно рассчитываются оценки вероятностей появления каждого символа в файле. В качестве символа мы будем брать один байт. Рассмотрим подробнее процесс получения оценок вероятностей. Пусть имеется алфавит $A = \{a_1, a_2 \ldots a_n.\}$, его мощность $|A| = N$, где $N = 256$. Введём множество счётчиков операторов кода $B = \{b_1, b_2 \ldots b_n.\}$. Каждый элемент этого

множества содержит число повторений соответствующего символа в исполняемом коде. Следовательно, искомые оценки вероятностей $C = \{c_1, c_2 \dots c_n.\}$ появления каждого символа в коде можно вычислить по формуле:

$$C = \frac{(A^n + B^n)}{t}, \quad (1)$$

где C – искомая вероятность стегопреобразования по отдельным частям исходного кода, исполняемого файлы в битах, A – количество алфавитных символов в битах, B – количество операнд кода в битах, t – время обработки информации в памяти процессора в секундах, а n – все тоже количество определенных операторов.

а)



б)

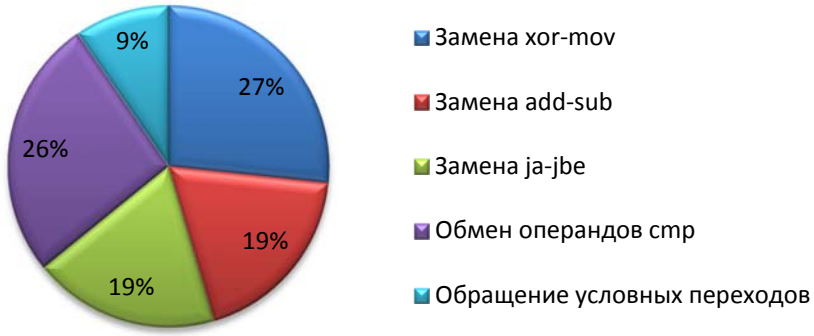


Рисунок. Корреляционный анализ: а) действий самомодифицирующегося кода для защиты информации в исполнимых файлах; б) количества инструкций в исполнимых файлах для стеговложения

Разумеется, что область проверки стеговложения исполнимого файла не ограничится одной части исполнимого кода, поэтому формула (1) актуальна в следующем квадратном уравнении:

$$S = \frac{C+\sqrt{(A^n+B^n)^n}}{2T}, \quad (2)$$

где S – та самая величина количества вложенной информации в битах, а T – глубина поиска стеганографированной информации в сек.

Благодаря формуле (2) возможно определить зависимость характеристик вложения на примере некоторых заранее известных данных о вложенной информации. Применив замену цепочек NOP, где в обработку ушел небольшой объем (например, до 64 бит, а это величина текста данного предложения), мы можем получить соответствующую статистику. Для этого сначала все данные представим в таблице, в которой будут применены эквивалентные замены различных операторов ассемблерного кода, которые можно наблюдать в исходных файлах исполняемых файлов. При этом возможно указывать любую случайную величину в пределах 64 бит и 5 секунд.

ТАБЛИЦА. Расчетные данные по величине количества вложенной информации в исполняемый файл

Тип вложения	Количество инструкций	Отношение объёма вкладываемой информации к объёму кода	Глубина поиска	Величина количества вложенной информации в битах
Замена xor-mov	64	64	2	89,6
Замена add-sub	45	32	2	53,9
Замена ja-jbe	45	62	4	149,8
Обмен операндов cmp	63	23	5	150,5
Обращение условных переходов	23	54	1	26,95

Как показано на этой таблице, что чем больше глубина поиска при стеговложении любой величина данных, тем больше информации можно вложить в данные использую простую замену цепочек NOP для разных операторов ассемблера, не влияя при этом на структуру данных используемого пространства и объема сегмента. Для того чтобы сделать обнаружение факта вложения информации в исполняемый код максимально трудным, требуется, чтобы статистика появления определённых инструкций в коде с вложением минимально отличалась от такой же

статистики в коде без вложений. Соответственно результатов данного исследования станет корреляционный анализ на графике (рис.), который также обладает качествами эвристического анализа обнаружения *n* – количества определенных операторов, что доказывает актуальность формулы (2).

Процентное соотношение по объёму вкладываемой информации к объёму исполнимого кода (рис. 1*а*), дает основание полагать, что при приблизительном количестве замен различных операторов *N* (рис. 1*б*), область проверки вложения информации на основе самомодифицирующегося кода достигается на 40 % от общей величины количества вложенной информации в битах в исполнимый файл при всех 100 %. Это означает, что общая глубина поиска скрытого вложения информации возможна в большинстве случаев лишь до 40 % от общей величины количества вложенной информации в битах.

Общее анализ показывает успех вложения при помощи самомодифицирующегося кода, не смотря на количество любых используемых параметров, а именно: количества операторов, глубины поиска стеганографированной информации, времени обработки информации в памяти и битов вложенной информации.

Список используемых источников

1. Штеренберг С. И. Методика применения в адаптивно системе локальных вычислительных сетей стеговложения в исполнимые файлы на основе самомодифицирующегося кода // Системы управления и информационные технологии. 2016. Т. 63. № 1. С. 51–54.

2. Штеренберг С. И., Виткова Л. А. Варианты вложения информации в исполнимый файл формата.Intel HEX при помощи языка Ассемблера // Инновации и инвестиции. 2015. № 7. С. 154–156.

3. Красов А. В., Верещагин А. С., Абатуров В. С., Методы скрытого вложения информации в исполняемые файлы // Известия Санкт-Петербургского государственного электротехнического университета ЛЭТИ. 2012. № 8. С. 51–55.

4. Shterenberg S. I., Krasov A. V., Ushakov I. A. Analysis of using equivalent instructions at the hidden embedding of information into the executable files // Journal of Theoretical and Applied Information Technology. 2015. Т. 80. № 1. PP. 28–34.

5. Красов А. В., Верещагин А. С. Анализ возможности скрытого вложения информации методом замены синонимов в исполняемый код процессоров семейства x86 // 63-я научно-техническая конференция профессорско-преподавательского состава, научных сотрудников и аспирантов: материалы / ГОУВПО СПбГУТ. – СПб., 2011.

6. Нечта И. В. Эффективный метод стегоанализа исполняемых файлов базирующийся на коде Хафменна // Вестик СибГУТИ. 2010. № 4. С. 47–54.

Статья представлена научным руководителем, кандидатом технических наук, доцентом В. И. Андриановым.

УДК 004.056

СИСТЕМНЫЙ ПОДХОД К ВНЕДРЕНИЮ И НАСТРОЙКЕ МЕЖСЕТЕВЫХ ЭКРАНОВ В ГОСУДАРСТВЕННЫХ ИНФОРМАЦИОННЫХ СИСТЕМАХ

А. Ю. Ярошенко

Национальный центр управления в кризисных ситуациях МЧС России

Приводятся организационные документы по использованию межсетевых экранов в государственных организациях, а также негативные примеры их настройки «по умолчанию». Доказывается необходимости системного подхода к внедрению и настройке межсетевых экранов в государственных информационных системах.

угрозы информационной безопасности, межсетевой экран, государственные информационные системы, внедрение и настройка, системный подход.

Применение межсетевых экранов (МСЭ) в государственных информационных системах (ГИС), включая информационные системы персональных данных, обуславливается как требованиями законодательства Российской Федерации, так и угрозами информационной безопасности, связанными с современной экспансией информационных технологий.

Нельзя забывать, что МСЭ в каждом определенном случае является частью, элементом системы обеспечения безопасности информации (СОБИ), в которой наряду с МСЭ есть и другие элементы, такие как антивирусные средства, подсистемы обнаружения вторжений, подсистемы мониторинга событий информационной безопасности, средства криптографической защиты информации и др. У СОБИ есть структура, состав, среда, в которой она функционирует, а значит МСЭ не может внедряться и настраиваться изолированно – он должен существовать в гармонии с окружающими его элементами, подсистемами, персоналом и в соответствии с организационными документами, в частности приказами ФСТЭК России [1, 2].

Организационные документы по использованию МСЭ от 1992 г. [4], равно как и вышедшие в 2016 г. [5], наряду с мерами от 2014 г. по защите конфиденциальной информации в ГИС [3], содержат в себе требование наличия тех или иных функций в МСЭ, а вышеупомянутые приказы ФСТЭК говорят о необходимости наличия МСЭ в ведомственных и государственных сетях, однако не содержат в себе четких инструкций по настройке МСЭ, требования наличия в листах доступа (*access-list*) необходимых, основополагающих правил. Как следствие, большинство государственных организаций, приобретая и устанавливая в своей сети

МСЭ с настройками «по умолчанию», считают свою миссию по обеспечению информационной безопасности (в этой части требований) выполненной.

В результате такой непрофессионально проделанной работы по установке МСЭ, часто в сети организации появляется еще одно сетевое устройство, выполняющее функции лишь маршрутизатора, то есть не используется по предназначению.

Например, межсетевой экран, основной функцией которого является фильтрование трафика, без дополнительных настроек пропускает через себя весь, в т. ч. нелегитимный трафик (рис. 1).

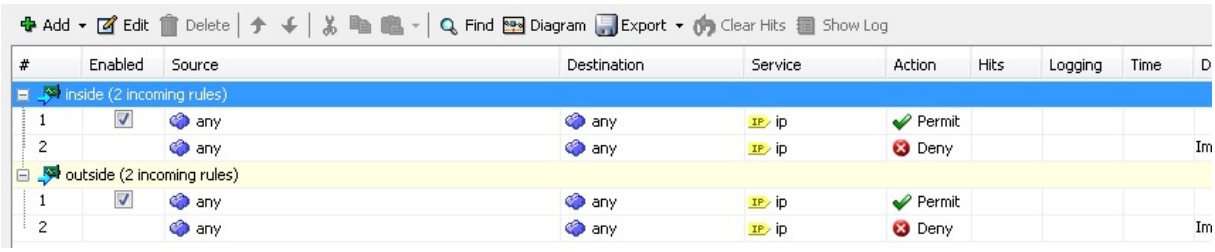


Рис. 1. Настройки МСЭ по умолчанию

Даже более-менее качественно настроенный МСЭ при возникновении каких-либо проблем с прохождением сетевого трафика «донастраивают», добавляя любимую всеми сетевыми администраторами, но избегаемую администраторами безопасности, строку «Permit ip any any», или «Разрешить все». Наличие на внутреннем сетевом интерфейсе в конце списка правил фильтрации строки «Permit ip any any», по сути, нейтрализует все запрещающие правила, находящиеся выше по списку, открывая безграничный сетевой доступ пользователям локальной сети. Наличие такого правила на внешнем интерфейсе обеспечивает не только злоумышленникам, но и случайным пользователям, находящимся за пределами организации, полный неконтролируемый доступ к ресурсам организации (рис. 2).

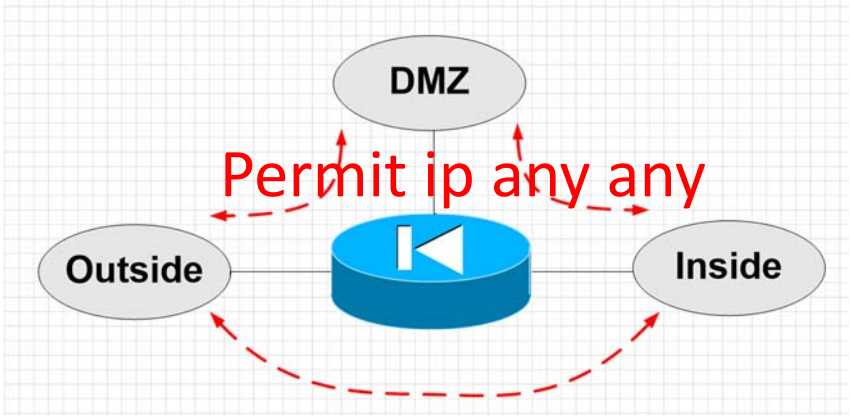


Рис. 2. Безграничный сетевой доступ на всех интерфейсах МСЭ

Агрессивная сетевая среда, современная практика и личный опыт администраторов безопасности диктуют необходимость системного подхода к настройке МСЭ, осуществление которой осложняется наличием обширного количества систем и устройств внутри сети, в демилитаризованной зоне и во внешней среде, от или к которым нужно предоставить доступ.

Тонкую настройку используемых повсеместно стандартных межсетевых экранов, не позволяющих «заглядывать» внутрь сетевого трафика и различать используемые протоколы, способных осуществлять фильтрацию лишь по IP-адресам и сетевым портам, невозможно было произвести в принципе. Так, например, настроив стандартный для http порт 80 для доступа к web-сайтам, открывались безграничные возможности для злоумышленников и продвинутых пользователей – ведь используя специальное программное обеспечение в восьмидесятый порт можно «завернуть» любой трафик, в т. ч. ftp, pop3, smtp, ssh, telnet, трафик торрент и тор-сетей, использовать анонимайзеры и т. д., не говоря уже про вирусы, трояны и другие вредоносные программы (рис. 3).

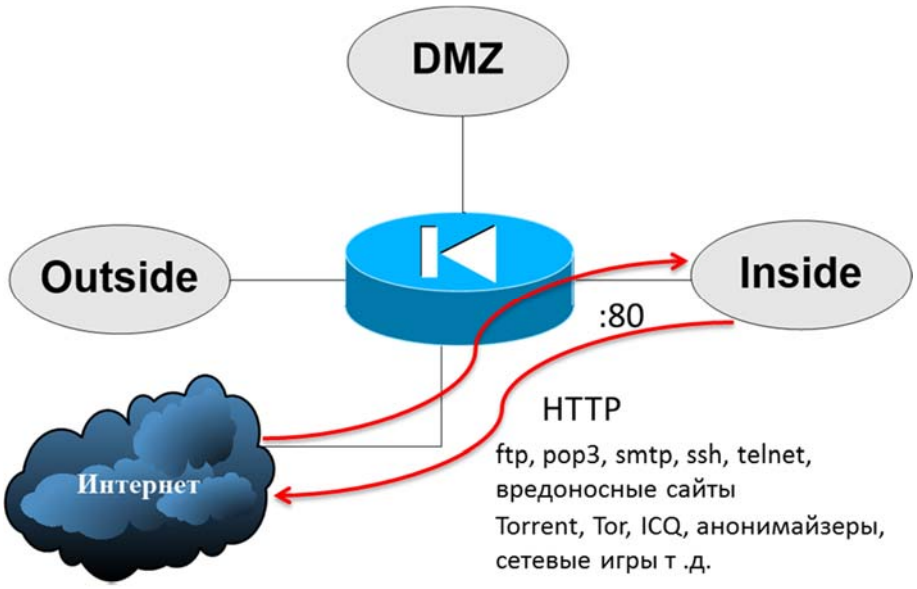


Рис. 3. Мнимая безопасность при ограничении открытых портов

В последние годы появились современные МСЭ, так называемые МСЭ следующего поколения (*Next Generation FireWall*, или NGFW), способные фильтровать трафик до седьмого уровня модели OSI. Для настройки NGWF не требуется больше переживать, что, открыв один порт, по сути, открывается входная дверь в или из ведомственной, или другой сети. В NGFW фильтрация трафика осуществляется по сетевым протоколам, по категориям сайтов, а также по тому или иному приложению web-ресурса. Например, открыв кадровым работникам необходимые для работы

социальные сети несколькими нажатиями кнопок компьютерной мыши можно запретить в них прослушивание музыки, просмотр видео, игры, переписку и т. д.

Приведенные примеры показывают, что в условиях стремительно развивающихся информационных технологий, а также лавинообразного развития хакерских технологий грамотное внедрение и настройка МСЭ при его взаимодействии с другими средствами защиты информации становится не только искусством администратора, но и наукой, что предполагает, как минимум, применение к рассмотренному процессу системного подхода.

Список используемых источников

1. Приказ ФСТЭК России от 11 февраля 2013 г. № 17 «Об утверждении требований о защите информации, не составляющей государственную тайну, содержащейся в государственных информационных системах».

2. Приказ ФСТЭК России от 18 февраля 2013 г. № 21 «Об утверждении состава и содержания организационных и технических мер по обеспечению безопасности персональных данных при их обработке в информационных системах персональных данных».

3. Методический документ «Меры защиты информации в государственных информационных системах», утвержден ФСТЭК России 11 февраля 2014 г.

4. Руководящий документ. Средства вычислительной техники. Межсетевые экраны. Защита от несанкционированного доступа к информации. Показатели защищенности от несанкционированного доступа к информации. Утверждено решением председателя Государственной технической комиссии при Президенте Российской Федерации от 25 июля 1997 г.

5. Выписка из приказа ФСТЭК России от 9 февраля 2016 г. № 9 «Об утверждении Требований в области технического регулирования к продукции, используемой в целях зашиты сведений, составляющих государственную тайну или относимых к охраняемой в соответствии с законодательством Российской Федерации иной информации ограниченного доступа (требований к межсетевым экранам)».

Статья представлена научным руководителем, доктором технических наук, профессором М. В. Буйневичем.

A N N O T A T I O N S

PLENARY MEETING

Koucheryavy A., Vybornova A. Tactile Internet. – PP. 6–11.
This article represents the history of the public telecommunication networks and opportunities of new networks creation on the basis of the Tactile Internet technologies. These networks are intended to provide tactile information transmission service. The article provides an analysis of the data transmission time delay requirements for such networks, that are also called ultra-low latency networks. Also the approaches for designing such networks are suggested in the context of ultra-dense heterogeneous network technologies introduction.
Key words: Tactile Internet, ultra-low latencies, ultra-dense networks, toroid network.

Leonov A., Nanii O., Treshchikov V. Trends of Development of Coherent Backbone Telecommunication Systems. – PP. 11–22.
The article overviews basic trends of development of modern telecom DWDM-systems: the transition to a more complex modulation formats, increasing the symbol rate, use of superchannels and flexible spectrum management (FlexGrid), the development of amplifiers systems and new types of optical fibers. It is shown that the existing technologies in theory enable achievement of the bandwidth 100 Tbit/s over a single fiber; a further increase in bandwidth requires involvement of new spectral ranges or spatial multiplexing using few-mode and multicore fibers.
Key words: DWDM, coherent systems, spectral efficiency, modulation format, symbol rate, FlexGrid, superchannel, few-mode fiber, multicore fiber.

Guilin W., Lu J., Borisov E. Two-Component Multi-Agent RoboticSystems Elements Interaction Model Scenarios. – PP. 22–31.
The article discusses the option of making a multi-agent robotic system able to function in different physical environments.
Key words: multi-agent systems, mobile robots, spherical robots, group interaction.

Ptitsyna L. Methodological Profiling Intellectualization of Information Infrastructures. – PP. 31–35.
A generalization of the directions of intellectualization of information infrastructures, systematized the purpose of each of the presented directions, formed the requirements for the methodology of intellectualization, proposed methodological concept of profiling intellectualization, highlighted typical situations methodological profiling, identified the key components of the methodological bases, considered particularly high-performance technologies, networking technologies, information technologies, security technologies, cognitive technologies, agent technologies, hypertehnologies, revealed formalization of the process of generating the key components of the methodological bases, described projects, the characteristics of projects.

Key words: network technologies, information technologies, security technologies, cognitive technologies, agent technologies, hypertehnologies, the generation of knowledge, overcoming uncertainty, achievements of goals, quality assurance.

Gromov I. The Information-Analytical System of Support of Decision-Making: Experience of Creation and Development Prospects. – PP. 35–45.

For effective management of the region state authorities should have operational statistics. Developing multidisciplinary tools for data collection. The proposed information-analytical system will provide a solution to the various problems in the industry, time and territorial aspect.

Key words: information-analytical system, public authorities, information collection, monitoring, analysis and forecasting of the complex.

Korzhik V. To 100th birthday of Information Theory Founder-Claude Shannon. – PP. 45–50.

The main biographic events of C. Shannon life are given. The main directions of his research activity and the most important scientific results are presented.

Key words: C. Shannon, biography, the main scientific results.

Forsgren H., Karvi T. Heuristics for Automatic Verification of Pairing-Based Cryptographic Protocols. – PP. 50–60.

We propose an automated method to aid the analysis of security protocols that use pair-ing-based cryptography. Our method is based on the constraint satisfiability problem. We start by presenting an algorithm to generate all the execution sequences and constraints, with or without an attacker. Then we define the normal forms of terms of various type and introduce a heuristic method to solve the constraints.

The same example protocol, Nalla's identity-based tripartite authenticated key agreement protocol, is used in all these phases to describe our method. Finally, we estimate our method against many other erroneous identity-based key agreement protocols and propose further developments.

Key words: nalla's identity-based, agreement protocol, algorithm.

RADIO TECHNOLOGY COMMUNICATION

Aogari F. S. A. Design of Microstrip Elliptic Band-Pass Filter with a Structure Composed of Two Lattices with the Same Electrical Length. – PP. 61–65.

This paper deals with the design of the structures consisting of two parallel-linked lattices of coupled multi-wire lines of equal length, which are among the most compact structures with transmission zeros at finite frequencies. During the research was used a transformation of capacitive matrix that allows to get geometric dimensions of the structure which are comfortable for the realization.

Key words: Elliptic Filter, Band-pass Filter, prototype, UHF-devices, lumped capacity, Shorted line, transformation of capacitive matrix, multiwire line.

Al-Ameri H., Steputin A. Analyzing Mechanisms of Load-Balancing in Heterogeneous Networks LTE – PP. 66–71.

The building of a heterogeneous network allows for the capacity network to be increased and improve its coverage area. However, the subscriber load in heterogeneous networks LTE is irregularly distributed across a network service area. The existing mechanisms of load-balancing that were described in the 3GPP specifications don't address these issues fully. This article outlines load balancing mechanisms in multiservice heterogeneous networks standard LTE.

Key words: LTE, heterogeneous networks, load balancing, CRE, eICIC, CoMB.

Al-Odhari A. H. Radiation Source Positioning in the High Mountains of Republic of Yemen using Unmanned Air Vehicle. – PP. 71–76.

In this paper we propose the use of unmanned air vehicles (UAVs) to improve the accuracy of emitters' positioning by the traditional time-difference method. The comparison of the estimates obtained for the case with mobile (UAVs) and fixed receivers was made. The option of their territorial distribution for the positioning accuracy improvement was offered.

Key words: positioning, TDOA, unmanned air vehicle (UAVs).

Ananev A., Prikota A. Automation of Approximation of Nonclassical Characteristic of Filter Devices. – PP. 76–80.

On an example of digital dispersing delay lines with the infinite impulse characteristic with Chebyshev approximation of group delay time the approach to resolution of problems of the automated synthesis, caused by complexity of search of vectors of initial approach and low stability of search of the optimal decision is offered.

Key words: nonclassical approximation, designing automation, dispersing delay lines, infinite-impulse response.

Angeluts A., Odoevskiy S. Analysis Methods of Image Processing for Automatic Target Detection. – PP. 80–84.

In this study, some image processing techniques applied to the task of automatic target detection are reviewed and analyzed. As follows from the carried analysis, a technique was chosen. It is supposed to be the basis for the further studies aimed on development of methods of image processing for automatic target detection on water surface.

Key words: videodata, moving camera, processing techniques, filtration, detection, optical flow method, Kalman filtering.

Andreev R., Bobrova E., Kachnov A. Deploying DAS System in the TRK "LETO". – PP. 85–88.

Examined the mail points of construction of the DAS system TRK "LETO". Presents the technical solution to implement the coverage on the basis of DAS systems.

Key words: DAS, indoor coverage.

Andreev R., Galchin R., Kachnov A. Implementation of the Main Operators in the DAS System TRK "LETO". – PP. 88–91.
Examined the key points of the introduction of more operators in the existing DAS system TRK "LETO". Presents the solution of the problem.
Key words: DAS, power balance, indoor coverage.

Andreev R., Kachnov A., Morozova T. On the Determination of the Azimuth Antenna Base Station. – PP. 91–95.
Review variants determine the azimuth of antenna base stations in real conditions of operation using different methods. Proposed methodology for assessing the accuracy of different azimuth antenna.
Key words: azimuth antenna, antenna, geolocation.

Antipin B., Vinogradov E. Analysis of Radiomonitoring Equipment Requirements to Monitor Radio Spectrum for Electromagnetic Compatibility Estimation. – PP. 95–100.
Radiomonitoring equipment performance requirements set in unified technical policy regulations for radio service departments and their effects on quality of electromagnetic compatibility estimation are analyzed. It is shown that the measuring equipment meeting the requirements enables to get qualitative information about electromagnetic environment but requirements to phase noise of the local oscillator may be made harder because powerful radio frequency interfering signals can substantially reduce quality of the wanted signal due to the reciprocal mixing effect.
Key words: radiomonitoring, electromagnetic compatibility, radio frequency spectrum, radiomonitoring equipment performance, unified technical policy.

Akhmedov B., Koryakovtsev A., Smirnov V. Assessment of the Main Errors of the Tracking Measurements of Radar Complexes of Investigation and Firing Control. – PP. 100–104.
Currently, due to the improvement of artillery systems and increasing the efficiency of conventional and special ammunition actual is the fight against the enemy artillery. Efficiency of this struggle to a large extent depends on the multi-purpose radar reconnaissance complexes and firing control, which determine coordinates of firing positions of the opponent by notches of shells and mines on the trajectory, and adjust artillery fire. This article describes the main error sources of the tracking measurements of radar complexes of investigation and firing control reveals the most significant of them, which must be considered when assessing the effectiveness of the complex.
Key words: radar complex intelligence, phased array antenna, tracking measurements, errors.

Babkov V., Starikov V. LTE Planning. – PP. 105–108.
This article contains methods of planning initial approximation LTE network and choice of cluster structure.
Key words: LTE RF Planning, cluster 4G, LTE Radio Link Budget.

Bashmakov P., Kapralov D., Kirik D. The Formation of Signal-Code Constructions for DVB-T2. – PP. 108–112.
We discuss the noise immunity in the multipath channel for transmittion signals of digital television DNV-T2. Approach to the solution of a problem of optimization of formation of signal-code construction design is offered.
Key words: DVB-T2 standard, digital television, signal-code construction.

Bogolepov G., Miheev A. The Principle of Formation of Radio-Based Software and Managed Module Formation with the Use of Cross-Channel Quadrature Relations. – PP. 112–115.
Recently became topical use of satellite communication systems for the transmission of information in remote areas where GSM network and the segment is underdeveloped or not developed at all. There is a problem of electromagnetic compatibility with operating in the adjacent frequency bands, as shown in Fig. Proposed to use a universal method of generating a radio signal based on the quadrature generator with the use of spectral efficient digital modulation.
Key words: radio frequency resource, complex envelope, elementary impulse.

Borisov E., Golod O., Egorov S. A Performance Analysis of Multipath Direction-Finder. – PP. 115–119.
This paper provides method for estimating the direction-of-arrival and relative coordinates of a boat using series of consequent angle and doppler frequency measurements. Performance of the proposed method is evaluated through computer simulation.
Key words: monostatic radar system, distance measurements, measuring coordinates, direction-of-arrival estimation, doppler frequency, radio direction-finding, accuracy of DOA estimation.

Borisov E., Mashkov G., Fokin G. Experimental Validation of Multipoint Joint Processing of Range Measurements via Software-Defined Radio Testbed. – PP. 120–125.
In this paper we present an algorithm for multipoint joint processing of range measurements with trial results accumulation. The approach for experimental validation is a software-defined radio (SDR) transceiver working on National Instruments (NI) Universal Software Radio Peripheral (USRP) hardware with LabVIEW software, performing transmission, reception and processing of signals. Presented solution was validated in static scenario and achieved position errors of several meters depending on the number of range measurement trials. The resulting error was affected by synchronization uncertainty due to network organization of transceiver stations and measurement processing unit.
Key words: Multipoint Joint Processing, Range Measurements, Software Defined Radio, Testded, Mean Square Error, Field Trials, USRP, LabVIEW.

Borisov E., Poddubny S. The Application of Time – Space Radiated Signals to Determine the Coordinates of Targets in Bistatic Radar System. – PP. 125–132.
The article considers the variant of the spatial – temporal signal processing in bistatic radar system, allowing to implement additional angular coordinate measurement and increase the accuracy of determining the location of objects.
Key words: bistatic radar system, space-time signal, azimuth information, total-delemere-azimuth, triangulation, positioning accuracy.

Vinogradov P. Prospects of use of Lithium Accumulators in Power Supply for Telecommunication. – PP. 132–135.

Increase of reliability of communication systems leads to more strict requirements imposed to power supply. The solution of this task is possible by using of various power sources as units of the uninterrupted and guaranteed power supply. Expansion of a zone of operation of telecommunication devices towards Far North results in need to apply the equipment with more wide range of temperatures. These answer conditions the developed rechargeable batteries on the basis of lithium. Lithium batteries are answered on these conditions.

Key words: power supply, uninterruptible power unit, the lithium battery.

Glazkov R. Application of Advanced Modulation Techniques in the Modern Mobile Communication Systems. – PP. 135–140.

The development of multimedia technologies, the introduction of new services and increase of the transmitted data volume requires increasing the efficiency of existing advanced mobile networks. At the moment, the emergence of new standards (5G) and the continuous improvement of the wireless transmission technology has led to an exponential increase in the frequency and the hardware and software resources needed by subscribers. However these resources are limited, and their useage requires significant funding.

Therefore, the optimization of the mobile communication system of the fifth generation on the physical layer is an urgent task at the moment. Research aimed to the implementation of new advanced modulation techniques allow to change the characteristics of the transmitted radio signal, and achieve significant savings of network resources. This, in turn, could increase the efficiency of the network as a whole. In this paper, the possibility of using such modulation techniques like FBMC, as well as other technologies that use digital N-OFDM like modulation method for 5G Networks are considered.

Key words: Modulation, multicarrier, N-OFDM, FBMC, UFMC, 5G.

Gogol A., Tumanova E. Parameters of the Images Quality Assessment of High-Definition and Three-Dimensional Images of Virtual and Augmented Reality. – PP. 140–143.

In this paper basic parameters of the images quality assessment of virtual and augmented reality are considered. The analysis an influence on reality perception of virtual three-dimensional space such parameters as: image depth, resolution, refresh rate of 4K, 8K formats and three-dimensional images is carried out.

Keywords: quality assessment, high-definition, three-dimensional image, augmented and virtual reality.

Deshina N., Kubalova A., Ryzhikova T. Strip Design Methods of Structures with Attenuation Poles in the end Frequencies. – PP. 143–149.

The basic types of structures with attenuation poles. Are: Strip structure with invertiruûŝimi lines lines and parallel loops; stripline structure consisting of parallel connection of two lattices associated multi-lane lines of equal length; Strip structure, consisting of two parallel connection short-circuit arrays connected multi-lane lines; Strip structure, consisting of two parallel connection open arrays connected lines; Strip structure on polusosredatočennyh items.

Key words: strip structure, mnogoprovodnaâ line, short circuit, polusosredatočennye elements, power inverters in parallel lines, grids, pole of attenuation, open the grille.

Deshina N., Kubalova A., Ryzhikova T. Designing Antennas and Microwave Structures Using HFSS Program. – PP. 149–155.

HFSS program is designed for three-dimensional design of microwave devices and uses several methods of calculation. A number of filters and advanced antennas with linear and circular polarization, analyzed using HFSS. Given the methods of calculation and installation of HFSS software options in the course of building three-dimensional models of waveguide and antenna structures. We consider the optimization of microwave structures, greatly enhances the design speed.

Key words: HFSS software, microwave devices, filters, antennas, linear and circular polarization, the three-dimensional model of the waveguide structure.

Dmitriev P. Using Heart Rate Data for Control of Trainee State. – PP. 155–158.

This paper analyzes possible solutions of human reliability problems and presents an approach to solving the aim of determining psychophysiological state based on heart rate variability (HRV). As a main tool LF/HF ratio was chosen. It can be calculated by spectral analysis of RR-intervals in real time mode.

The possibility is considered and justified of applicability proposed approach for simulators and training complexes. An example of this approach is a simulator coupled with personal respiratory protective equipment (RPE) for training to work properly.

This article contains some results of experimental studies. This material may be considered as a reserve for further researches.

Key words: trainee, heart rate variability, heart rate, simulator system, training complex

Ivanov A., Kovaleva T., Ryzhikova T. Results of Modeling and Experimental Studies of Electrophysical Properties of High q-Factor Composites. – PP. 159–163.

The paper presents the results of simulation and experimental studies of radio transparent properties of high-q composites designed for antenna radomes and shelters operating in a given frequency range.

Key words: polymer matrix, disperse filler, fiberglass.

Ivanova M. Search Video by User Request. – PP. 163–167.

Need to find a video section in the files or databases has led to the development of image search systems. These systems use different methods. Of greatest interest are the object-oriented search methods, since they are based on the recognition of objects in the image. However, the main problem is the "semantic gap". There are ways of significantly reducing the gap. However, now, there is no method that would be completely solved the problem of the "semantic gap".

Key words: search methods, semantic gap, low-level feature, semantic features, object-oriented search method.

Kamaldinova J., Likontsev A. Prospects of Use of Ka-band Satellite Broadband in the Republic of Kazakhstan. – PP. 167–173.
The problem of research of Ka-band satellite for broadband access and the creation of satellite communication and broadcasting "KazSat-4" (hereinafter KazSat-4). And foreigners are the main tests, the rationale and the ways of solution.
Keywords:Ka-band, broadband, satellite communications.

Kasabaeva D., Stepanov A. Comparison of LABVIEW and SIMULINK in Digital Signal Processing Systems Simulation. – PP. 173–177.
The article is dedicated to LabVIEW and the Simulink, as a part of the MATLAB system in the simulation of digital signal processing systems. The article describes the pecuarities of working with these packages, their advantages and disadvantages. A digital filter is considered as an example of simulation . The article presents the Simulink-model of digital filtering system and its block diagram, constructed in LabVIEW.
Key words: MATLAB, LabVIEW, Simulink, Simulink-model digital filter.

Kachnov A., Penkin V., Rybakov A. The Development of Mobile Information Provision Systems Using Meteor Communication Channels. – PP. 177–181.
The problem of creating a mobile communication system using the communication channels of the meteor, which is part of an integrated system of information support of safety of navigation of the Northern sea route. Considered variant of implementation of mobile (wearable) system. The results of approbation of technical solutions.
Key words: Meteor radio communication, shortwave radio, telecommunications, data transmission system.

Kirik D., Malyshev A. Model of a Data Transmission Channel in Systems of Mobile Medicine. – PP. 181–185.
We discuss standardization problems in systems of mobile medicine. We provided the most significant and used standards.
Key words: ZigBee, protocol, mobile medicine, telemedicine.

Kudriashov N., Mihalev O., Petrenko M. Development of the Perspective Radio Transmitters HF Range Military Destination. – PP. 185–190.
Currently in Russia most of transmitting short-wave communication devices has several disadvantages: low efficiency, constructed on the old element base, are not able to broadcast in digital formats. Construction of a radio transmitter according to the method Canna able to broadcast in analog modulation types, and digital radio standard DRM using Class D amplifier and modern domestic element base will improve the transmitter efficiency, the quality of the programs and to expand coverage area.
Key words: amplifier, Digital Radio Mondiale, efficiency, modulation.

Lavrukhin V., Lezhepekov A. Study Standard Mechanisms Measuring WiFi Stations to Select the Access Point for Connect-Ing. – PP. 190–194.
WiFi network selection of the subscriber station to the network to connect to, or point to a stupa inside of the network is not regulated by the IEEE 802.11 standard. Therefore, the decision

as to which network to connect to, falls on the shoulders of the end user La Wi-Fi devices, i. e. subscriber. Although each manufacturer of devices with built-in Wi-Fi may help the user to choose a network based on any of the available subscriber station measurements, most companies offer users a modest set of criteria for network selection. First, is the level of the Signa-La, estimated graphically by the number of "bars" on the WiFi icon. Secondly, it is the name of the network. And, thirdly, it is a flag that indicates the network or not. All of these options do not allow the user to effectively select a network in the modern world.
In this work experimentally proved the inefficiency of the existing automatic methods.
Key words: WiFi station, access point, frame, measurement.

Likontsev A., Likontsev D., Shakhobiddinov A. About the Results of Numerical Modeling of Radio Extender Antenna. – PP. 194–197.

The report presents the results of numerical modeling of directional characteristics and matching of four-element "Yagi" antenna. The simulation results of the antenna array from the two antennas in E and H planes stacks are shown. Such an antenna can be used as a radio extender of mobile communication in places with poor reception of signals.
Key words: radio extender, antenna, mobile communication, poor reception.

Makarov L., Protasenya S. The Iterative Model of the Action of Biophysical Factors. – PP. 198–202.

Considered the issues of system modeling events in vivo with consideration of circadian rhythms, cell mitosis, neural activity of sensory systems and biochemical factors responsible for the formation of the forecast of development of the processes of life.
Key words: computer simulation, dissipative system.

Malikova J., Stepanov A. Graphical Interface of Wavelet Image Processing for Users of Kazakhstan. – PP. 203–206.

The article describes the proposed GUI wavelet image processing, designed for users of Kazakhstan. The article presents the stages of interface development, a detailed description of its elements, the advantages in comparison with expansion pack Wavelet Toolbox built-in MATLAB system. The article ends up demonstrating the processing results of one of the test images.
Key words: Wavelet, image, graphic interface, MATLAB.

Odoevskiy S., Pokrovskaya V. Priority Tasks of Processing and Transfer Radar Information. – PP. 206–209.

The paper is dedicate to the problems of radar data processing. The description of the basic algorithm path detection (Kalman filter) is described. The main problems in the processing of information received from radar are described. For further consideration proposed a method for predicting the trajectory of the object based on the method of physical regularization and the Green's function.
Key words: radar information processing, tertiary information processing, Kalman filter, method of physical regularization, the Green's function.

Sungatullin E., Ustimenko V. Broadband Jammer Signal Forming – PP. 210–213.
Broadband Jammer Signals in downlink (from base station to mobile station) channels are used to secure from information leakage in networks of wireless mobile systems. The article describes digital jammer signal forming using voltage controlled oscillators (VCO) as more optimal method than analog jammer signal forming schemes. Experimentally formed jammer signal proves that the modeled signal forming scheme is correct.
Key words: jammer, mobile systems, frequency modulated jammer signal, band-limited white noise, digital-to-analog converter, 3G, VCO, pseudorandom sequence.

Fedorov S. DVB-S2X – Extensions to the Standard DVB-S2. – PP. 214–217.
Standard DVB-S2x (ETSI EN 302 307 part 2) is an extension of the standard DVB-S2 (ETSI EN 302 307 part 1) and provides additional technologies and features that provide increased efficiency for use in DTH (Direct to Home – DTH), the propagation digital TV programs via the main lines of communication, VSAT and DSNG applications. The standard also affects the market for mobile applications.
Key words: DVB-S2, DVB-S2x, bandwidth satellite links, digital TV.

Shuvalov D. Integral Assessing of Acoustic Quality of Sound Signals. – PP. 217–221.
Currently, researchers have proposed a variety of subjective criteria for assessing the contribution of room acoustics in the quality of audio signal, the corresponding objective parameters, on the basis of which assessment is calculated. In this paper, the basic criteria and parameters were examined and their systematization was carried out.
Key words: reverberation time, assessment criterion, sound pressure, speech intelligibility.

INFORMATION AND COMMUNICATION NETWORKS AND SYSTEMS

Avramenko M., Goikhman V. M2M Solution for Environmental Monitoring. – PP. 222–226.
Technologies of Internet of Things, such as "Machine to Machine, are already used to improve the state of the environment, for example: to recycle oil, CO2 emissions reduction, to control of noise pollution and cleaning of drains . That's why the development of M2M solution for environmental monitoring is an essential task.
Key words: m2m, internet of things, mqtt, http, traffic.

Andrianov V., Vitkova L., Saharov D. Research of Algorithm Protection Public Personal Data in Information Systems. – PP. 227–231.
The report explores the protection algorithm publicly available data, based on the introduction of self-modifying code in graphic images and files. Analyzes the existing solutions and methods that are applied in the context of monitoring, retrieval and protection of graphic images

and files in information systems. The use of publicly accessible personal data leads to new formulations of problems in the field of design of integrated systems for the protection of public personal data in information systems.
Keywords: public personal information, information systems, graphics, photography, self-modifying code, monitoring, steganography.

Arkhipov V., Yakovlev V. Simulation of Resistant Graphical Password Attack on the Basis of use Reed-Solomon Codes and Research of its Characteristics. – PP. 232–235.
New approach to creation of the table of comparison between password symbol and a subset of input symbols for password systems on the basis of a Reed–Solomon code tolerant to video-recording attacks. Estimates of resistance of system of password protection to different types of attacks are received.
Key words: authentication, password protection, graphical password, video-recording attacks, Graphical password, tolerant to video-recording attacks, shoulder-surfing attacks.

Birikh E., Sakharov D. Model Intruder Distributed Information Network. – PP. 235–238.
Intruder model - (in computer science), abstract (formalized or non-formalized) description of the intruder access control rules. The model identifies the intruder: the category (type) of offenders, which may affect the object; objectives that may be pursued offenders in each category, possible quantitative composition, used tools, accessories, equipment, weapons, etc.; Typical scenarios of possible actions of offenders, describing the sequence (algorithm) action groups and individual perpetrators, their methods of action at each step.
Key words: protection of information, the model, the offender, network operation.

Bogolepov G., Odnolko O., Ponomarev K. Viterbi Decoding Algorithm and Convolutional Codes Feasibility Estimation for Modern Communication System Problems. – PP. 238–241.
Error-correction coding applies to reduce energy costs in cellular and satellite communication systems. Convolutional coding uses in data communication systems. Convolutional coders are used in the GSM standard. There are several algorithms, which can decode convolutional codes. One of them is the Viterbi algorithm.
Key words: error-correction coding, convolutional codes, turbo codes, Viterbi algorithm.

Boltov Y. Build the Field of Special Points in Images Based on the Equation. – PP. 242–247.
The image processing based on its presentation as scalar fields, generated by Helmholtz equation, is described in this article.
The fields of special points that retained the value of chromatic level difference are built.
These fields are compared with fields built early through Laplacian
Keywords: field, special points, the Helmholtz equations, digital image, the green's function.

Borodko A. Modernization of ONVIF Protocol for use in the Large Video Surveillance System. – PP. 247–251.
The weak ability to filter video sources in ONVIF is considered a scalability limitation for large video surveillance systems. Offered a new ONVIF compliant service for the construction of large video surveillance systems with several thousands of sources.
Key words: metadata, video surveillance system, Safe City, ONVIF.

Buzykov L., Ermakova T. Analysis of Hemodynamic Signal for Obtaining and Using its Fractal Properties. – PP. 252–256.

Nowadays, self-similarity and fractality of human body is not in doubt. It allows to suggest that fractality properties can be used in medical area. Researches of hemodynamic signals for the presence of the fractal properties and investigation of possibility of developing mathematic methods for such analysis are performed in this article. Based on selected math methods of analysis a software for processing signal with consideration of its fractal properties has been developed.

Key words: self-similarity, analysis of hemodynamic, patient monitor, fractal.

Buinevich M., Izrailov K., Mostovich D. A Comparative Analysis of Approaches to Finding Vulnerabilities in Software Code. – PP. 256–260.

This article describes and analyzes the existing approaches for vulnerability search in a software code. There are considered such approaches as "black", "white" and "grey boxes", fuzzing, and test cases, manual and automatic, as well as static and dynamic approaches. Selection criteria and comparison of approaches are produced on the example of the algorithmization method of a machine code.

Key words: information safety, vulnerability search, algorithmization method.

Bylina M., Chaimardanov P. Virtual Laboratory Setup for Research of Single-Stage EDFA. – PP. 260–265.

This paper presents a virtual laboratory setup for research of single-stage EDFA based on silica fiber doped with erbium ions, designed for laboratory work in the disciplines of the department "Photonics and communication lines". The setup is designed using the generalized mathematical model of a single-stage EDFA optical amplifier with multi-channel signal sources and pumping. Setup allows studying the processes of propagation of pumps and signals on the activated fiber, signal amplification, the depletion of pump, and formation of forward and backward spontaneous emission noise. The simulation results are presented in the form of charts, which can be saved for further analysis and processing. The setup provides multivariate objects of research because it allows forming the amplifiers on the basis of several types of erbium-doped fiber leading manufacturers and setting various lengths of these fibers. The setup will be implemented in the educational process of the department "Photonics and communication lines".

Key words: EDFA, Erbium Doped Fiber Amplifier, optical amplifier, fiber, doped with erbium ions, virtual laboratory setup, multichannel signal, multichannel pump, forward pump, backward pump, amplified spontaneous emission, gain coefficient.

Bylina M., Chaimardanov P. Mathematical Model of a Single-Stage EDFA Amplifier with Multi-Channel Sources of Signal and Pump. – PP. 265–270.

The paper presents a mathematical model of a single-stage optical amplifier based on silica fiber doped with active particles - ions erbium Er3+. The model consists of kinetic equations that allow calculating the population of the energy levels of the active particles and the propagation equations describing the change in signal power of pump and amplified spontaneous emission noise along the activated fibers. A special feature of this model is the possibility of calculating the optical amplifier that uses multiple sources forward and backward pumping and designed to amplify the multi-channel signal. The main calculation results of the amplifier

are output power, gain and signal-to-noise ratio for each channel, forward and backward amplified spontaneous emission noise. The validity of the model is confirmed by comparing the calculation results with the results obtained by other researchers.
Key words: EDFA, optical amplifier, fiber, doped with erbium ions, mathematical model, multichannel signal, multichannel pump, forward pump, backward pump, amplified spontaneous emission, gain coefficient.

Vitkova L., Ryabova O., Sakharov D. Problem Questions of Creation and Usage of Open Data Sets of State Authorities. – PP. 271–276.
Open data is part of the global policy concepts of Public openness and Public policy innovation. However, when creating and using open data sets poses a number of challenges. The article describes the concept and framework of open data, the existing problems of their creation and distribution possible solutions.
Key words: open data, open standard, public data, open government, open sources, public data monitoring.

Vladimirov S. About the Majority-Logic Decoding of Shortened Maximum Length Code with K Linear-Independent Elements. – PP. 276–281.
In clause the majority-logic decoding algorithm of shortened maximum length code with k linear-independent elements is considered. The method of shortening for maximum length code and variants of optimal shortened codes in accordance with maximum code distance are added in. Method of error-detection decoding for shortened code combination with this algorithm is introduced.
Key words: maximum length code, majority-logic decoding, error correcting coding, probabilistic characteristics, error detection.

Vlasov D. Construction Issues of Information Security System for Typical Object of Russian Emercom. – PP. 281–285.
The article reveals the content of the main construction issues of information security system for typical object of Russian Emercom. Firstly, it analyzes the current state of information security at the facilities of Russian Emercom. Secondly, it shows the synthesis of a complex of counteraction means of information security threats for typical object of Russian Emercom. Thirdly, it creates information security policy for object of Russian Emercom at regional level. And fourthly, the effectiveness of the information security system for typical object of Russian Emercom is estimated.
Key words: information security threats, typical object of Russian Emercom, information security policy, effectiveness assessment of information security system.

Volshchukov M., Ivanov A. Ergonomics Information Exchange as a Factor in Accelerating the Design of Information Systems. – PP. 285–288.
This period caused significant influence of ergonomics in the design of information systems. More and more attention is paid to the criticality of information exchange between the technical and human systems in modern conditions, as well as the impact of engineering and psychological aspects of the change to the design of information systems. Using the methods of addressing ergonomics information exchange when designing information systems enhance the quality

of the training requirements in the formalization of the domain, which in turn will reduce the number of iterations, and thus the time to develop the system.
Key words: ergonomics, engineering psychology, subject area, information systems.

Voronkov K., Mendelson M. Digitalization Analog Systems Power Line Communication – PP. 289–293.

We study the problem of digitalization of analog systems for power line communication with the help of equipment K-LEP, representing three interconnected and at the same time functionally mutually independent unit - the multiplexer, modem and high-frequency unit. It is shown that these approach solves the problem of digitization HF communication systems in a short time and get a significant effect due to the minimal amount of capital expenditures and installation works. This delivers more bandwidth and more flexibility to use different download options for interacting high-frequency communication systems.
Key words: HF communications over power lines, adaptive high-speed modem, a flexible multiplexer, high-frequency unit.

Gamil A. The Method of Time Characteristics Estimation Networks Based on IMS Subsystem with the Message Retransmission Mechanism. – PP. 294–299.

In this paper we propose a SIP-session model with the message retransmission mechanism in network based on IMS subsystem over the transmission protocol UDP. Offered formulas for estimating the delay time of signaling messages involved in the process of establishing a session, taking into account their retransmissions of IP-based network for various kinds of faults and failures.
Key words: IMS, SIP, message retransmission, the quality of service.

Gerasimova I., Paramonov A. Analysis of Traffic and Quality of Service in Wireless Self-Organizing Networks. – PP. 299–303.

The article is dedicated to analysis of wireless self-organizing networks (SON) technologies, traffic characteristics and requirements to QoS in SON. The materials cited in this article are the results of researches in IoT development field and in characteristics, created by IoT traffic.
Key words: self-organizing networks, SON, machine-to-machine traffic, M2M, quality of-service, QoS, supervisory control and data acquisition, SCADA.

Gerling E., Kulishkina E. Security Measures of Communication Object. – PP. 303–308.

This report examines the security measures of the communication object. Vulnerabilities of the object are analyzed and universal methods for information and object security are offered. To ensure the security of the object it's proposed to use access control systems, security alarms, video surveillance, management security systems and devices , external protected communication channels, Access management and identification, the instruction for staff.
Key words: access management and identification, the object security.

Glagolev S., Dubov A., Rudnitsky V., Sumkin V., Hrichkov V. Reflectometry of the Subscriber Network PON. – PP. 308–312.

Feature PON subscriber area – is the presence of large numbers of compounds at low fiber length. Industrial OTDRs for testing this path are at the limit of their capabilities, in addition,

the cost and time of measurement unacceptably large. The use of semiconductor lasers for generating red light probing signals improves the basic parameters of the reflectometer while substantially reducing its cost. Additional benefits can be obtained by using the method of integral reflectometry.
Key words: reflectometer, PON, fiber, red light source, Avalanche Photodiode, APD.

Glagolev S., Kolotovkina G., Hrapova E. Indicators Reliability of Fiber – Optic Communication Lines and Methods of Assessment. –PP. 312–315.
Fiber – optic lines are widely used in telecommunication networks of different levels – from intercontinental routes to corporate and home computer networks. One of the main topics that should be considered when designing any fiber-optic highway connection – fiber-optic reliability metrics and evaluation methods depending on optical communication lines construction technology (groundwater , air and underwater) .
Key words: optical fiber, reliability indices, reliability assessment, construction technology, wavelength division multiplexing technology.

Glagolev S., Kolotovkina G., Hrapova E. Optical Multiplexers for WDM Technology. – PP. 315–320.
There are currently actively developing WDM technology (Wavelength Division Multiplexing), which allows to increase the network bandwidth efficiently and quickly. The main WDM system device that unite several wavelength into a single aggregate stream at the transmitting side, a multiplexer. At the receiving side a demultiplexer performs the inverse operation. This device has the property of reversibility, which allows us to consider only the demultiplexing technology.
Key words: Wavelength Division Multiplexing, demultiplexers, technology AWG.

Godlevskiy A., Korzhik V. Stegosystem with Improved Security for Embedding of Information Into Digital Motionless Images. – PP. 320–323.
Stegosystem with an opportunity to control the amount of pixel luminance changes is considered. To solve this problem are used Hamming codes with variable parameters. The computer program with friendly interface is presented. It is shown that this program works correctly. Open problems are presented.
Key words: stegosystem, Hamming codes, matrix embedding.

Goikhman V., Dremina A. Statistical Analysis of Traffic when Uploading Photos to Social Network. – PP. 324–329.
The article is devoted to statistical analysis of traffic when uploading photos to social networks. The studies were conducted for the three most popular networks available for personal computer: vk.com, facebook.com, twitter.com. The image is loaded on a predetermined schedule, using different browsers. In the analysis of the dependence of the magnitude of image compression from one type of browser based on download speeds of the time of day, the resulting ratio of the volume of incoming and outgoing traffic.
Keywords: Wireshark, Chrome, Firefox, Opera, IExplorer, vk.com, facebook.com, twitter.com social network, traffic analysis.

Goikhman V., Savelieva A. Protocols of the Internet of Things – PP. 329–334.
This article discusses the protocols of the Internet of things, overview protocols peculiar properties, possible applications, further it is classified. Contains an analysis and justify the protocol choice depends on the specifics of the planned Internet of things network. Actuality of the subject is due to the variety of existing protocols, Internet of Things standards and the lack of established terminology, describes the concept as a whole.
Keywords: internet of things, IoT, IoT protocols, M2M, XMPP, SOAP, COAP, STOMP, MQTT, DDS.

Goncharova D., Ulyanov A. Analysis of data Transmission Protocols in core Networks. – PP. 335–338.
This article deals with protocols of packet traffic transmission in optical transport networks OTN/xWDM. Presents analysis of channel layer protocol functions, based on GFP and Ethernet headers. Explains superfluity of protocols in encapsulation of packet traffic in OTN. It proposed using of GFP protocol as base protocol of channel layer of core networks with necessity of extension its functions by adding new header fields. It designs bandwidth backbones win by eliminating ethernet protocol in OTN networks based on statistical data of the structure of traffic and the experiment associated with the definition of a medium-sized packages of different types of traffic.
Key words: optical transport networks, OTN, generic framing procedure, GFP, ethernet, switching, superfluity of protocols.

Dikaneva K., Nebaeva K. Data Embedding Schemes for Video. – PP. 339–343.
Two data embedding schemes for video called MIDCAP and MIDVIS were shown in this article. The data is embedded during the process of MPEG-4 compression. The middle frequency components of the DCT blocks are used for embeddingin purposed schemes. There were shown several problems which can appear during the embedding, and their remedial measures.
Key words: MPEG-4, DCT, data embedding, video.

Dinh D., Kirichek R. Research on the Installation of Wireless Sensor Nodes with Different types of Unmanned Aerial Vehicles. – PP. 344–348.
In recent years, a new class of networks – flying sensor networks has appeared in the studies of ubiquitous sensor networks. The unmanned aerial vehicles (UAVs) are used as the flying units, which collect data from remote sensor nodes. A key challenge is the installation of sensor nodes in a large area, which can be solved using the UAV. In this paper, we considered different approaches of the installation of sensor nodes by UAV based on different criteria. In particular, we analyzed different types of UAVs and their capabilities (travel time, speed, payload, etc.) to delivery sensor nodes to a given territory and subsequent installation.
Key words: ubiquitous sensor networks, flying ubiquitous sensor networks, unmanned aerial vehicles, UAVs, sensor nodes, installation of sensor nodes, coverage.

Dubrovin N., Ushakov I., Chechulin A. Big Data Technologies for Security Information and Event Management Systems. – PP. 348–353.
In the conditions of continuous increase in quantity and diversity of the data coming to systems of information security, opportunities of traditional storage systems and processing even more

often appear insufficiently for the operational analysis and formation of decisions. It is offered to apply technology of Big data to the solution of this problem. In article the main methods and concepts of technology of Big data, and also architecture of the developed program prototype for carrying out experiments are considered.
Key words: Big data, Hadoop, data processing, computing cluster, SIEM.

Elagin V. Approaches to Modeling of Lawful Interception at SDN. – PP. 353–358.
The article investigates the models and implementations of lawful interception in telecom networks. The main attention is paid to organization of LI in SDN. At the same time considered OpenFlow protocol operating procedures.
Keywords: simulation of queuing systems, lawful interception, software-defined network, OpenFlow protocol, post-NGN networ.

Esalov K., Pavlenko M. Technicians of Social Engineering in Information Environments and the Analysis of Methods of Protection Against Them. – PP. 358–363.
Safety is called the first of five main problems of the Internet. At present information networks represent effective, but full of threats and dangers, Wednesday. And despite variety of various means of protection, there are threats from which it isn't simple to be protected program or hardware. One of such threats is the social engineering. This report is devoted to consideration of technology of application of social engineering in computer communication networks. In him different types of the attacks connected with use of social engineering are analysed and the existing and possible methods of their prevention are described.
Key words: information security, social engineering, prevention of threats, network attack, phishing.

Zhernova K., Korzhik V. Comparison of New Russian Federation Block Cipher Standard (GOST R 34.12-2015) with Known Before Block Ciphers and Estimation of this Hardware Implemented Standard Breaking on. – PP. 363–368.
Encryption and decryption algorithms of new Russian Federation block cipher standard (GOST R 34.12-2015) is considered. These algorithms are compared with algorithms of such well known block ciphers as DES, AES, GOST-28147-89. New standard seems to be closer to optimal block cipher structure than known before. But its hardware implementation is still vulnerable to side attacks.
Key words: block cipher, linear and non-linear transform, algorithm GOST R 34.12-2015, attack on block ciphers, DPA-attack, side attack.

Zakharov M., Kirichek R. Internet of Things Devices Hub. – PP. 368–371.
Due to the fact that the concept of the Internet of Things became commonly used in the near future is expected to increase avalanche devices connected to the Internet, both in industry and in the housing sector. To ensure easy user interaction with equipment from different manufacturers need to realize the possibility of Internet Things centralized management within an enterprise, office, apartments, etc. The solution to this problem is the development and creation of the Internet of Things hub devices.
Key words: Internet of Things, hub, wireless access.

Ivanov V., Pankov R., Udaltsov A. The Study of Bandwidth Estimation in Transport Networks for Special Purposes. – PP. 371–377.
The paper discusses the principles of construction and structure of transport network for special purposes. Detail the issues of assessing the capacity of transport networks for special purposes, the basic properties and requirements to be met.
Key words: communications network, transport network, transmission network, bandwidth, the access node, communication service, network requirements, channels of communication, group transmission paths, digital hierarchy.

Ivanov V., Patric O. SCS Standards Evolution. – PP. 377–380.
This article is contented cause of appearance and next development of SCS standards. In this article also is showed changes of SCS cables electrical data, which is regulated by International Standard ISO/IEC 11801.
Key words: Structural cable system, standards of SCS, date regulations.

Ivanov S., Safronov Y. Analysis of Information on DWDM Domestic and Foreign Production. – PP. 381–385.
This article presents an analysis of information systems of coarse wavelength division multiplexing - CWDM and systems of dense wavelength division multiplexing - DWDM, which today are the main systems to solve the problem and provide virtually unlimited bandwidth growth. Just do not forget about such a system as the tunable optical multiplexers IO - ROADM, which allow you to easily and quickly increase the capacity of the link where it is necessary, without resorting to expensive network redesign and methods without stopping the provision of telecommunications services.
Key words: DWDM, CWDM, ROADM.

Kazakov D., Krasov A., Lokhanko N., Podoliak R. Method of Protection of Communication Networks Against DDOS Attacks by Using the Flowspec BGP. – PP. 386–390.
This article focuses on BGP Flow Specification is described in RFC5575 and often abbreviated as BGP FlowSpec. This extension to BGP whose main task is to dynamically reflect the DDoS attacks. The aim of the article put the story of the protocol on its functioning, reviewed and analyzed various scenarios for countering DDoS attacks at various topologies networks, describes the features of BGP FlowSpec, as well as other options in addition to its use to prevent DDoS attacks.
Key words: network security, anti DDoS, BGP FlowSpec.

Kirichek R., Petrikov A. Problems of Network Security on the Internet of Things. – PP. 391–394.
Currently, the Internet of Things is the most important concept in the field of telecommunications, and at the same time one of the potentially dangerous technology. The article is devoted to the review and study of the actual problems of network security within the concept of the Internet of Things. The characteristic features of IoT-devices in terms of network security, analyzes the main causes of vulnerability, as well as the main types of attacks. The impossibility of using classical methods of information protection for the majority of IoT-devices, as well

as formulated the task to ensure the confidentiality, integrity and availability of information depending on the functions performed by IoT-devices.
Key words: Internet of Things, network security, confidentiality, integrity, encryption.

Kirichek R., Razumov A. The Case Study of the Influences of Intentional Electromagnetic Interference on the Attacking Channels of the Internet of Things. – PP. 395–399.
Widespread acceptance of technologies, which connect with using Internet of Things, puts new tasks for improving the resistance and resiliency of wireless communications.
One of the gauge for the safe use of wireless communication channels is their protection from exposure ultrashort electromagnetic pulses as the most negative factor of influence on the process of data transfer.
Key words: Internet of Things, intentional electromagnetic interference, matlab, simulink, simulation modeling.

Kirichek R., Hoang Tr. A Comparative Analysis of the Functioning of Routing Algorithms in wireless Sensor Networks Under Intentional Electromagnetic Interference Conditions. – PP. 400–405.
Article investigates possible vulnerabilities of wireless sensor networks to intentional destructive electromagnetic interference. A comparative analysis of routing protocols used in wireless sensor networks based on a set of criteria necessary for the effective functioning in the conditions of intentional electromagnetic influences.
Key words: wireless sensor networks (WSN), fault tolerance, routing, reliability, sensor node, intentional electromagnetic interference.

Kirichek R., Yastrebov E. Software and Hardware Planning for Autonomous Flight of Unmanned Aerial Vehicles Public. – PP. 405–410.

Currently, most of the polarity of the received unmanned aerial vehicles (UAV), the public view of ease of operation and low cost. Because of the wide spread of wireless sensor networks in the various sectors of agriculture and industry started to use UAVs to collect data from remote sensor fields for further delivery to the public communication network. One of the key challenges in this area - the creation of hardware and software for UAV autonomous flight without the active involvement of the operator. The paper presents a study of the existing tools for the UAV mission planning for various platforms (PC, Android, iOS), as well as the modification and use of these solutions to specific problems. Make a choice and provide a rationale for the software that formed the basis of your application. The developed application allows you to plan the optimal route for the UAV overflight sensor nodes distributed in space, makes it possible to download the flight task in the flight controller and display basic flight data telemetry channel.
Key words: unmanned aerial vehicle, route, telemetry, communications channel software.

Kislyakov S., Lankevich K. Optimization Algorithm for WFM System as Instrument to Customer Loyalty Control. – PP. 410–414.
Customer loyalty depends on many factors, including how well-performing operator agreement with the customer, in particular, as a punctual visiting specialists. The two-stage optimization

algorithm improves the quality of customer service by reducing the execution time and the guarantee of service in precisely chosen time interval.
Key words: Workforce Management (WFM), customer loyalty, optimization.

Kislyakov S., **Habaev N.** A Method of Controlling Customer Churn Through a System of Integrated Technical Support. – PP. 414–417.
In today's world for telecommunications companies to introduce new technical solutions it is no longer crucial to obtain more customers. The main purpose of automation of business processes support operator - assistance to clients in case of complaints on problems with communication or other services. However, these systems can be used "off-label" – to control the outflow of customers.
Key words: Customer loyalty, class Assurance system, outflow management.

Kovzur M., Pavlukovich M. Method of the Organization of the Accredited Certifying Center. – PP. 417–421.
The popular trend is the increasing of electronic document in connection with the widespread Internet. The necessity of monitoring integrity of the electronic documents in data channel have appeared. People can use a qualified electronic signature to protect electronic documents. To obtain such signature the accredited certification center is used.. This article describes the method used to organize the accredited certification centre. Also article describes a number of processes and specific conditions, which implementation is required for the operation of the accredited certification center.
Key words: digital signature, qualified electronic signature, certifying center, document integrity.

Kovzur M. The Ways of Modernization of the Key Distribution Protocol for Secured IP-Telephony. – PP. 421–426.
IP-telephony at the present stage of telecommunication network evolution in the Russian Federation is used to provide services to the population and to the corporate sector. Dedicated communication channels and public communication channels are used in order to provide IP-telephony services. All this makes actual the issue of the protection of media traffic from unauthorized access. The security level provided by cryptographic protocol Secure Real-time Transport Protocol and time to establish a secure connection are largely determined by the key distribution protocol, one of which is Zimmermann Real-time Transport Protocol (ZRTP). The article describes the proposals for modification of the protocol ZRTP to reduce the time the successful execution of the protocol and improve information security through the introduction of the method of automatic detection of active violator.
Key words: IP-telephony, modification of the ZRTP, key distribution protocol, VoIP, SRTP.

Korzhik V., Kropivko I. Acoustic Stegosystem Using Echo-Signals for Information Hiding Detection Methods Investigation. – PP. 427–431.
Stegosystem design with embedding in audio cover objects and transmission over acoustic media is sufficiently new and effective way for information security providing. The detection methods for such stegosystems based on the use of cepstrum analysis are theoretically and practically investigated in this paper.

It is shown that for appropriated selection of stegosystem parameters these methods can provide a sufficient detection reliability.
Key words: stegosystem, audiosignals, echo-signals, cepstrum analysis.

Korzhik V., Tokareva M. Method of System Steganalysis Based on Statistical Estimation of Extracted Sequence under the Condition of Their Encryption Before Embedding, by Strong Cipher. – PP. 431–436.
New system attack for detection of digital image stegosystem is proposed. It is assumed that the embedded sequence extracted algorithm is known before steganalysis. Then decision about a stegosystem presence is taken if the extracted and encrypted before embedding by strong cipher sequence satisfies to NIST criteria of pseudorandomness. Experimental results confirm that such attack works.
Key words: stegosystem, encryption, digital images, NIST-based criteria of pseudorandomness.

Kuznetsov V, Sumkin V. Investigation of the Erbium Amplifier. – PP. 436–441.
The article is devoted to the investigation of the optical amplifier EDFA made by the authors. The EDFA operating principles and use were considered, the investigation of the amplifier parameters depending on the variations of the input signal power, the pump signal and the length of erbium-doped fiber were carried out.
Key words: optical amplifier, optical fiber, pump signal, signal power, wavelength, amplified spontaneous emission, gain factor, threshold power.

Kuznetsov I., Lipatnikov V., Sakharov D. Method of Information and Computer Network Based Short-Term Forecasting Spread of Computer Viruses. – PP. 441–446.
The article describes a method of controlling information and computer network on the basis of short-term forecasting the spread of a computer virus, developed on the basis of the model spread epidemic diseases, as well as a method of control with the use of predictive models (Model Predictive Control).
Keywords: data-processing network; computer virus; data protection; control using predictive models; Model Predictive Control (MPC); State-Space Model Predictive Control (SSMPC); SSMPC; InformSec; IBM; MRS; model state space, epidemiological model.

Le T., Simonina O. Using SDN to Support QoS in Wireless Networks with a High Density of Network Devices – PP. 446–450.
In the article, we proposed to use a software-defined network (SDN) based solution to manage traffic flows in Wi-Fi networks with a high density of network devices. Traffic classification based on the DSCP value in the IP-packet headers. After categorization, the traffic will be assigned priority at the port of OpenFlow switch. This method allows organizing end-to-end quality assurance and supporting traffic classification in the internetting.
Key words: classification, SDN, QoS, Wi-Fi, DSCP.

Leykin A. Security Solutions for SCTP. – PP. 451–456.
The Stream Control Transmission Protocol is a transport protocol initially developed to transport signaling messages SS7 over IP networks. The new features of SCTP make it also

a suitable candidate for applications which nowadays use the standard transport protocols TCP and UDP. Many of these applications have strict requirements with respect to end-to-end security. Providing end-to-end security by using IPsec or the Transport Layer Security (TLS) protocol in combination with SCTP is subject to functional and performance related limitations. These can be avoided by integrating security functions directly into SCTP (S-SCTP).
Key words: SCTP, SIGTRAN, S-SCTP, TLS, IPSec, End-to-End security.

Loginov S. On Usage of Multiagent Systems for Network Management. – PP. 456–461.
Paper justifies the relevance of creating new models and methods for describing device communication in a wireless ad hoc network taking into account new business requirements. To portray device communication author suggests describing the behavior of the resources in this networks as intelligent agents and usage of game theory instruments.
Key words: Game theory, coalitional game theory, ad hoc networks.

Lushnikova T. Using Netflow for Network Traffic Analysis. – PP. 461–466.
The Netflow protocol is one of the most popular network monitoring tools. Howether using Netflow for scientific research gives some restrictions for analysing of network traffic characteristics.
In this paper we focus on the dropping this restrictions. We discuss the features of the Netflow protocol and the format of the exported data. Besides, we represent algorithm that allow us to analyze sessions instead Netflow flows.
Key words: Netflow, flow-tools, TCP flags, session assembling, traffic monitoring.

Mazepkin S., Matveykin G., Fedoseev D. Mathematical Model for Estimation Optical Fibers Specific Chromatic Dispersion Coefficient. – PP. 466–470.
An optical signal propagating along the fiber is distorted due to the dispersion of various kinds. The article describes mathematical model for calculating specific chromatic dispersion coefficient based on the three-membered Sellmeyer equation. Proposed version of the calculation allows to determine with high confidence specific chromatic dispersion optical coefficient of fiber with given chemical composition of the core and cladding.
Key words: optical fiber, the refractive index, wavelength, mode, chromatic dispersion, polarization mode dispersion.

Matukhin A., Meltenisov M. Model of Generation the Signal Responses to Effect of the Chromatic Dispersion in the Optical Fiber. – PP. 470–475.
The investigation of chromatic dispersion effect is one of current issues in the modern fiber-optic transmission systems. The analytical description of dispersion effect in the time-domain is of special interest. The one of possible variation of description is the echo-signals model. The possibility of representation the signal propagation process in the form of the sequential generation of echo-signal pairs is substantiated in this paper.
Key words: model, time domain, coefficients, optical fiber, chromatic dispersion, echo signals.

Mishin A., Yurkin D. Creation of a Schielding Router Conforming to Requirements of the Guidance Document FSTEC of the Russia. – PP. 475–479.
In any large network topology there is such element as a router. This network device performs tasks such as routing, filtering, and the fragmentation of packets. The functionality of the modern routers is very high.
Key words: UNIX, schielding router, netfilter, iptables.

Mylnikov P. Investigation of Probability Characteristics of the Key Generated Based on the MIMO Channel Output Quantization. – PP. 479–484.
The statistical characteristics of a key obtained on the estimation of MIMO random channel transmission parameters are investigated. The correlation coefficients, Shannon entropy, Renyi entropy, minimum entropy and the statistical range are studied based on the simulation. The statistical characteristics of a key are estimated using graphic and assessment tests.
Key words: wireless network security, MIMO channel, key distribution, entropy, statistical tests, NIST STS.

Mylnikov P., Yakovlev V. Key Generation Procedure for Optimizing the System Parameters Based on the Signals in Phase Quantization MIMO Channel. – PP. 484–488.
The method of key distribution in wireless MIMO-based channels with mobile units is investigated. The expressions for estimating a probability of a correct and an incorrect decision of the signal phase quantization based on the use of guard interval are given. Optimization of system parameters providing the highest key generation rate is investigated under the condition of given probability for shared key coinciding.
Key words: wireless network security, MIMO channel, optimization, cryptographic key.

Nebaeva K., Popov L. A Comparative Study of the Methods of Digital Video Steganalysis. – PP. 489–493.
In this paper some existing methods of digital video steganalysis, utilizing different approaches of processing of video sequences, in which the information was embedded, are considered. Besides, the analysis of these steganographic methods and conclusions about an opportunity of practical employment in real time applications are represented.
Key words: steganography, steganalysis, digital video sequence, linear collusion, temporal correlations, asymptotic memoryless detection, spread spectrum embedding, multiplicative embedding.

Nebaeva K., Skorodumov S. Steganography in IP-Telephony and its Implementation Complexity. – PP. 494–498.
The article discusses the possibility of using the flow of containers to embed hidden information, namely, the data packets are transmitted in real time protocol RTP application level. This protocol is considered as the basic standard for the transmission of voice and video IP-based networks and together with codecs.
Key words: Digital steganography, IP-telephony, RTP, codec.

Nikitin B., Sergeev A., Smirnov G. The Standardization of an Optical Path of Amplifiers – PP. 499–502.

In the article the questions of regulation of components of fiber-optical transmission line with optical amplifiers. The basic requirements for technical characteristics of optical signals at the point of rationing, to the transmitting and receiving devices, as well as to the optic tract. Issues considered popular in the design of communication lines. In addition, knowledge of rules, technical operation of fiber-optic transmission lines, working with the technology of synchronous digital hierachie levels STM-4, 16, 64.

Key words: rationing, elementary cable section, the optical path loss, dispersion, accumulated dispersion, attenuation, jitter, MPI-S to MPI-R, PMD, polarization-mode dispersion, an optical interface, a point of regulation, the code of the application, the ratio "signal-noise", noise-factor, transmitting device, receiving device, coefficient of variance.

Ostroumov O., Savischenko N. The Assessment of Communication Channel Noise Immunity with Fading and Diversity Reception. – PP. 503–507.

The article is dedicated to the noise immunity assessment method of high frequency radio communication channels at the diversity reception of the multipositioned signals. The accurate expressions of the error possibility calculation in the communication channel in the conditions of Rice and Releigh fading are received. The usage of different kinds of the diversity reception for the communication quality improvement is proved.

Key words: fading, diversity reception, error possibility, multipositioned signals.

Pirmagomedov R., Hudoev I. Overview of Trends of Neural Network Technology in Medicine. – PP. 508–512.

This paper examines the impact of the development of telecommunications technologies to the healthcare system. Particular attention is paid to the nanonetworks in medicine. The possible deployment methods nanonetworks in various contexts of the human environment, considered architecture and applications nanonetworks in medicine, as well as present the modern prototypes and ideas for their implementation. Identify problems standing in the way of development the Internet of Nano-Things on the part of technology that has yet to be implemented in the future, and on the part of the modern Internet and telecommunication equipment.

Key words: Internet of Nano-Things, nanonetworks, nanostructures, healthcare system.

Podolsky D., Rogozinsky G. The Parsing Results Sonification. – PP. 512–516.

The article presents the parsing results of four popular websites for their acoustic display called sonification. It extends the analysis of complex information by using of a human ear that makes faster detection of the features in the data stream.

The gathered data during a week was sonificated as an appropriate timbral classes by sound and music computing system Csound.

Keywords: data sonification, parsing, Csound.

Polyakova E. Calculation of Optical Combinations Using Matrix Optics Method. – PP. 516–519.

Light transmission through an ideal centred optical system problem can be solved in different ways. Along with the common calculations exists matrix method, that allows to correlate input

and output parameters of the system. Matrix optics method is valid for optical systems calculations based on using optical microcomponents.
Key words: fibre-optic microcomponent, lens microcomponent, specific fibes, transfer matrix.

Rogozinsky G., Shchekochikhin A. Implementation of Sonification's Methods and Sensors Networks in the Distributed System of Soundscapes Generation. – PP. 520–524.
The authors are in a research of automating of music and soundscapes composition. The distributed system of automated music composition consists of computer network; genetic algorithm is applied as a basis for automated music composition model. This paper is on reviewing of sonification methods and authors approach for their implementation for sensors network data sonification.
Key words: algorithmic composition, data sonification, sensor networks.

Serdyuk S. Organization Problems of the Trusted Communication Digital Network with Integrated Services of Russian Emercom in an Untrusted Telecommunication Framework. – PP. 525–529.
Among enormous organization problems of Russian Emercom trusted network in an untrusted telecommunications framework there are problems of topology, load balancing and safe scaling. Certain examples of known solutions are given. Scientifically technical task of the synthesis of mechanism complex of Russian Emercom telecommunications network safe scaling is updated.
Key words: trusted network, untrusted framework, topology, load balancing, safe scaling, mechanism complex.

Simonina O., Umirov E. Models of the QoS in IoT Networks. – PP. 529–534.
This paper deals with models for traffic parameters estimation taking into consideration the bandwidth and QoS requirements.
Key words: IoT, QoS.

Tikhonov S. Investigation of a Hardware Implemented Block Cipher Breaking Practical Opportunity Based on the Power Analysis Attack, by the Example of GOST 28147-89. – PP. 534–539.
The peculiarities and the complexity of the practical implementation of block ciphers breaking (in particular, GOST 28147-89) running on Atmel microcontroller and based on power consumption side attack are considered. Description of technical devices complexity, which provide such attack with minimal costs is presented. The operations with the greatest leakage of secret information along side channel are found. Proposals for increase the effectiveness such attack are given.
Key words: secret key, algorithm DES, S-boxes, power attacks, side-channel attacks, differential power analysis (DPA).

Fitsov V. The Simulation Model of the System DPI, Based GPSS World Software. – PP. 539–545.
This article describes the development and use of a simulation model of the system DPI. Used simulation software GPSS World. In constructing the simulation model takes general architecture of the system DPI. Show algorithm of model. Attempted to assess system performance parameters by varying the flow of incoming traffic.
Key words: DPI, signature, QoS, GPSS, queuing system (QS), queuing network.

Shterenberg S. The Correlation and Heuristic Analysis of the Action of Self-Modifying Code for the Protection of Information in the Executable File. – PP. 545–550.
The article discusses ways of representing elements of self-modifying code in executable files for adaptive systems. Based on the way, should bring the correlation and heuristic analysis of the action of self-modifying code to derive specifications operate the software. This self-modifying code is designed to protect software from compromising the integrity.
Key words: self-modifying code, executable file, data protection, software, adaptive system.

Yaroshenko A. Systematic Approach to Implementation and Customization of Firewalls in State Information Systems. – PP. 551–554.
The article presents the organizational documents for the use of firewalls in state organizations, as well as negative examples of "default" options. Also there are proved the necessity for a systematic approach to the implementation and customization of firewalls in state information systems.
Key words: information security threats, firewall, state information systems, implementation and customization, systematic approach.

АВТОРЫ СТАТЕЙ

FORSGREN Harri — postgraduate Department of Computer Science University of Helsinki, Timo.Karvi@cs.Helsinki.FI

GUILIN Wen — Hunan University, China, begspb1976@mail.ru

KARVI Timo — PhD, lector Department of Computer Science University of Helsinki, Timo.Karvi@cs.Helsinki.FI

LU Jian — Key Laboratory of Advanced Design and Simulation Techniques for Special Equipment, Ministry of Education; State Key Lab of Advanced Design and Manufactory for Vehicle Body, Hunan University, Changsha, Hunan 410082, China, begspb1976@mail.ru

АВГАРИ Файз Салех Али — аспирант кафедры радиосистем и обработки сигналов Санкт-Петербургского государственного университета телекоммуникаций им. проф. М. А. Бонч-Бруевича, fsaleh28@yahoo.com

АВРАМЕНКО Максим Валентинович — студент Санкт-Петербургского государственного университета телекоммуникаций им. проф. М. А. Бонч-Бруевича, avramenko.maxim2012@yandex.ru

АЛЬ-АМЕРИ Хамед Абдо — аспирант кафедры радиосвязи и вещания Санкт-Петербургского государственного университета телекоммуникаций им. проф. М. А. Бонч-Бруевича, hamedru2008@gmail.com

АЛЬ-ОДХАРИ Абдулвахаб Хуссейн — аспирант кафедры радиосвязи и вещания Санкт-Петербургского государственного университета телекоммуникаций им. проф. М. А. Бонч-Бруевича, abdwru2011@yandex.ru

АНАНЬЕВ Александр Владиславович — кандидат технических наук, докторант кафедры радиоэлектроники Военного учебно-научного центра Военно-воздушных сил «Военно-воздушной академии имени профессора Н. Е. Жуковского и Ю. А. Гагарина», sasha303_75@mail.ru

АНГЕЛУЦ Ангелина Алексеевна — аспирант кафедры конструирования и производства радиоэлектронных средств Санкт-Петербургского государственного университета телекоммуникаций им. проф. М. А. Бонч-Бруевича, angeluts@bk.ru

АНДРЕЕВ Роман Александрович — начальник отдела эксплуатации ООО «Гиперион», andreeffrom@mail.ru

АНДРИАНОВ Владимир Игоревич — кандидат технических наук, профессор кафедры защищенных систем связи Санкт-Петербургского государственного университета телекоммуникаций им. проф. М. А. Бонч-Бруевича, vladimir.i.andrianov@gmail.com

АНТИПИН Борис Маврович — кандидат технических наук, доцент кафедры телевидения и метрологии Санкт-Петербургского государственного университета телекоммуникаций им. проф. М. А. Бонч-Бруевича, Boris_Antipin@mail.ru

АРХИПОВ Валерий Викторович — аспирант кафедры защищенных систем связи Санкт-Петербургского государственного университета телекоммуникаций им. проф. М. А. Бонч-Бруевича, vvarh@mail.ru

АХМЕДОВ Булат Игорьевич — магистрант Балтийского государственного технического университета им Д. Ф. Устинова «ВОЕНМЕХ», Ahmedov_Bulat@mail.ru

БАБКОВ Валерий Юрьевич — доктор технических наук, профессор кафедры радиопередающих устройств и средств подвижной связи Санкт-Петербургского государственного университета телекоммуникаций им. проф. М. А. Бонч-Бруевича, babkov_v@mail.ru

БАШМАКОВ Павел Александрович — инженер по внедрению холдинга PT Electronics, bashmakovpa@gmail.com

БИРИХ Эрнест Владимирович — заместитель начальника отдела по защите прав субъектов персональных данных и информационных технологий Управления Роскомнадзора по Северо-Западному федеральному округу, Санкт-Петербург, be198297@gmail.com

БОБРОВА Екатерина Валерьевна — инженер отдела эксплуатации ООО «Гиперион», bobrova12504@gmail.com

БОГОЛЕПОВ Григорий Сергеевич — заместитель начальника НИО-5 Военной академия связи имени Маршала Советского Союза С. М. Буденного, bogolepv@inbox.ru

БОЛТОВ Юрий Федорович — кандидат технических наук, доцент кафедры программной инженерии и вычислительной техники Санкт-Петербургского государственного университета телекоммуникаций им. проф. М. А. Бонч-Бруевича, ufb@edwer.spb.ru

БОРИСОВ Евгений Геннадьевич — кандидат технических наук, профессор кафедры радиосистем и обработки сигналов Санкт-Петербургского государственного университета телекоммуникаций им. проф. М. А. Бонч-Бруевича, begspb1976@mail.ru

АВТОРЫ СТАТЕЙ

БОРОДКО Александр Владимирович — кандидат технических наук, доцент кафедры сетей связи и передачи данных Санкт-Петербургского государственного университета телекоммуникаций им. проф. М. А. Бонч-Бруевича, borodkoa@mail.ru

БУЗЮКОВ Лев Борисович — кандидат технических наук, профессор кафедры программной инженерии и вычислительной техники Санкт-Петербургского государственного университета телекоммуникаций им. проф. М. А. Бонч-Бруевича, levbuz@mail.ru

БУЙНЕВИЧ Михаил Викторович — ведущий научный сотрудник Управления организации научной работы и подготовки научных кадров Санкт-Петербургского государственного университета телекоммуникаций им. проф. М. А. Бонч-Бруевича, bmv1958@yandex.ru

БЫЛИНА Мария Сергеевна — кандидат технических наук, доцент кафедры фотоники и линий связи Санкт-Петербургского государственного университета телекоммуникаций им. проф. М. А. Бонч-Бруевича, BylinaMaria@mail.ru

ВИНОГРАДОВ Евгений Михайлович — кандидат технических наук, ведущий научный сотрудник научно-исследовательской лаборатории радиоконтроля и электромагнитной совместимости Санкт-Петербургского государственного университета телекоммуникаций им. проф. М. А. Бонч-Бруевича, vin@irga.sut.ru

ВИНОГРАДОВ Петр Юрьевич — кандидат технических наук, доцент кафедры радиосвязи и вещания Санкт-Петербургского государственного университета телекоммуникаций им. проф. М. А. Бонч-Бруевича, power@sut.ru

ВИТКОВА Лидия Андреевна — аспирант кафедры защищенных систем связи Санкт-Петербургского государственного университета телекоммуникаций им. проф. М. А. Бонч-Бруевича, iskinlidia@gmail.com

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

ВЛАСОВ Дмитрий Сергеевич — заместитель начальника отдела информационных технологий, АСУ и связи СЗРЦ МЧС России, prikerx@bk.ru

ВОЛЩУКОВ Матвей Юрьевич — аспирант кафедры сетей связи и передачи данных Санкт-Петербургского государственного университета телекоммуникаций им. проф. М. А. Бонч-Бруевича, neve75@mail.ru

ВОРОНКОВ Константин Игоревич — начальник лаборатории систем вторичного уплотнения Санкт-Петербургского государственного университета телекоммуникаций им. проф. М. А. Бонч-Бруевича, voronkovkonstantin@yandex.ru

ВЫБОРНОВА Анастасия Игоревна — кандидат технических наук, доцент кафедры сетей связи и передачи данных Санкт-Петербургского государственного университета телекоммуникаций им. проф. М. А. Бонч-Бруевича, a.vybornova@gmail.com

ГАЛЬЧИН Рома Игоревич — инженер отдела эксплуатации ООО «Гиперион», rrez571@gmail.com

ГАМИЛЬ Абдуллах Абдулрахман — аспирант кафедры инфокоммуникационных систем Санкт-Петербургского государственного университета телекоммуникаций им. проф. М. А. Бонч-Бруевича, obad-85a@mail.ru

ГЕРАСИМОВА Ирина Александровна — магистрант, группа ИКТГ-56м Санкт-Петербургского государственного университета телекоммуникаций им. проф. М. А. Бонч-Бруевича, iris.gia93@mail.ru

ГЕРЛИНГ Екатерина Юрьевна — кандидат технических наук, доцент кафедры защищенных систем связи Санкт-Петербургского государственного университета телекоммуникаций им. проф. М. А. Бонч-Бруевича, abri@rambler.ru

ГЛАГОЛЕВ Сергей Федорович — кандидат технических наук, доцент, заведующий кафедрой фотоники и линий связи Санкт-Петербургского государственного университета телекоммуникаций им. проф. М. А. Бонч-Бруевича, glagolevsf@yandex.ru

ГЛАЗКОВ Роман Викторович — аспирант кафедры радиопередающих устройств и средств подвижной связи Санкт-Петербургского государственного университета телекоммуникаций им. проф. М. А. Бонч-Бруевича, roman.v.glazkov@ya.ru

ГОГОЛЬ Александр Александрович — доктор технических наук, профессор, заведующий кафедрой телевидения и метрологии Санкт-Петербургского государственного университета телекоммуникаций им. проф. М. А. Бонч-Бруевича, Al.Gogol@mail.ru

ГОДЛЕВСКИЙ Артур Константинович — студент Санкт-Петербургского государственного университета телекоммуникаций им. проф. М. А. Бонч-Бруевича, artigodl@gmail.com

ГОЙХМАН Вадим Юрьевич — кандидат технических наук, доцент кафедры инфокоммуникационных систем Санкт-Петербургского государственного университета телекоммуникаций им. проф. М. А. Бонч-Бруевича, vg@sotsbi.ru

ГОЛОД Олег Саулович — кандидат технических наук, доцент кафедры радиосистем и обработки сигналов Санкт-Петербургского государственного университета телекоммуникаций им. проф. М. А. Бонч-Бруевича, oleg-spbru@mail.ru

ГОНЧАРОВА Дарья Сергеевна — студентка Санкт-Петербургского государственного университета телекоммуникаций им. проф. М. А. Бонч-Бруевича, 0309dariya@inbox.ru

ГРОМОВ Иван Александрович — Председатель Комитета по информатизации и связи Санкт-Петербурга, kis@gov.spb.ru

ДЁШИНА Наталия Олеговна — старший преподаватель кафедры конструирования и производства радиоэлектронных средств Санкт-Петербургского государственного университета телекоммуникаций им. проф. М. А. Бонч-Бруевича, salo_piter141@mail.ru

ДИКАНЕВА Катерина Николаевна — студентка Санкт-Петербургского государственного университета телекоммуникаций им. проф. М. А. Бонч-Бруевича, k.n.dikaneva@gmail.com

ДИНЬ Чыонг Зюи — магистрант кафедры сетей связи и передачи данных Санкт-Петербургского государственного университета телекоммуникаций им. проф. М. А. Бонч-Бруевича, duydthiph@gmail.com

ДМИТРИЕВ Павел Дмитриевич — аспирант кафедры радиосвязи и вещания Санкт-Петербургского государственного университета телекоммуникаций им. проф. М. А. Бонч-Бруевича, p-dmitriev@list.ru

ДРЕМИНА Анастасия Дмитриевна — студентка Санкт-Петербургского государственного университета телекоммуникаций им. проф. М. А. Бонч-Бруевича, vg@sotsbi.ru

ДУБРОВИН Никита Дмитриевич — магистрант кафедры защищённых систем связи Санкт-Петербургского государственного университета телекоммуникаций им. проф. М. А. Бонч-Бруевича, nikita.dubrovin.dm@gmail.com

ДЮБОВ Андрей Сергеевич — Кандидат технических наук, доцент кафедры фотоники и линий связи Санкт-Петербургского государственного университета телекоммуникаций им. проф. М. А. Бонч-Бруевича, blip@bk.ru

ЕГОРОВ Станислав Геннадьевич — ассистент кафедры радиосистем и обработки сигналов Санкт-Петербургского государственного университета телекоммуникаций им. проф. М. А. Бонч-Бруевича, sgegorov@gmail.ru

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

ЕРМАКОВА
Татьяна Вячеславовна — аспирант кафедры программной инженерии и вычислительной техники Санкт-Петербургского государственного университета телекоммуникаций им. проф. М. А. Бонч-Бруевича, t.ermakova89@gmail.com

ЕСАЛОВ
Кирилл Эдуардович — ассистент кафедры инфокоммуникационных систем Санкт-Петербургского государственного университета телекоммуникаций им. проф. М. А. Бонч-Бруевича, yk@bonch-ikt.ru

ЖЕРНОВА
Ксения Николаевна — студентка Санкт-Петербургского государственного университета телекоммуникаций им. проф. М. А. Бонч-Бруевича, orolakela@yandex.ru

ЗАХАРОВ
Максим Валерьевич — студент, инженер кафедры сетей связи и передачи данных Санкт-Петербургского государственного университета телекоммуникаций им. проф. М. А. Бонч-Бруевича, zaharov.spbgut@gmail.com

ИВАНОВ
Андрей Дмитриевич — магистрант кафедры конструирования и производства радиоэлектронных средств Санкт-Петербургского государственного университета телекоммуникаций им. проф. М. А. Бонч-Бруевича, audi_3d@rambler.ru

ИВАНОВ
Александр Юрьевич — доктор технических наук, профессор кафедры сетей связи и передачи данных Санкт-Петербургского государственного университета телекоммуникаций им. проф. М. А. Бонч-Бруевича, alexandr.y@mail.ru

ИВАНОВ
Василий Геннадьевич — кандидат военных наук, доцент кафедры организации Военной академии связи им. Маршала Советского Союза С. М. Буденного, wasj2006@yandex.ru

ИВАНОВ
Владимир Степанович — кандидат технических наук, доцент кафедры фотоники и линии связи Санкт-Петербургского государственного университета телекоммуникаций им. проф. М. А. Бонч-Бруевича, vsivanovspb@yandex.ru

ИВАНОВ
Сергей Александрович — кандидат технических наук, старший научный сотрудник научно-исследовательского центра Военной академии связи им. Маршала Советского Союза С. М. Буденного, sa-ivanov@inbox.ru

ИВАНОВА Мария Игоревна — аспирант кафедры телевидения и метрологии Санкт-Петербургского государственного университета телекоммуникаций им. проф. М. А. Бонч-Бруевича, klarnetistka@mail.ru

ИЗРАИЛОВ Константин Евгеньевич — научный сотрудник ФГУП «ГосНИИПП» ФСТЭК России, konstantin.izrailov@mail.ru

КАЗАКОВ Дмитрий Борисович — начальник управления информатизации Санкт-Петербургского государственного университета телекоммуникаций им. проф. М. А. Бонч-Бруевича, dkazakov@spbgut.ru

КАЙМОЛДИНОВА Жулдыз Амангелдиевна — магистрант Евразийского Национального университета им. Л. Н Гумилева, rumitbol@gmail.com

КАПРАЛОВ Дмитрий Дмитриевич — аспирант кафедры конструирования и производства радиоэлектронных средств Санкт-Петербургского государственного университета телекоммуникаций им. проф. М. А. Бонч-Бруевича, dmitry_kapralov@mail.ru

КАСАБАЕВА Дана Бердибековна — магистрант Евразийского Национального университета им. Л. Н. Гумилева, danaenu@mail.ru

КАЧНОВ Андрей Владимирович — Начальник отдела автоматизации Акционерного общества Научно-производственного предприятия «Авиационная и морская электроника», mfp_nio12@mail.ru

КИРИК Дмитрий Игоревич — кандидат технических наук, доцент, заведующий кафедрой конструирования и производства радиоэлектронных средств Санкт-Петербургского государственного университета телекоммуникаций им. проф. М. А. Бонч-Бруевича, d_i_kirik@mail.ru

КИРИЧЕК Руслан Валентинович — кандидат технических наук, доцент кафедры сетей связи и передачи данных Санкт-Петербургского государственного университета телекоммуникаций им. проф. М. А. Бонч-Бруевича, kirichek@sut.ru

КИСЛЯКОВ Сергей Викторович — кандидат технических наук, доцент кафедры инфокоммуникационных систем Санкт-Петербургского государственного университета телекоммуникаций им. проф. М. А. Бонч-Бруевича, s.kislyakov@argustelecom.ru

КОВАЛЕВА Татьяна Юрьевна — кандидат технических наук, доцент кафедры конструирования и производства радиоэлектронных средств Санкт-Петербургского государственного университета телекоммуникаций им. проф. М. А. Бонч-Бруевича, tankrivous@yandex.ru

КОВЦУР Максим Михайлович — старший преподаватель кафедры защищенных систем связи Санкт-Петербургского государственного университета телекоммуникаций им. проф. М. А. Бонч-Бруевича, maxkovzur@mail.ru

КОЛОТОВКИНА Галина Валерьевна — магистрант кафедры фотоники и линий связи Санкт-Петербургского государственного университета телекоммуникаций им. проф. М. А. Бонч-Бруевича, galina_kolotovkina@mail.ru

КОРЖИК Валерий Иванович — доктор технических наук, профессор кафедры защищённых систем связи Санкт-Петербургского государственного университета телекоммуникаций им. проф. М. А. Бонч-Бруевича, val-korzhik@yandex.ru

КОРЯКОВЦЕВ Александр Васильевич — оператор научной роты Военной академии связи им. Маршала Советского Союза С. М. Буденного, a.koriakovtcev@gmail.com

КРАСОВ Андрей Владимирович — кандидат технических наук, доцент кафедры защищённых систем связи Санкт-Петербургского государственного университета телекоммуникаций им. проф. М. А. Бонч-Бруевича, krasov@pisem.net

КРОПИВКО Иван Валерьевич — студент группы ИКТБ-58м Санкт-Петербургского государственного университета телекоммуникаций им. проф. М. А. Бонч-Бруевича, ivalkrop@gmail.com

КУБАЛОВА Анна Рудольфовна — кандидат технических наук, доцент кафедры теории электрических цепей Санкт-Петербургского государственного университета телекоммуникаций им. проф. М. А. Бонч-Бруевича, kubalovaap@mail.ru

КУДРЯШОВ Никита Валерьевич — старший оператор научной роты Военной академии связи им. Маршала Советского Союза С. М. Буденного, nikita471@yandex.ru

КУЗНЕЦОВ Вячеслав Сергеевич — студент Санкт-Петербургского государственного университета телекоммуникаций им. проф. М. А. Бонч-Бруевича, slava_kuznetsov@inbox.ru

КУЗНЕЦОВ Илья Алексеевич — оператор научной роты Военной академия связи им. Маршала Советского Союза С. М. Буденного, IKuznecov25@yandex.ru

КУЛИШКИНА Елена Игоревна — студентка Санкт-Петербургского государственного университета телекоммуникаций им. проф. М. А. Бонч-Бруевича, kulishkina_94@mail.ru

КУЧЕРЯВЫЙ Андрей Евгеньевич — доктор технических наук, профессор, заведующий кафедрой сетей связи и передачи данных Санкт-Петербургского государственного университета телекоммуникаций им. проф. М. А. Бонч-Бруевича, akouch@mail.ru

ЛАВРУХИН Владимир Алексеевич — начальник НОЦ «Беспроводные инфотелекоммуникационные сети» Санкт-Петербургского государственного университета телекоммуникаций им. проф. М. А. Бонч-Бруевича, vlavrukhin@sut.ru

ЛАНКЕВИЧ Ксения Евгеньевна — студент группы ИКТС-55м Санкт-Петербургского государственного университета телекоммуникаций им. проф. М. А. Бонч-Бруевича, k.lankevich@argustelecom.ru

ЛЕ Чан Дык — аспирант кафедры сетей связи и передачи данных Санкт-Петербургского государственного университета телекоммуникаций им. проф. М. А. Бонч-Бруевича, letranduc.telecom@gmail.com

ЛЕЖЕПЁКОВ Антон Сергеевич — инженер НОЦ «Беспроводные инфотелекоммуникационные сети» Санкт-Петербургского государственного университета телекоммуникаций им. проф. М. А. Бонч-Бруевича, lezhepekov@spbgut.ru

ЛЕЙКИН Антон Владиславович — старший преподаватель кафедры инфокоммуникационных систем Санкт-Петербургского государственного университета телекоммуникаций им. проф. М. А. Бонч-Бруевича, a.v.leykin@gmail.com

ЛЕОНОВ Андрей Владимирович — кандидат физико-математических наук, заместитель начальника научно-исследовательского отдела ООО «Т8», leonov.av@t8.ru

ЛИКОНЦЕВ Алексей Николаевич — кандидат технических наук, доцент кафедры радиосистем и обработки сигналов Санкт-Петербургского государственного университета телекоммуникаций им. проф. М. А. Бонч-Бруевича, likontsev-rts@mail.ru

ЛИКОНЦЕВ Дмитрий Николаевич — кандидат технических наук, доцент кафедры систем телерадиовещания Ташкентского Университета информационных технологий, dlikontsev@mail.ru

ЛИПАТНИКОВ Валерий Алексеевич — доктор технических наук, профессор, старший научный сотрудник научно-исследовательского центра Военной академии связи им. Маршала Советского Союза С. М. Буденного, lipatnikovanl@mail.ru

ЛОГИНОВ Сергей Сергеевич — аспирант кафедры инфокоммуникационных систем Санкт-Петербургского государственного университета телекоммуникаций им. проф. М. А. Бонч-Бруевича, ss7loginov@gmail.com

ЛОХАНЬКО Никита Олегович — студент Санкт-Петербургского государственного университета телекоммуникаций им. проф. М. А. Бонч-Бруевича, krasov@pisem.net

ЛУШНИКОВА Татьяна Юрьевна — аспирант кафедры инфокоммуникационных систем Санкт-Петербургского государственного университета телекоммуникаций им. проф. М. А. Бонч-Бруевича, lushnikova@iks.sut.ru

МАЗЕПКИН Сергей Сергеевич — старший оператор научной роты Военной академии связи им. Маршала Советского Союза С. М. Буденного, mazepkin.sergey@mail.ru

МАКАРОВ Леонид Михайлович — кандидат технических наук, профессор кафедры конструирования и производства радиоэлектронных средств Санкт-Петербургского государственного университета телекоммуникаций им. проф. М. А. Бонч-Бруевича, elfbio@gmail.com

МАЛИКОВА Жадра Бейсенгалиевна — магистрант Евразийского Национального университета им. Л. Н. Гумилева, jadra_92-92@mail.ru

МАЛЫШЕВ Алексей Геннадьевич — аспирант кафедры конструирования и производства радиоэлектронных средств Санкт-Петербургского государственного университета телекоммуникаций им. проф. М. А. Бонч-Бруевича, agmalyshev93@mail.ru

МАТВЕЙКИН Григорий Валерьевич — старший научный сотрудник Военной академии связи им. Маршала Советского Союза С. М. Буденного, matveykingv@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

МАШКОВ Георгий Михайлович — доктор технических наук, первый проректор – проректор по учебной работе Санкт-Петербургского государственного университета телекоммуникаций им. проф. М. А. Бонч-Бруевича, MashkovGM@sut.ru

МЕЛЬТЕНИСОВ Михаил Александрович — аспирант кафедры сетей связи и передачи данных Санкт-Петербургского государственного университета телекоммуникаций им. проф. М. А. Бонч-Бруевича, meltenisov@gmail.com

МЕНДЕЛЬСОН Марк Александрович — кандидат технических наук, доцент, ведущий научный сотрудник лаборатории систем вторичного уплотнения Санкт-Петербургского государственного университета телекоммуникаций им. проф. М. А. Бонч-Бруевича, mendvas@mail.ru

МИХАЛЕВ Олег Александрович — кандидат технических наук, начальник 3 отдела научно-исследовательского центра Военной академии связи им. Маршала Советского Союза С. М. Буденного, olemihalev@yandex.ru

МИХЕЕВ Александр Александрович — оператор научной роты Военной академии связи им. Маршала Советского Союза С. М. Буденного, amiheev1991@gmail.com

МИШИН Александр Сергеевич — студент Санкт-Петербургского государственного университета телекоммуникаций имени профессора М. А. Бонч-Бруевича, alexandrmishinn@ya.ru

МОРОЗОВА Татьяна Михайловна — инженер отдела эксплуатации ООО «Гиперион», morozovat.m@mail.ru

МОСТОВИЧ Дарья Ивановна — инженер-программист ФГУП «ГосНИИПП» ФСТЭК России, d.mostovich@mail.ru

МЫЛЬНИКОВ Павел Дмитриевич — начальник сектора Научно-исследовательского и проектно-конструкторского института информатизации, автоматизации и связи на железнодорожном транспорте, paul.mylnikov@gmail.com

НАНИЙ Олег Евгеньевич — кандидат физико-математических наук, профессор, начальник научно-исследовательского отдела ООО «Т8», naniy@t8.ru

НЕБАЕВА Ксения Андреевна — кандидат технических наук, доцент кафедры защищенных сетей связи Санкт-Петербургского государственного университета телекоммуникаций им. проф. М. А. Бонч-Бруевича, cbor.mail@gmail.com

НИКИТИН Борис Константинович — кандидат технических наук, доцент кафедры фотоники и линий связи Санкт-Петербургского государственного университета телекоммуникаций им. проф. М. А. Бонч-Бруевича, nbk117@mail.ru

ОДНОЛЬКО Осип Эдуардович — оператор научной роты Военной академии связи им. Маршала Советского Союза С. М. Буденного, odnosip@mail.ru

ОДОЕВСКИЙ Сергей Михайлович — доктор технических наук, профессор кафедры конструирования и производства радиоэлектронных средств Санкт-Петербургского государственного университета телекоммуникаций им. проф. М. А. Бонч-Бруевича, tmm_osm@rambler.ru

ОСТРОУМОВ Олег Александрович — адъюнкт Военной академии связи им. Маршала Советского Союза С. М. Буденного, oleg-26stav@mail.ru

ПАВЛЕНКО Михаил Евгеньевич — студент Санкт-Петербургского государственного университета телекоммуникаций им. проф. М. А. Бонч-Бруевича, www.noize@mail.ru

ПАВЛЮКОВИЧ Мария Вячеславовна — студент группы МС-21 Санкт-Петербургского государственного университета телекоммуникаций им. проф. М. А. Бонч-Бруевича, zetterstrom000@gmail.com

ПАНКОВ Роман Николаевич — слушатель Военной академии связи им. Маршала Советского Союза С. М. Буденного, ronasava@mail.ru

ПАРАМОНОВ Александр Иванович — доктор технических наук, профессор кафедры сетей связи и передачи данных Санкт-Петербургского государственного университета телекоммуникаций им. проф. М. А. Бонч-Бруевича, alex-in-spb@yandex.ru

ПАТРИК Олег Гарриевич — кандидат технических наук, доцент кафедры фотоники и линий связи Санкт-Петербургского государственного университета телекоммуникаций им. проф. М. А. Бонч-Бруевича, oleg.patric@gmail.com

ПЕНКИН Алексей Владимирович — ИНЖЕНЕР отдела автоматизации Акционерного общества Научно-производственного предприятия «Авиационная и морская электроника», mfp_nio13@mail.ru

ПЕТРЕНКО Михаил Игоревич — командир взвода (научного), младший научный сотрудник научно-исследовательского центра Военной академии связи им. Маршала Советского Союза С. М. Буденного, mishany11@mail.ru

ПЕТРИКОВ Александр Вячеславович — аспирант кафедры сетей связи и передачи данных Санкт-Петербургского государственного университета телекоммуникаций им. проф. М. А. Бонч-Бруевича, petrikofff@gmail.com

ПИРМАГОМЕДОВ Рустам Ярахмедович — кандидат технических наук, доцент кафедры сетей связи и передачи данных Санкт-Петербургского государственного университета телекоммуникаций им. проф. М. А. Бонч-Бруевича, lts.pto@yandex.ru

ПОДДУБНЫЙ Сергей Сергеевич — кандидат технических наук, доцент кафедры радиосистем и обработки сигналов Санкт-Петербургского государственного университета телекоммуникаций им. проф. М. А. Бонч-Бруевича, kafedra.rts@mail.ru

ПОДОЛЯК Родион Сергеевич — аспирант кафедры защищённых систем связи Санкт-Петербургского государственного университета телекоммуникаций им. проф. М. А. Бонч-Бруевича, podolyak.rs@gmail.com

ПОДОЛЬСКИЙ Дмитрий Анатольевич — инженер НОЦ «Медиацентр» Санкт-Петербургского государственного университета телекоммуникаций им. проф. М. А. Бонч-Бруевича, podolsky.dmitry94@gmail.com

ПОКРОВСКАЯ Вера Игоревна — аспирант кафедры конструирования и производства радиоэлектронных средств Санкт-Петербургского государственного университета телекоммуникаций им. проф. М. А. Бонч-Бруевича, panchenko_vera@bk.ru

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

ПОНОМАРЕВ Константин Дмитриевич — оператор научной роты Военной академии связи им. Маршала Советского Союза С. М. Буденного, kostapon@yandex.ru

ПОПОВ Леонид Геннадьевич — студент Санкт-Петербургского государственного университета телекоммуникаций им. проф. М. А. Бонч-Бруевича, leonidlitvinovo1994@mail.ru

ПРИКОТА Александр Валерьевич — ведущий специалист отдела программных технологий ООО «Эремекс», sasha303_75@mail.ru

ПРОТАСЕНЯ Сергей Витальевич — кандидат технических наук, доцент кафедры конструирования и производства радиоэлектронных средств Санкт-Петербургского государственного университета телекоммуникаций им. проф. М. А. Бонч-Бруевича, serj_p@pochta.ru

ПТИЦЫНА Лариса Константиновна — доктор технических наук, профессор, заведующая кафедрой информационных управляющих систем Санкт-Петербургского государственного университета телекоммуникаций им. проф. М. А. Бонч-Бруевича, ptitsina_lk@inbox.ru

РАЗУМОВ Александр Александрович — аспирант кафедры сетей связи и передачи данных Санкт-Петербургского государственного университета телекоммуникаций им. проф. М. А. Бонч-Бруевича, gagarn@bk.ru

РОГОЗИНСКИЙ Глеб Гендрихович — кандидат технических наук, руководитель направления аудиотехнологий НОЦ «Медиацентр» Санкт-Петербургского государственного университета телекоммуникаций им. проф. М. А. Бонч-Бруевича, gleb.rogozinsky@gmail.com

РУДНИЦКИЙ Валерий Борисович — кандидат технических наук, доцент фотоники и линий связи Санкт-Петербургского государственного университета телекоммуникаций им. проф. М. А. Бонч-Бруевича, mavvr2@mail.ru

РЫБАКОВ Алексей Игоревич — аспирант кафедры радиопередающих устройств и средств подвижной связи Санкт-Петербургского государственного университета телекоммуникаций им. проф. М. А. Бонч-Бруевича, lexeus.r1@gmail.com

РЫЖИКОВА Татьяна Аркадьевна — старший преподаватель кафедры конструирования и производства радиоэлектронных средств Санкт-Петербургского государственного университета телекоммуникаций им. проф. М. А. Бонч-Бруевича, t.rigikova@yandex.ru

РЯБОВА Ольга Николаевна — консультант Управления Роскомнадзора по СЗФО, ryabova2000@rambler.ru

САВЕЛЬЕВА Анастасия Андреевна — студентка Санкт-Петербургского государственного университета телекоммуникаций им. проф. М. А. Бонч-Бруевича, aasaveleva@yandex.ru

САВИЩЕНКО Николай Васильевич — доктор технических наук, профессор, профессор кафедры сетей связи и передачи информации Санкт-Петербургского государственного университета телекоммуникаций им. проф. М. А. Бонч-Бруевича, snikaspb@mail.ru

САФРОНОВ Юрий Алексеевич — оператор научной роты Военной академии связи им. Маршала Советского Союза С. М. Буденного, www.batel@mail.ru

САХАРОВ Дмитрий Владимирович — кандидат технических наук, доцент кафедры защищенных систем связи Санкт-Петербургского государственного университета телекоммуникаций им. проф. М. А. Бонч-Бруевича, руководитель Управления Роскомнадзора по СЗФО, D.Sakharov@rkn.gov.ru

СЕРГЕЕВ Алексей Николаевич — старший преподаватель кафедры фотоники и линий связи Санкт-Петербургского государственного университета телекоммуникаций им. проф. М. А. Бонч-Бруевича, a32@bk.ru,

СЕРДЮК Сергей Сергеевич — заместитель начальника отдела безопасности информации ФКУ НЦУКС МЧС России, s.s.serdyuk@mail.ru

СИМОНИНА Ольга Александровна — кандидат технических наук, доцент кафедры сетей связи и передачи данных Санкт-Петербургского государственного университета телекоммуникаций им. проф. М. А. Бонч-Бруевича, olga.simonina@spbgut.ru

СКОРОДУМОВ Сергей Андреевич — студент Санкт-Петербургского государственного университета телекоммуникаций им. проф. М. А. Бонч-Бруевича, serge.a.skor@mail.ru

СМИРНОВ Вениамин Васильевич — кандидат технических наук, профессор, доцент кафедры радиоэлектронных систем управления Балтийского государственного технического университета им Д. Ф. Устинова «ВОЕНМЕХ», leg1onner2007@gmail.com

СМИРНОВ Геннадий Михайлович — старший преподаватель кафедры фотоники и линий связи Санкт-Петербургского государственного университета телекоммуникаций им. проф. М. А. Бонч-Бруевича, smirnov_g@bk.ru

СТАРИКОВ Владимир Владимирович — аспирант кафедры радиопередающих устройств и средств подвижной связи Санкт-Петербургского государственного университета телекоммуникаций им. проф. М. А. Бонч-Бруевича, vl.vl.starikov@gmail.com

СТЕПАНОВ Андрей Борисович — кандидат технических наук, доцент кафедры радиосистем и обработки сигналов Санкт-Петербургского государственного университета телекоммуникаций им. проф. М. А. Бонч-Бруевича, dsp.sut@yandex.ru

СТЕПУТИН Антон Николаевич — кандидат технических наук, доцент кафедры радиосвязи и вещания Санкт-Петербургского государственного университета телекоммуникаций им. проф. М. А. Бонч-Бруевича, руководитель проекта 1234G.ru, steputin@1234G.ru

СУМКИН Владимир Радомирович — старший преподаватель кафедры фотоники и линий связи Санкт-Петербургского государственного университета телекоммуникаций им. проф. М. А. Бонч-Бруевича, sumkinv@mail.ru

СУНГАТУЛЛИН Эльдар Нурисламович — аспирант кафедры радиосвязи и вещания Санкт-Петербургского государственного университета телекоммуникаций им. проф. М. А. Бонч-Бруевича, sungeldar@mail.ru

ТИХОНОВ Сергей Владимирович — аспирант кафедры защищённых систем связи Санкт-Петербургского государственного университета телекоммуникаций им. проф. М. А. Бонч-Бруевича tikhonovc@yandex.ru

ТОКАРЕВА Маргарита Владимировна — студентка Санкт-Петербургского государственного университета телекоммуникаций им. проф. М. А. Бонч-Бруевича, margaret.7t@gmail.com

ТРЕЩИКОВ Владимир Николаевич — кандидат физико-математических наук, Генеральный директор ООО «Т8», info@t8.ru

ТУМАНОВА Евгения Ивановна — старший преподаватель кафедры телевидения и метрологии Санкт-Петербургского государственного университета телекоммуникаций им. проф. М. А. Бонч-Бруевича, evjeny@gmail.com

УДАЛЬЦОВ Александр Владимирович — помощник начальника учебно-методического отдела Военной академии связи им. Маршала Советского Союза С. М. Буденного, axil2003@yandex.ru

УЛЬЯНОВ Андрей Викторович — аспирант, ассистент кафедры сетей связи и передачи данных Санкт-Петербургского государственного университета телекоммуникаций им. проф. М. А. Бонч-Бруевича, ulyanov_av@spbgut.ru

УМИРОВ Ерлан Алимханович — магистрант кафедры сетей связи и передачи данных Санкт-Петербургского государственного университета телекоммуникаций им. проф. М. А. Бонч-Бруевича, umirov90@bk.ru

УСТИМЕНКО Вячеслав Михайлович — кандидат технических наук, профессор кафедры радиосвязи и вещания Санкт-Петербургского государственного университета телекоммуникаций им. проф. М. А. Бонч-Бруевича, ustimenko38@yandex.ru

УШАКОВ Игорь Александрович — старший преподаватель кафедры защищённых систем связи Санкт-Петербургского государственного университета телекоммуникаций им. проф. М. А. Бонч-Бруевича, ushakovia@gmail.com

ФЕДОРОВ Сергей Леонидович — кандидат технических наук, доцент кафедры телевидения и метрологии Санкт-Петербургского государственного университета телекоммуникаций им. проф. М. А. Бонч-Бруевича, sergf7@mail.ru

ФЕДОСЕЕВ Денис Олегович — кандидат технических наук, научный сотрудник Военной академии связи им. Маршала Советского Союза С. М. Буденного, matveykingv@gmail.com

ФИЦОВ Вадим Владленович — старший преподаватель кафедры инфокоммуникационных систем Санкт-Петербургского государственного университета телекоммуникаций им. проф. М. А. Бонч-Бруевича, noldi@bonch-ikt.ru

ФОКИН Григорий Алексеевич — кандидат технических наук, доцент кафедры радиосвязи и вещания Санкт-Петербургского государственного университета телекоммуникаций им. проф. М. А. Бонч-Бруевича, grihafokin@gmail.com

ХАБАЕВ Никита Сергеевич — магистрант кафедры инфокоммуникационных систем Санкт-Петербургского государственного университета телекоммуникаций им. проф. М. А. Бонч-Бруевича, n.xabaev@argustelecom.ru

ХОАНГ Лэ Чунг — аспирант кафедры сетей связи и передачи данных Санкт-Петербургского государственного университета телекоммуникаций им. проф. М. А. Бонч-Бруевича, hoangtrung.telecom@gmail.com

ХРАПОВА Елена Алексеевна — магистрант кафедры фотоники и линий связи Санкт-Петербургского государственного университета телекоммуникаций им. проф. М. А. Бонч-Бруевича, alena.xrapowa@yandex.ru

ХРИЧКОВ Валентин Александрович — преподаватель кафедры фотоники и линий связи Санкт-Петербургского государственного университета телекоммуникаций им. проф. М. А. Бонч-Бруевича, hrichkovv@gmail.com

ХУДОЕВ Иван Владимирович — аспирант кафедры сетей связи и передачи данных Санкт-Петербургского государственного университета телекоммуникаций им. проф. М. А. Бонч-Бруевича, khvanches@gmail.com

ЧАЙМАРДАНОВ Павел Александрович — аспирант кафедры фотоники и линий связи Санкт-Петербургского государственного университета телекоммуникаций им. проф. М. А. Бонч-Бруевича, pchai@yandex.ru

ЧЕЧУЛИН Андрей Алексеевич — кандидат технических наук, доцент кафедры защищённых систем связи Санкт-Петербургского государственного университета телекоммуникаций им. проф. М. А. Бонч-Бруевича, andreych@bk.ru

ШАХОБИДДИНОВ Алишер Шопатхиддинович — старший преподаватель кафедры систем телерадиовещания Ташкентского Университета информационных технологий, alishah@list.ru

ШТЕРЕНБЕРГ Станислав Игоревич — аспирант, ассистент кафедры защищенных систем связи Санкт-Петербургского государственного университета телекоммуникаций им. проф. М. А. Бонч-Бруевича, shterenberg.stanislaw@yandex.ru

ШУВАЛОВ Дмитрий Владимирович — аспирант кафедры радиосвязи и вещания Санкт-Петербургского государственного университета телекоммуникаций им. проф. М. А. Бонч-Бруевича, dmitryshuvalov@mail.ru

ЩЕКОЧИХИН Алексей Виктрович — аспирант, ассистент кафедры радиотехники и информационных технологий Санкт-Петербургского государственного института кино и телевидения, ashekochikhin@gmail.com

ЮРКИН Дмитрий Валерьевич — кандидат технических наук, доцент кафедры защищенных систем связи Санкт-Петербургского государственного университета телекоммуникаций им. проф. М. А. Бонч-Бруевича, dvyurkin@ya.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

ЯРОШЕНКО Александр Юрьевич — начальник отдела безопасности информации ФКУ НЦУКС МЧС России, a.yaroshenko@mchs.gov.ru

ЯСТРЕБОВ Егор Евгеньевич — студент группы СП-22 Санкт-Петербургского государственного университета телекоммуникаций им. проф. М. А. Бонч-Бруевича, astore.hawk@gmail.com

АВТОРСКИЙ УКАЗАТЕЛЬ

СПбГУТ ■ SPbSUT

АПИНО-2016

СБОРНИК НАУЧНЫХ СТАТЕЙ

ТОМ 1 VOL. 1

COLLECTION OF SCIENTIFIC PAPERS

ICAIT 2016

С.-ПЕТЕРБУРГ ■ 10-11.03.2016 ■ ST. PETERSBURG