ИНФОРМАЦИОННЫЕ ТЕХНОЛОГИИ И ТЕЛЕКОММУНИКАЦИИ

научное рецензируемое издание
электронный научный журнал
выпуск 4(12), 2015

TELECOM IT

electronic scientific journal
vol. 4(12)(2015)

СПб ГУТ)))

ISSN 2307-1303

ИНФОРМАЦИОННЫЕ ТЕХНОЛОГИИ И ТЕЛЕКОММУНИКАЦИИ

электронный научный журнал научное рецензируемое издание

TELECOM IT

electronic scientific journal

Учредитель и издатель федеральное государственное образовательное бюджетное учреждение высшего профессионального образования «Санкт-Петербургский государственный университет телекоммуникаций им. проф. М. А. Бонч-Бруевича» (СПбГУТ)

Адрес учредителя, издателя и редакции: С.-Петербург, пр. Большевиков д.22, корп.1, 193232

Электронное представительство журнала www.itt.sut.ru, e-mail: itt@spbgut.ru

Размещение журнала в РИНЦ (elibrary.ru) осуществляется по договору от 20 февраля 2013 года № 59-02/2013

Рукописи проходят редакционно-издательскую подготовку

Электронное издание. Цена свободная

Settler and publisher The Bonch-Bruevich Saint-Petersburg State University of Telecommunications

Address of the Settler and Publisher, Editorial Office: 193232, Russia, St-Petersburg, Prospekt Bolshevikov 22-1

Electronic representative of the Journal www.itt.sut.ru, e-mail: itt@spbgut.ru

The Journal is included in Russian Science Citation Index (www.elibrary.ru RINTS or Science index)

The electronic scientific journal has review institute

Free price

Редакционная коллегия

Баскин Л. М., д-р ф.-м. наук, профессор, СПбГУТ, Россия
Кучерявый Е. А., канд. техн. наук, PhD, senior member IEEE, профессор департамента электроники и коммуникаций, Технологический университет Тампере, Финляндия
Буйневич М. В., д-р техн. наук, профессор, СПбГУТ, Россия
Макаров В. В., д-р экон. наук, профессор, СПбГУТ, Россия
Машков Г. М., д-р техн. наук, профессор, СПбГУТ, Россия

Редакция

Бачевский С. В., главный редактор, д-р техн. наук, профессор
Кучерявый А. Е., заместитель главного редактора, д-р техн. наук, профессор
Владыко А. Г., заместитель главного редактора, канд. техн. наук, member IEEE
Минаков Л. М., ответственный секретарь, IT журнала
Аникевич Е. А., литературный редактор, канд. техн. наук
Аникевич Е. М., корректура, верстка

International Edition

Chilamkurti N., PhD, Senior Member of IEEE, La Trobe University, Australia
Giambene G., PhD, Senior Member of IEEE, University of Siena, Italy
Hosek J., PhD, Brno University of Technology, Czech Republic
Pignaton de Freitas E., PhD, The Federal University of Rio Grande do Sul, Brazil
Seilov Sh., Dr. Of Science, (Economics), president of Academy of infocommunications, Kazakhstan
Sudheer S. K., PhD, University of Kerala, India

Editorial Office

Bachevsky S., editor-In-chief, Dr. Of Science, (Eng-ing), professor
Koucheryavy A., deputy editor-In-chief, Dr. Of Science, (Eng-ing), professor
Vladyko A., CEO & Science Editor, Cand. Of Science, (Eng-ing)
Minakov L., COO & CIO
Anikevich E., literary editing, Cand. Of Science, (Eng-ing)
Anikevich E., proofreading, page proofs

Неисключительные права на все материалы, опубликованные в настоящем журнале принадлежат СПбГУТ. Воспроизведение, копирование, распространение возможно при наличии письменного разрешения от СПбГУТ. По вопросам приобретения неисключительных прав и использования журнала обращайтесь по тел. (812) 326-31-63, доб. 1388 или itt@spbgut.ru. Ссылка на первоисточник обязательна.

За достоверность сведений, изложенных в статьях, ответственность несут авторы публикаций. Мнение редакции может не совпадать с мнением авторов статей.

Минимальные системные требования для просмотра издания: тип компьютера, процессор, сопроцессор, частота: Pentium IV и выше или аналогичное; оперативная память (RAM): 256 Мб и выше; необходимо на винчестере: не менее 64 Мб; ОС MacOS, Windows (XP, Vista, 7) или аналогичное; видеосистема: встроенная; дополнительное ПО: Adobe Reader версия от 7.X или аналогичное. Защита от незаконного распространения: реализуется встроенными средствами Adobe Acrobat.

В оформлении обложки была использована иллюстрация, расположенная по адресу http://www.comandcom.ru/upload/iblock/ca1/ca1a50c8f734df83193fbcb4577df95f.jpg

Подписано в печать 01.10.2015.
Опубликовано на www.itt.sut.ru 30.10.2015.
Заказ № 019-ИТТ-2015. www.itt.sut.ru

© СПбГУТ
© Л. М. Минаков, оформление

СОДЕРЖАНИЕ

СИСТЕМЫ, СЕТИ И УСТРОЙСТВА ТЕЛЕКОММУНИКАЦИЙ

4 **Богданов И. А., Кучерявый А. Е.**
Ложные структуры в Интернете Вещей

11 **Былина М. С., Глаголев С. Ф.**
Расчет параметров передающего блока ВОСП, стабилизированного по мгновенному значению мощности

25 **Былина М. С., Чаймарданов П. А.**
Комплекс виртуальных лабораторных работ по исследованию параметров передачи кабельных цепей

40 **Воеводин Ю. В., Киричек Р. В.**
Обзор уникальных программно-аппаратных параметров различных технологий Интернета Вещей

48 **Данилов К. Н., Киричек Р. В., Кулик В. А.**
Методы обнаружения Интернет Вещей в глобальной сети

57 **Динь Ч. З., Киричек Р. В., Кучерявый А. Е., Парамонов А. И.**
Методы инсталляции сенсорных узлов с квадрокоптера общего пользования

67 **Киричек Р. В., Кулик В. А., Кучерявый А. Е.**
Программно-аппаратный комплекс для тестирования устройств Интернета Вещей

77 **Киричек Р. В., Нгуен Д. К., Герасимова Е. М.**
Сравнительный обзор технологии Li-Fi и перспектива практического использования для Интернета Вещей

87 **Киричек Р. В., Шилин П. А.**
Анализ использования БПЛА как узла сети VANET

97 **Мутханна А. С., Хакимов А. А.**
Сравнение протоколов WEB-вещей

СИСТЕМНЫЙ АНАЛИЗ, УПРАВЛЕНИЕ И ОБРАБОТКА ИНФОРМАЦИИ

108 **Владимиров С. С.**
Эффективность мажоритарного декодирования кода максимальной длины по k-элементным линейно-независимым комбинациям в двоичном симметричном канале

СИСТЕМЫ, СЕТИ И УСТРОЙСТВА ТЕЛЕКОММУНИКАЦИЙ

УДК 004.725.7

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

I. A. Bogdanov Bonch-Bruevich Saint-Petersburg State University of Telecommunication

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

A. E. Koucheryavy Bonch-Bruevich Saint-Petersburg State University of Telecommunication

ЛОЖНЫЕ СТРУКТУРЫ В ИНТЕРНЕТЕ ВЕЩЕЙ

FALSE STRUCTURES IN THE INTERNET OF THINGS

Реализация концепции Интернета Вещей выявила новые проблемы, возникающие при внедрении приложений Интернета Вещей. В основе этих проблем лежат следующие принципиальные положения концепции Интернета Вещей: чрезвычайно большое число вещей, требования по низкому энергопотреблению и ограниченные вычислительные ресурсы самих вещей. Эти принципиальные особенности сетей связи для приложений Интернета Вещей приводят к возможности создания ряда ложных структур, которые и являются предметом анализа статьи.

The special features of the Internet of Things (IoT) likely enormous number of things, energy consumption limitation, simplicity and cheapness of things are considered. The new types of intrusion to the IoT networks are analyzed. The false flows, the false clouds and networks cloning are investigated.

Интернет Вещей, ложные потоки, ложные облака, клонирование.

Internet of Things, false flows, false clouds, cloning.

Внедрение концепции Интернета Вещей [1–3] привело к пониманию новых особенностей сетей связи, которые проявляются и в архитектуре сети, и в моделях трафика, и в сетевой безопасности и т. д. Выделим следующие особенности концепции Интернета Вещей, которые оказывают непосредственное влияние на сетевую безопасность при ее внедрении.

Требования по низкому энергопотреблению для приложений Интернета Вещей, в первую очередь беспроводных сенсорных сетей, связаны как с тем, что число Интернет Вещей очень велико, так и с тем, что во многих

случаях электропитание, например сенсорных узлов, осуществляется за счет невозобновляемых источников энергии. Последнее определяет новую существенную проблему в области сетевой безопасности для приложений Интернета Вещей, а именно: проведение атак на энергетическую систему сетей связи с целью преднамеренного отъема энергии, например, у сенсорных узлов. С этой целью в [4, 5] предложено использовать потоки ложных событий.

Облачные технологии играют ключевую роль в архитектуре сетей при реализации концепции Интернета Вещей. Действительно, зачастую Интернет Вещи имеют ограниченные вычислительные возможности и использование облачных ресурсов является единственной возможностью эффективной организации сети. При этом передаваемые в облако данные могут представлять интерес для различного рода злоумышленников. Сетевая безопасность такой структуры в условиях повсеместного распространения облаков не может быть гарантирована по многим показателям, а наиболее современный подход, предложенный в [6], заключается в создании ложных облаков.

Понятие сетевой безопасности (network-based security) введено Сектором стандартизации телекоммуникаций Международного союза Электросвязи (МСЭ-Т). В соответствии с рекомендацией МСЭ-Т Y.2701 [7] для сетей связи следующего поколения NGN сетевая безопасность включает в себя:

- инфраструктуру провайдеров сетей и услуг и ее составляющие (например, сетевые элементы, системы, интерфейсы, данные, информацию), ресурсы и возможности (например, сигнализацию, управление, передачу трафика), предоставляемые провайдерами услуги;
- услуги и возможности сети NGN;
- информацию и связи конечного пользователя в сети (например, персональные данные).

Вместе с тем, в рекомендации подчеркивается, что безопасность пользовательских сетей (например, локальной сети) и безопасность при взаимодействии пользователей в одноранговых сетях (peer-to-peer) не являются предметом требований к безопасности в NGN.

Прогнозируемое чрезвычайно большое число интернет вещей требует самоорганизации при построении сетей. Кроме того, во многих приложениях концепции Интернета Вещей узлы таких сетей очень просты физически и имеют низкую стоимость. Поэтому еще одно направление создания ложных структур в сетях приложений Интернета Вещей – клонирование элементов таких сетей. Проблемы клонирования изучались, например, в [8].

На рис. 1 приведена классификация ложных структур при внедрении Интернета Вещей.

Рис. 1. Ложные структуры в Интернете Вещей

Потоки ложных событий

В таких моделях предполагается создание потоков ложных событий, которые должны воздействовать на сеть на сетевом уровне модели взаимодействия открытых систем [4, 5]. Ложное событие так же, как и легальное событие требует реакции от сенсорного узла, которая в данном случае выражается в детектировании события и формировании пакета информации для передачи информации о возникновении события либо для головного узла кластера, либо непосредственно от головного узла к шлюзу. Это требует дополнительного расхода энергии и уменьшает жизненный цикл сети. Имея информацию о реальных потоках событий, технически несложно создать подобные им потоки ложных событий. В последние годы все больше внимания в научных исследованиях уделяется беспроводным сенсорным сетям с мобильными узлами. Поэтому, указанные выше задачи должны быть решены как для беспроводных сенсорных сетей со стационарными узлами, так и с мобильными.

К настоящему разработана модель вторжения в беспроводную сенсорную сеть с целью уменьшения ее жизненного цикла с использованием потоков ложных событий. Модель разработана на основе типовых геометрических, количественных и энергетических параметров беспроводных сенсорных сетей с применением базового алгоритма кластеризации для гомогенной мобильной сенсорной сети при вторжении в сеть пуассоновского и детерминированного потоков ложных событий.

В процессе исследований выявлено также, что длительность жизненного цикла беспроводной сенсорной сети может существенно зависеть от вида потока ложных событий и при прочих равных условиях при воздействии детерминированного потока может быть почти в два раза меньше, чем при воздействии пуассоновского.

Кроме того, доказано, что остаточную энергию и длительность жизненного цикла беспроводной сенсорной сети при воздействии потоков ложных событий можно увеличить, если придать сенсорным узлам мо-

бильность со скоростью 2 м/с (типовая скорость, используемая в моделях для мобильных сенсорных сетей).

Разработана также модель для периметрического вторжения ложных потоков в пуассоновское сенсорное поле и получены результаты, не противоречащие предыдущим.

Ложные облака

Концепция и методы реализации ложных облаков представлены в [6]. Там же предложены и методы защиты от сбора информации со стороны ложных облаков. Для получения доступа к конфиденциальным данным, идущим от типовой интернет вещи к облаку, предложено использовать метод клонирования пакетов и их последующую отправку к дублирующему облаку (ложному облаку).

Для отправки данных в облако интернет вещь должна иметь подключение к точке доступа сети связи общего пользования. Перехват и перенаправление данных может быть реализован в непосредственной близости к каналу связи «интернет вещь – точка доступа».

Метод защиты от использования ложных облаков на базе применения алгоритмов гибридного шифрования (например, RSA-512 и AES-128) требует относительно больших вычислительных мощностей интернет вещи и не может быть реализован для вещей на базе микроконтроллеров, имеющих 8-и или 16-ти битную разрядность ЦПУ (например, AVR или ARM), а также для устройств с малым объемом памяти.

В предложен метод создания уникальных паттернов сетевого трафика интернет вещи, который может быть использован и для маломощных интернет вещей на базе микроконтроллера, и для более мощных вещей на базе микропроцессоров.

Клонирование сетей приложений Интернета Вещей

Миниатюрные размеры и низкая стоимость таких интернет вещей как сенсорные узлы, а также самоорганизация этих узлов в сеть, способствовали появлению новых методов вторжения в приложения Интернета Вещей, получивших название клонирования. Клонирование отдельных сенсорных узлов рассмотрено, например, в [8]. Однако для клонирования подходят не только отдельные узлы, но и сенсорные поля в целом, и их фрагменты. При этом могут быть определены два сценария клонирования. В первом (рис. 2) клонированная сеть или ее фрагменты располагаются непосредственно на территории сенсорного поля, а во втором сценарии клонированная сеть образует новое поле (рис. 3), располагающееся в непосредственной близости от легального сенсорного поля. Второй сценарий должен найти широкое применение для летающих сенсорных сетей [9, 10].

Рис. 2. Клонирование сенсорного поля или его фрагмента
на территории легального поля

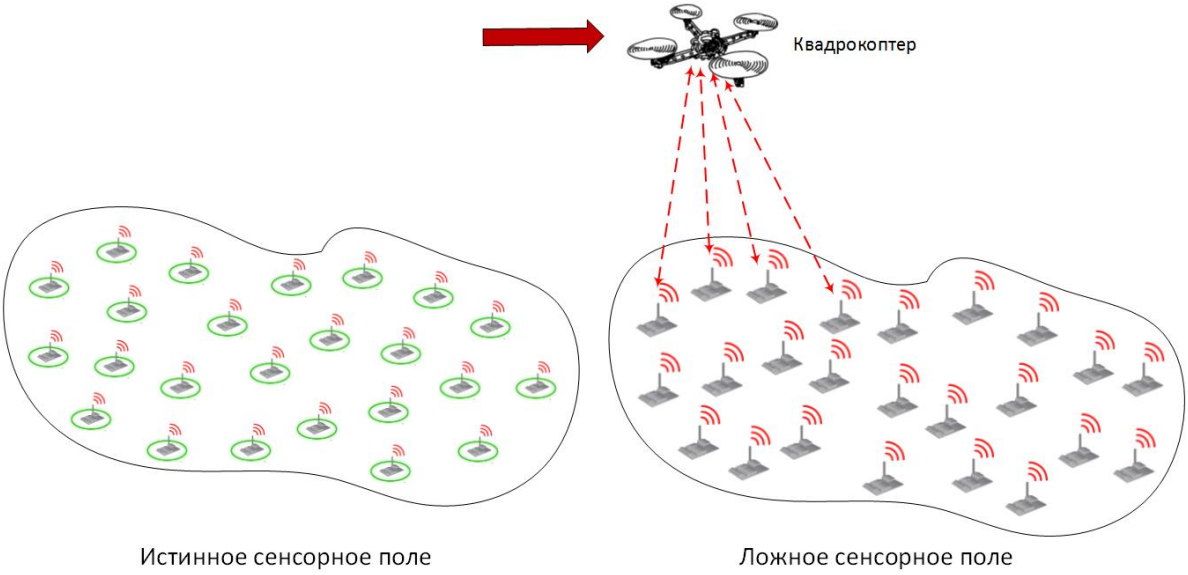


Рис. 3. Клонирование сенсорного поля или его фрагмента путем создания
клонированного поля в непосредственной близости от легального

Для выявления клонированных сенсорных полей или их фрагментов можно использовать характеристики трафика, циркулирующего в сети или, например, уже упоминавшийся метод создания уникальных паттернов.

Заключение

Принципиальные изменения, происходящие в сетях связи при внедрении приложений Интернета Вещей, приводят к появлению разнообразных ложных структур. В статье проведена классификация таких ложных структур, рассмотрено состояние исследований в области потоков ложных со-

бытий и ложных облаков, предложены новые способы клонирования в сенсорных сетях.

Библиографический список

1. **Кучерявый А. Е.** Самоорганизующиеся сети / А. Е. Кучерявый, А. Е. Прокопьев, Е. А. Кучерявый. – СПб. : Любавич, 2011. – 311 с.

2. **Кучерявый А. Е.** Интернет Вещей / А. Е. Кучерявый // Электросвязь. – 2013. – № 1. – С. 21–24.

3. **Kirichek R.** Internet of Things Laboratory Test Bed / R. Kirichek, A. Koucheryavy // International Conference on Wireless Communication, Networking and Application. WCNA 2014. – LNEE 978 – Heidelberg: Springer, 2016.

4. **Богданов И. А.** Характеристики жизненного цикла мобильной сенсорной сети при различных потоках ложных событий / И. А. Богданов, А. И. Парамонов, А. Е. Кучерявый // Электросвязь. – 2013. – № 1. – С. 32–33.

5. **Bogdanov I.** The mobile Sensor Network Life-Time under Different Spurious Flows Intrusion / I. Bogdanov, A. Koucheryavy, A. Paramonov // LNCS, Springer. 13 th NEW2AN, LNCS 8121, August, 2013.

6. **Киричек Р. В.** Ложные облака Интернета Вещей. Методы защиты / Р. В. Киричек, В. Кулик, А. Г. Владыко, И. А. Богданов, А. Е. Кучерявый // Информационные технологии и телекоммуникации. – 2015. – № 3 (11). – С. 27–39.

7. **Recommendation Y.2701.** Security Requirements for NGN Release 1. ITU-T, Geneva, April 2007.

8. **Bhattasali T.** A Survey of Recent Intrusion Detection Systems in Wireless Sensor Networks. Advanced in Network Security and Applications / T. Bhattasali, R. Chaki // Conference Proceedings of Fourth International Conference on Network security and Applications (CNSA 2011), Chennai, India, July 15–17, 2011.

9. **Кучерявый А. Е.** Теоретические и практические направления исследований в области летающих сенсорных сетей / А. Е. Кучерявый, А. Г. Владыко, Р. В. Киричек // Электросвязь. – 2015. – № 7. – С. 9–11.

10. **Koucheryavy A.** State of the Art and Research Challenges for Public Flying Ubiquitous Sensor Networks / A. Koucheryavy, A. Vladyko, R. Kirichek // Internet of Things, Smart Spaces, and Next Generation Networks and Systems / Ed. by S. Balandin, S. Andreev, Y. Koucheryavy. – Springer International Publishing Switzerland. – 2015, LNCS. – Vol. 9247. – PP. 299–308.

References

1. **Kucherjavyj A. E.** Samoorganizujushhiesja seti / A. E. Kucherjavyj, A. E. Prokop'ev, E. A. Kucherjavyj. – SPb. : Ljubavich, 2011. – 311 s.

2. **Kucherjavyj A. E.** Internet Veshhej / A. E. Kucherjavyj // Jelektrosvjaz'. – 2013. – № 1. – S. 21–24.

3. **Kirichek R.** Internet of Things Laboratory Test Bed / R. Kirichek, A. Koucheryavy // International Conference on Wireless Communication, Networking and Application. WCNA 2014. – LNEE 978 – Heidelberg: Springer, 2016.

4. **Bogdanov I. A.** Harakteristiki zhiznennogo cikla mobil'noj sensornoj seti pri razlichnyh potokah lozhnyh sobytij / I. A. Bogdanov, A. I. Paramonov, A. E. Kucherjavyj // Jelektrosvjaz'. – 2013. – № 1. – S. 32–33.

5. **Bogdanov I.** The mobile Sensor Network Life-Time under Different Spu-rious Flows Intrusion / I. Bogdanov, A. Koucheryavy, A. Paramonov // LNCS, Springer. 13 th NEW2AN, LNCS 8121, August, 2013.

6. **Kirichek R. V.** Lozhnye oblaka Interneta Veshhej. Metody zashhity / R. V. Kirichek, V. Kulik, A. G. Vladyko, I. A. Bogdanov, A. E. Kucherjavyj // Informacionnye tehnologii i telekommunika-cii. – 2015. – № 3 (11). – S. 27–39.

7. **Recommendation Y.2701.** Security Requirements for NGN Release 1. ITU-T, Geneva, April 2007.

8. **Bhattasali T.** A Survey of Recent Intrusion Detection Systems in Wireless Sensor Networks. Advanced in Network Security and Applications / T. Bhattasali, R. Chaki // Conference Proceedings of Fourth International Conference on Network security and Applications (CNSA 2011), Chen-nai, India, July 15–17, 2011.

9. **Kucherjavyj A. E.** Teoreticheskie i prakticheskie napravlenija issle-dovanij v oblasti letajushhih sensornyh setej / A. E. Kucherjavyj, A. G. Vladyko, R. V. Kirichek // Jelektrosvjaz'. – 2015. – № 7. – S. 9–11.

10. **Koucheryavy A.** State of the Art and Research Challenges for Public Flying Ubiquitous Sensor Networks / A. Koucheryavy, A. Vladyko, R. Kirichek // Internet of Things, Smart Spaces, and Next Generation Networks and Systems / Ed. by S. Balandin, S. Andreev, Y. Koucheryavy. – Springer International Publishing Switzerland. – 2015, LNCS. – Vol. 9247. – PP. 299–308.

Кучерявый Андрей Евгеньевич – доктор технических наук, профессор, заведующий кафедрой «Сети связи и передача данных» Федерального государственного бюджетного образовательного учреждения высшего образования «Санкт-Петербургский государственный университет телекоммуникаций им. проф. М. А. Бонч-Бруевича», akouch@mail.ru

Богданов Игорь Александрович – аспирант кафедры «Сети связи и передача данных» Федерального государственного бюджетного образовательного учреждения высшего «Санкт-Петербургский государственный университет телекоммуникаций им. проф. М. А. Бонч-Бруевича»,igorek.b@mail.ru

УДК 681.7.069

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

M. S. Bylina Bonch-Bruevich Saint-Petersburg State University of Telecommunication

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

S. F. Glagolev Bonch-Bruevich Saint-Petersburg State University of Telecommunication

РАСЧЕТ ПАРАМЕТРОВ ПЕРЕДАЮЩЕГО БЛОКА ВОСП, СТАБИЛИЗИРОВАННОГО ПО МГНОВЕННОМУ ЗНАЧЕНИЮ МОЩНОСТИ

CALCULATION PARAMETERS ARE PASSED BLOCK FOTS, STABLE ON INSTANTANEOUS VALUES POWER

Рассмотрены структурная и принципиальная схемы оптического передающего блока (ОПБ) с прямой модуляцией лазерного диода по интенсивности, стабилизированного по мгновенному значению излучаемой мощности и предназначенного для волоконно-оптической системы передачи (ВОСП) со скоростью менее 2,5 Гбит/с. Предложены критерии выбора элементной базы ОПБ, математические выражения и последовательность расчета параметров ОПБ. Содержание статьи может быть полезно разработчикам элементов ВОСП, а также студентам, обучающимся по направлению «Инфокоммуникационные технологии и системы связи».

The structural and schematic diagram of an optical transmitter unit (OTU) direct modulation laser diode intensity stabilized by the instantaneous value of radiated power and designed for fiber-optic transmission system (FOTS) at a rate of less than 2,5 Gbit / s. The criteria of selection of the element base OTU, mathematical expressions and sequence-of calculating the parameters of the OTU. The content of the article can be useful to developers FOTS elements, as well as students studying the direction of "Information and Communication Technologies and Communication."

волоконно-оптическая система передачи (ВОСП), оптический передающий блок (ОПБ) ВОСП, источник излучения, модуляция по интенсивности, система стабилизации оптической мощности, операционный усилитель.

fiber-optic transmission system (FOTS), optical transmitter unit (OTU) FOTS, a radiation source, the intensity modulation, optical power stabilization system, an operational amplifier.

Введение

Целью работы является создание методики расчета стабилизированного по мощности оптического передающего блока (ОПБ) с прямой моду-

ляцией лазерного диода (ЛД) для волоконно-оптической системы передачи (ВОСП).

Структурная схема стабилизированного по мощности передающего устройства

На рис. 1 показана структурная схема ОПБ с системой стабилизации мощности (ССМ).

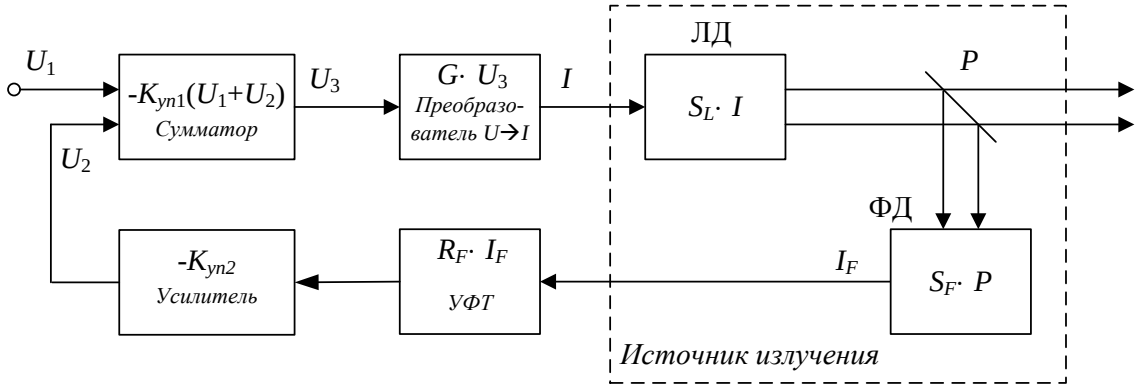


Рис. 1. Структурная схема ОПБ с ССМ

Основным элементом ОПБ является ЛД со встроенным контрольным фотодиодом (ФД).

Ток накачки для ЛД создает преобразователь напряжения U_3 в ток I, который имеет коэффициент преобразования G с размерностью проводимости. Выходная оптическая мощность P в первом приближении пропорциональна току накачки.

$$P = S_L I = S_L G U_3, \tag{1}$$

где S_L – коэффициент преобразования ЛД.

Ток ФД повторяет изменения оптической мощности ЛД и с помощью трансимпедансного усилителя фототока (УФТ) и усилителя напряжения с коэффициентом $K_{уп2}$ преобразуется в напряжение U_2, пропорциональное P:

$$U_2 = -S_F R_F K_{уп2} P, \tag{2}$$

где S_F – чувствительность контрольного ФД, с учетом доли оптической мощности, поступающей на него;

R_F – коэффициент преобразования УФТ.

Форму и частоту изменений выходной оптической мощности P задает напряжение U_1, которое суммируется в усилителе-сумматоре с коэффициентом $K_{уп1}$ с напряжением отрицательной обратной связи (ООС) U_2, кото-

рое повторяет реальные изменения P, но имеет обратный знак (фазу) по отношению к U_1. Обычно можно считать, что $U_1 \approx U_2$.

В рассматриваемом передающем блоке используется прямая модуляция ИИ по интенсивности двоичным кодом с возвратом (RZ) и без возврата (NRZ) к 0 (рис. 2).

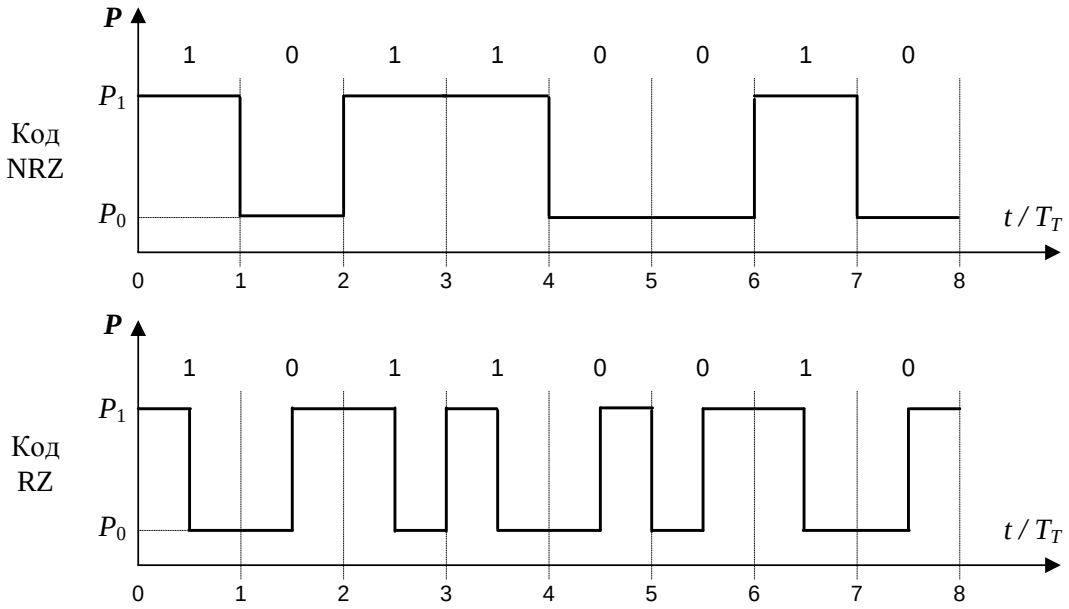


Рис. 2. Упрощенная форма сигнала на выходе передающего устройства при передаче двоичных сигналов с модуляцией по интенсивности с кодами NRZ и RZ

При равной вероятности 0 и 1 среднее значение излучаемой мощности будет одинаковым для кодов RZ и NRZ

$$\bar{P} = (P_1 + P_0)/2 = P_1\,(1 + 1/k_{ext})/2, \qquad (3)$$

где P_1 и P_0 – мощности, соответствующие передаче логической 1 и 0, соответственно;

$k_{ext} = P_1 / P_0$ – коэффициент экстинкции, который определяется рекомендациями Международного союза электросвязи для различных типов ВОСП.

С учетом ООС для мощности оптического излучения на выходе передающего блока можно получить выражение

$$P = \frac{U_1 K_{yn1} G S_L}{1 + K_{yn1} K_{yn2} G S_L S_F R_F}. \qquad (4)$$

Величину $A_0 = K_{yn1} K_{yn2} G S_L S_F R_F$ называют величиной петлевого усиления. Если A_0 >> 1 выражение (3) можно представить в виде:

$$P = \frac{U_1 K_{yn1} G S_L}{1+\mathrm{A}_0} \approx \frac{U_1 K_{yn1} G S_L}{\mathrm{A}_0} = \frac{U_1}{K_{yn2} S_F R_F}. \quad (5)$$

Из (5) видно, что ООС с большой величиной петлевого усиления подавляет изменения выходной оптической мощности P, связанные с изменением произведения K_{yn1} G S_L. Самым нестабильным элементом является ЛД. Его коэффициент преобразования S_L значительно изменяется под действием окружающих условий и старения. Параметры K_{yn1} и G относятся к числу стабильных и мало изменяются под действием температуры и времени. Выходная мощность определяется входным напряжением U_1 и произведением стабильных параметров $K_{yn2} S_F R_F$. Для обеспечения необходимой стабильности величину петлевого усиления выбирают в пределах 50–200.

Остаточную нестабильность выходной мощности при изменении параметра S_L можно определить по выражению

$$\frac{\Delta P}{P} = \frac{\Delta S_L}{S_L \cdot A_0}, \quad (6)$$

Выражения (1)–(5) являются приближенными. При более строгом анализе структурной схемы необходимо учитывать нелинейность модуляционной и вольтамперной характеристик ЛД, инерционные свойства ЛД, ФД и входящих в структурную схему операционных усилителей, на которых строятся все блоки структурной схемы.

Далее в работе получены более строгие расчетные выражения с учетом следующих допущений: модуляционная характеристика ЛД линейна и характеризуется коэффициентом преобразования S_L; быстродействие ЛД определяется его эквивалентной постоянной времени τ_L; все операционные усилители одинаковы, они характеризуются коэффициентом усиления K_y и постоянной времени τ_y; быстродействие ФД определяется его эквивалентной емкостью C_F.

Параметры источников излучения

К характеристикам и параметрам ЛД относятся вольтамперная (ВАХ), и ваттамперная (ВтАХ) характеристики, средняя длина волны излучения, максимальная рассеиваемая в ИИ мощность, постоянная времени нарастания/спада τ_L выходной оптической мощности при ступенчатом изменении тока накачки.

Одним из основных параметров источника излучения является средняя длина волны излучения λ. В расчетах следует учитывать зависимость λ от температуры:

$$\lambda = \lambda_0 + \delta\lambda_T (T - T_0), \quad (7)$$

где T_0 – температура перехода, К, при которой длина волны излучения равна λ_0, нм;

$\delta\lambda_T$ – коэффициент, учитывающий изменение длины волны с изменением температуры, нм/К.

Как элемент электрической цепи ЛД представляет собой прямо смещенный *p-n* переход и характеризуется ВАХ, то есть зависимостью тока через переход (тока накачки) от напряжения на переходе

$$I = I_{0T} \cdot \left[exp\left(\frac{U \cdot e}{k \cdot T \cdot m}\right) - 1\right] = I_{0T} \cdot \left[exp\left(\frac{U}{\varphi_T \cdot m}\right) - 1\right], \quad (8)$$

где I_{0T} – тепловой обратный ток;

$\varphi_T = kT / e$ – температурный потенциал;

$e = 1{,}6 \cdot 10^{-19}$ Кл – заряд электрона;

$k = 1{,}38 \cdot 10^{-23}$ Дж/К – постоянная Больцмана;

T – абсолютная температура, К;

m – коэффициент рекомбинации, зависящий от электрофизических свойств полупроводника (для ЛД InGaAsP/InP $m = 3$).

Ток I_{0T} называют тепловым обратным током в соответствии с механизмом его образования и сильной зависимостью от температуры. Функцию $I_{0T}(T)$ характеризуют величиной ΔT_y – приращением температуры, вызывающим удвоение тока:

$$\Delta T_y = \frac{k \cdot T_0^2}{h \cdot \nu} \ln 2, \quad (9)$$

где T_0 – средняя температура перехода, К;

ν – частота излучения ИИ. Для заданной температуры T тепловой ток

$$I_{0T}(T) = I_{0T}(T_0) \cdot 2^{(T - T_0)/\Delta T_y}. \quad (10)$$

Для примера на рис. 3а показано семейство ВАХ *p-n* перехода для трех температур 280, 300 и 320 К при следующих исходных данных: $\lambda_0 = 1660$ нм, $I_{0T}(T_0) = 30$ нА, $\delta\lambda_T = 0.2$ нм/К.

Электрическую мощность, рассеиваемую в *p-n* переходе ЛД при протекании по нему тока накачки I можно рассчитать по выражению:

$$P_{el} = I \cdot U = \frac{k \cdot T \cdot m \cdot I}{e} ln\left(\frac{I}{I_{0T}} + 1\right). \quad (11)$$

На рис. 3б показано семейство зависимостей P_{el} от тока накачки.

Задаваясь максимально допустимой средней мощностью, рассеиваемой на ЛД, равной, например, 150 мВт, определим по рис. 3б максимальный (при температуре 320 К) и минимальный (при температуре 280 К)

средние токи накачки. Они составляют 135 мА и 120 мА, что соответствует изменениям напряжения на ЛД от 1,1 В (T = 320 К) до 1,25 В (T = 280 К). Основной характеристикой ЛД при прямой модуляции излучения по интенсивности является модуляционная (ВтАХ) характеристика, то есть зависимость излучаемой мощности от тока накачки I (прямого тока через p-n переход), которую для ЛД можно аппроксимировать следующими выражениями

$$P = \begin{cases} S_0 \cdot I & при\ I \le I_{pr} \\ S_0 \cdot I_{pr} + S_1 \cdot (I - I_{pr}) - S_2 \cdot (I - I_{pr})^2 & при\ I > I_{pr} \end{cases}, \quad (12)$$

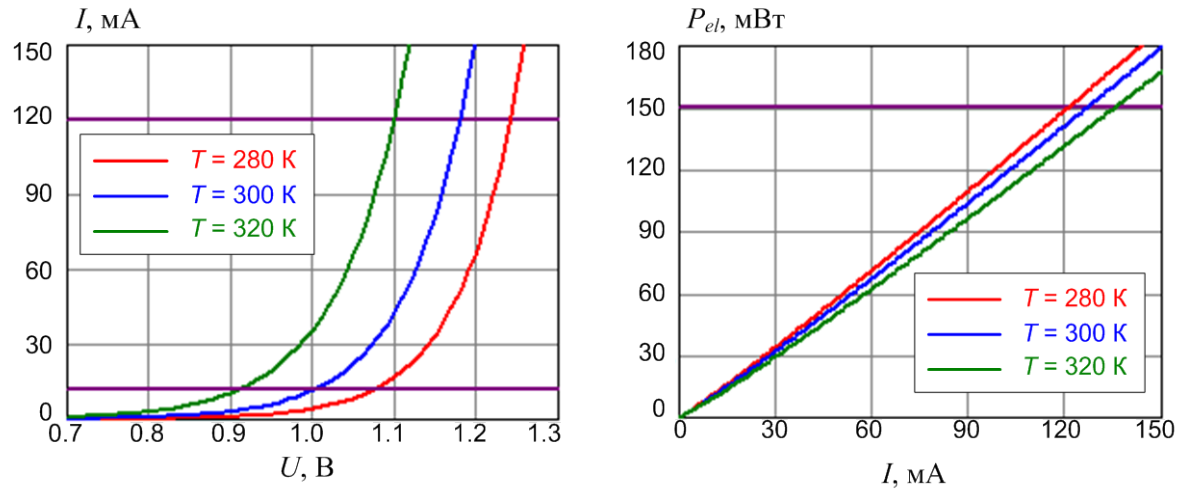
где S_0, S_1 и S_2 – коэффициенты, характеризующие модуляционную характеристику ЛД;

I_{pr} – пороговый ток ЛД, который существенно зависит от температуры:

$$I_{pr} = I_{prx} \cdot exp[(T - T_x)/T_x], \quad (13)$$

где T_x – характеристическая температура, которая составляет 50–70 К для ЛД InGaAsP/InP (λ = 1,3–1,55 мкм);

I_{prx} – пороговый ток при температуре T_x.



а *б*

Рис. 3. Вольтамперные характеристики ЛД (а)
и зависимость рассеиваемой в ЛД мощности от тока накачки (б)

В расчетах следует учитывать зависимость S_1 от температуры:

$$S_1 = S_{10} + \delta S_{1T}(T - T_0), \quad (14)$$

где T_0 –температура перехода, К, при которой $S_1 = S_{10}$;

δS_{1T} – коэффициент, учитывающий изменение S_1 с изменением температуры, мВт/(мА·К).

Для примера на рис. 4 показаны результаты расчетов зависимостей выходной мощности от тока накачки при различных значениях температуры по выражению (11) с учетом (12) и (13) при следующих исходных данных: S_0 = 0,0075 мВт/мА, S_1 = 0,325 мВт/мА, S_2 = 0,0012 мВт/мА^2, I_{prx} = 0,15 мА, T_x = 60 К, δS_{1T} = –0,001 мВт/(мА·К).

Из рис. 4 следует, что при температуре 320 К максимальная мощность составляет 19 мВт. Выберем эту мощность в качестве номинальной, которую мы и будем стабилизировать. Ток накачки будет изменяться от 90 (T = 280 K) до 160 (T = 320 K) мА.

Определим также среднюю крутизну преобразования в ЛД тока в оптическую мощность S_L, которая лежит в пределах от 0,15 (T = 320 K) до 0,29 (T = 280 K) мВт/мА. Среднее значение крутизны преобразования для дальнейших расчетов можно принять равным $\bar{S}_L = 0{,}22$ мВт/мА.

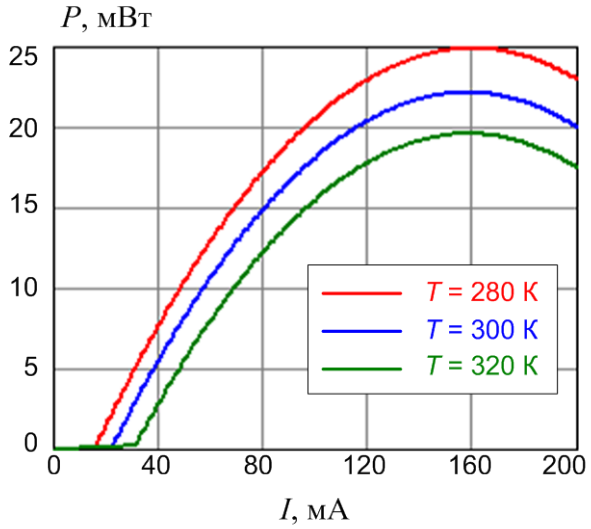


Рис. 4. Семейство модуляционных характеристик ЛД

Оценим коэффициент полезного действия (КПД) ИИ, который определим, как отношение излучаемой оптической мощности к потребляемой. Он лежит в пределах от 15 до 18 %.

Преобразователь напряжения в ток накачки и оптическую мощность

Принципиальная и эквивалентная схемы подключения ЛД к преобразователю напряжения в ток накачки показаны на рис. 5.

Анализ схемы позволил получить выражение для коэффициента передачи схемы в комплексной форме и его модуля

$$K_1(j\omega) = \frac{P(j\omega)}{U_3(j\omega)} = \frac{S_L}{R_L \cdot \frac{1+K_y}{K_y} \cdot \left(1 - \omega^2 \cdot \frac{\tau_y \cdot \tau_L}{1+K_y} + j\omega \cdot \left(\tau_L + \frac{\tau_y}{1+K_y}\right)\right)}, \quad (15)$$

$$K_1(\omega) = \frac{P(\omega)}{U_3(\omega)} = \frac{S_L}{R_L \cdot \frac{1+K_y}{K_y} \cdot \sqrt{\left(1 - \omega^2 \cdot \frac{\tau_y \cdot \tau_L}{1+K_y}\right)^2 + \omega^2 \cdot \left(\tau_L + \frac{\tau_y}{1+K_y}\right)^2}}. \quad (16)$$

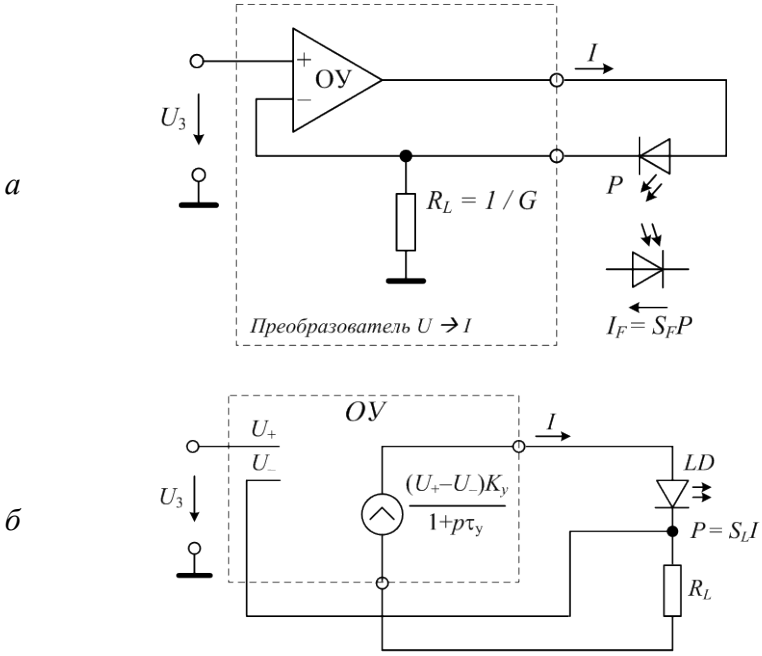


Рис. 5. Принципиальная (а)
и эквивалентная (б) схемы преобразователя напряжения в ток накачки

На рис. 6 представлены результаты расчета АЧХ преобразователя напряжения в ток накачки. Расчет проведен по выражению (16) при следующих параметрах: S_L = 0,22 Вт/А, τ_L = 5 нс, K_y = 5000, τ_y = 2,5 нс, R_L = 10 Ом.

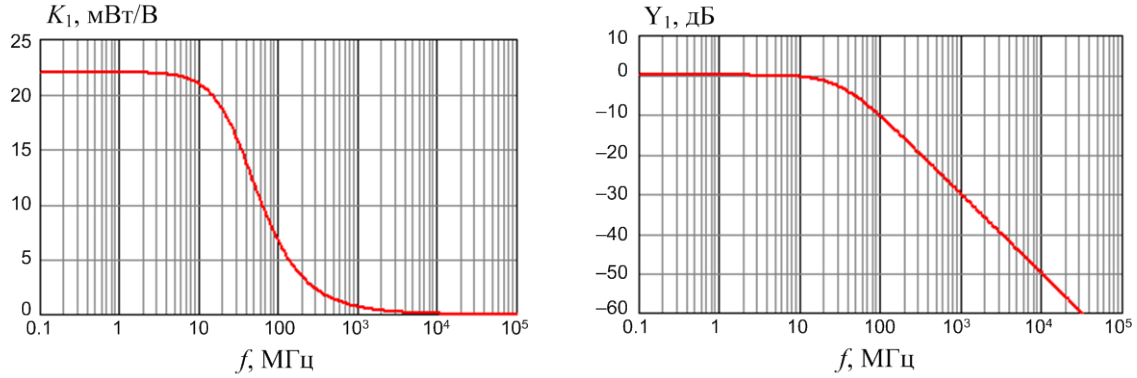
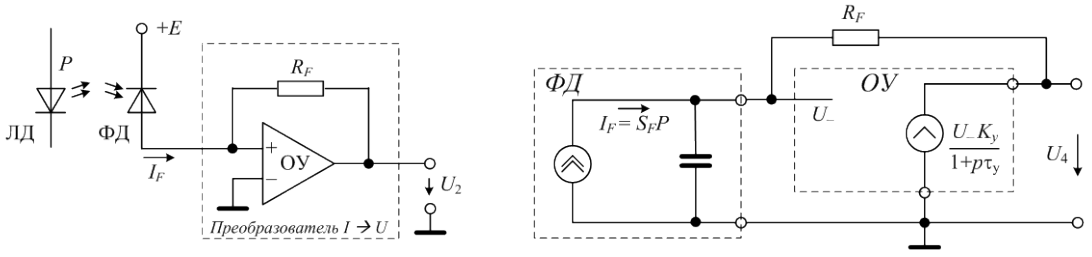


Рис. 6. АЧХ преобразователя напряжения в ток накачки вместе с ЛД в линейном (а)
и логарифмическом (б) масштабах

Преобразователь оптической мощности в напряжение

Величина фототока I_F контрольного ФД пропорциональна этой мощности и преобразуется в напряжение U_2 с помощью УФТ. Принципиальная и эквивалентная схемы подключения ФД к УФТ показаны на рис. 7.



а *б*

Рис. 7. Упрощенная принципиальная схема подключения контрольного ФД к УФТ (а) и ее эквивалентная схема (б)

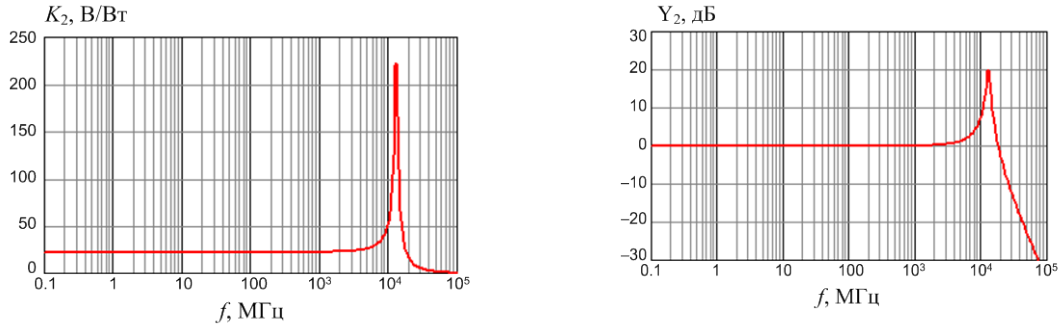
Анализ схемы позволил получить выражение для коэффициента передачи схемы в комплексной форме и его модуля

$$K_2(j\omega) = \frac{U_2(j\omega)}{P(j\omega)} = \frac{-S_F \cdot R_F}{\frac{K_y+1}{K_y} \cdot \left[1 - \frac{\omega^2 \cdot R_F C_F \cdot \tau_y}{K_y+1} + \frac{j\omega \cdot (R_F C_F + \tau_y)}{K_y+1}\right]}, \quad (17)$$

$$K_2(\omega) = \frac{U_2(\omega)}{P(\omega)} = \frac{S_F \cdot R_F}{\frac{K_y+1}{K_y} \cdot \sqrt{\left(1 - \frac{\omega^2 \cdot R_F C_F \cdot \tau_y}{K_y+1}\right)^2 + \omega^2 \cdot \left(\frac{R_F C_F + \tau_y}{K_y+1}\right)^2}}. \quad (18)$$

На рис. 8 представлены результаты расчета АЧХ цепи ООС. Расчет проведен по выражению (18) при следующих параметрах: S_F = 0,075 А/Вт, C_F = 0,5 нФ, R_F = 300 Ом, K_y = 5000, τ_y = 2,5 нс.

Из рис. 8 видно, что на частоте примерно 1,5 ГГц имеет место значительный выброс на АЧХ УФТ, который возрастает с увеличением сопротивления R_F.



а *б*

Рис. 8. АЧХ преобразователя фототока в напряжение вместе с ФД в линейном (а) и логарифмическом (б) масштабах

Для обеспечения необходимого напряжения $U_2 = U_1 \approx 1$ В на выходе цепи ООС используется дополнительный инвертирующий усилитель напряжения, схема которого аналогична схеме усилителя сумматора, но с другими значениями сопротивлений R_1 и R_2. Его расчет проведен ниже.

Усилитель сумматор и дополнительный усилитель

Для замыкания петли ООС системы стабилизации оптической мощности используется усилитель-сумматор сигналов U_1 и U_2 с коэффициентом усиления

$$K_{yn} = -R_2/R_1. \tag{19}$$

Принципиальная и эквивалентная схемы усилителя-сумматора показаны на рис. 9.

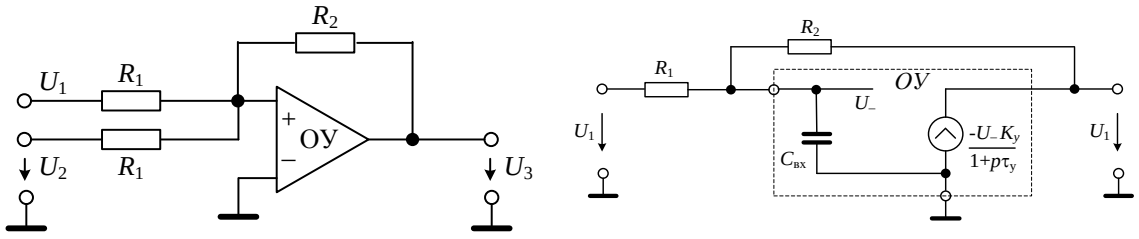


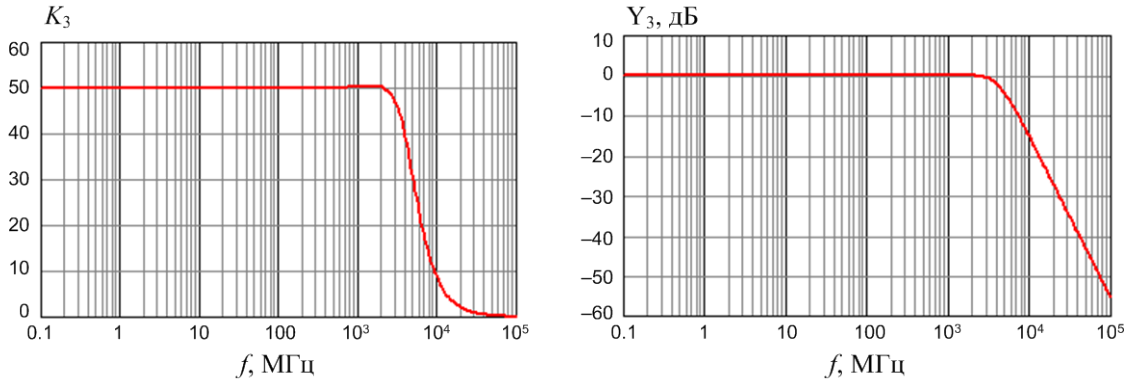
Рис. 9. Принципиальная (а) и эквивалентная (б) схемы усилителя-сумматора

Анализ схемы позволил получить выражение для коэффициента передачи усилителя-сумматора в комплексной форме и для модуля

$$K_3(j\omega) = \frac{U_3(j\omega)}{U_1(j\omega)} = \frac{-K_{yn1}}{1-\omega^2 \cdot \frac{C_{bx}R_2 \cdot \tau_y}{1+K_{yn1}+K_y} + j\omega \cdot \frac{C_{bx}R_2+(1+K_{yn1})\tau_y}{1+K_{yn1}+K_y}}, \tag{20}$$

$$K_3(\omega) = \frac{U_3(\omega)}{U_1(\omega)} = \frac{K_{yn1}}{\sqrt{\left(1-\omega^2 \cdot \frac{C_{bx}R_2 \cdot \tau_y}{1+K_{yn1}+K_y}\right)^2 + \left[\omega \cdot \frac{C_{bx}R_2+(1+K_{yn1})\tau_y}{1+K_{yn1}+K_y}\right]^2}}. \tag{21}$$

На рис. 10 представлены результаты расчета АЧХ усилителя-сумматора. Расчет проведен по выражению (21) при следующих параметрах: C_{bx} = 0,3 пФ, R_2 = 5000 Ом, K_{yn1} = 50, K_y = 5000, τ_y = 2,5 нс.



а *б*

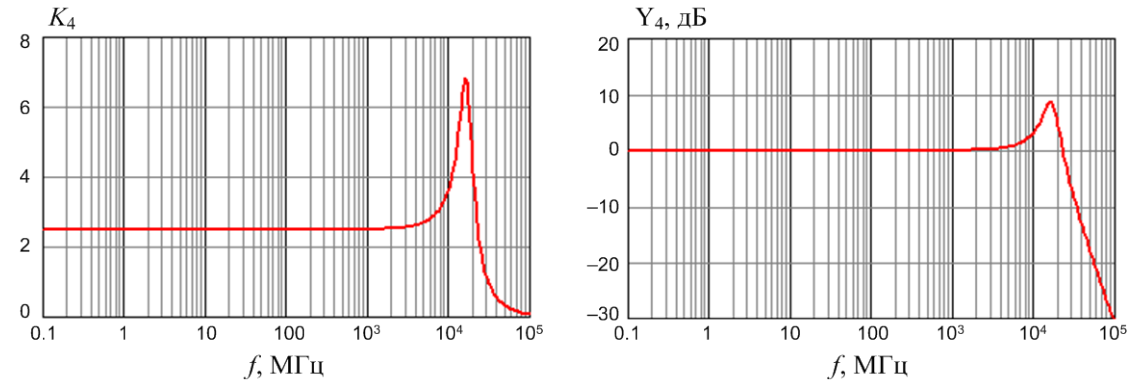
Рис. 10. АЧХ усилителя-сумматора в линейном (а) и логарифмическом (б) масштабах

Проведем расчет дополнительного усилителя напряжения в цепи ООС. Его схема аналогична схеме, представленной на рис. 9, а расчетные выражения аналогичны выражениям (20) и (21):

$$K_4(j\omega) = \frac{U_2(j\omega)}{U_4(j\omega)} = \frac{-K_{yn2}}{1-\omega^2 \cdot \frac{C_{bx}R_2 \cdot \tau_y}{1+K_{yn2}+K_y} + j\omega \cdot \frac{C_{bx}R_2+(1+K_{yn2})\tau_y}{1+K_{yn2}+K_y}}, \quad (22)$$

$$K_4(\omega) = \frac{U_2(\omega)}{U_4(\omega)} = \frac{K_{yn2}}{\sqrt{\left(1-\omega^2 \cdot \frac{C_{bx}R_2 \cdot \tau_y}{1+K_{yn2}+K_y}\right)^2 + \left[\omega \cdot \frac{C_{bx}R_2+(1+K_{yn2})\tau_y}{1+K_{yn2}+K_y}\right]^2}}, \quad (23)$$

На рис. 11 представлены результаты расчета АЧХ дополнительного усилителя. Расчет проведен по выражению (23) при следующих параметрах: R_2 = 1000 Ом, K_{yn2} = 2,5, K_y = 5000, τ_y = 2,5 нс.



а *б*

Рис. 11. АЧХ дополнительного усилителя в линейном (а)
и логарифмическом (б) масштабах

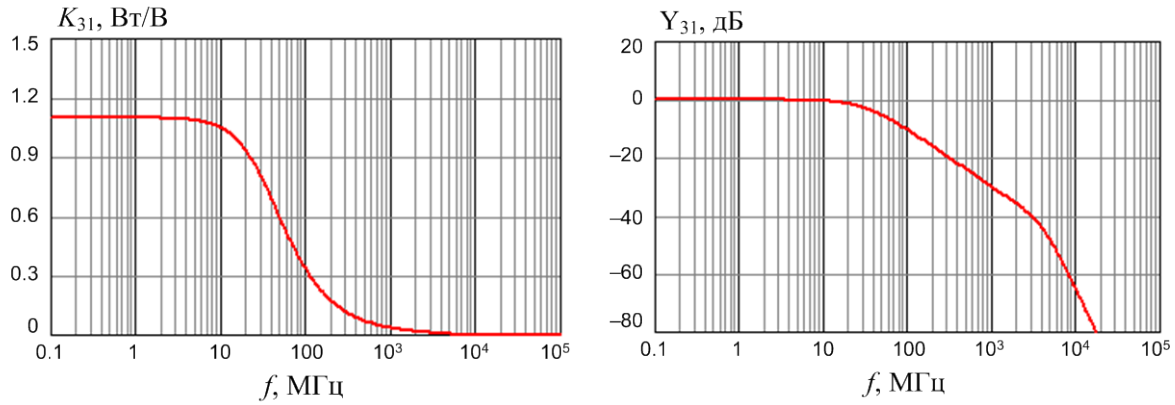
Параметры прямой ветви и петлевого усиления

Определим комплексный коэффициент передачи прямой ветви системы стабилизации оптической мощности и его модуль

$$K_{31}(j\omega) = \frac{P(j\omega)}{U_1(j\omega)} = K_3(j\omega)K_1(j\omega), \quad (24)$$

$$K_{31}(\omega) = \frac{P(\omega)}{U_1(\omega)} = K_3(\omega)K_1(\omega). \quad (25)$$

На рис. 12 показаны АЧХ прямой ветви ССМ, рассчитанные по выражению (25).



а *б*

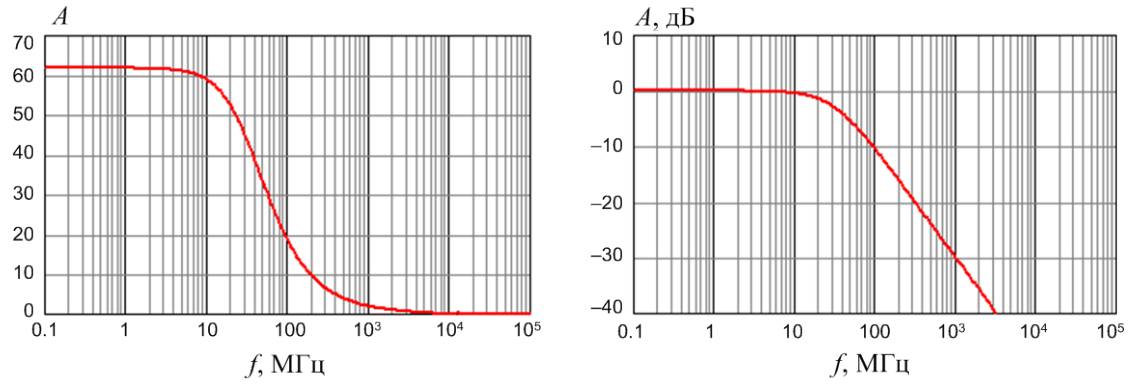
Рис. 12. АЧХ прямой ветви системы стабилизации оптической мощности в линейном (а) и логарифмическом (б) масштабах

Определим комплексный коэффициент всех элементов ССМ (петлевой коэффициент передачи)

$$A(j\omega) = \frac{U_2(j\omega)}{U_1(j\omega)} = K_3(j\omega)K_1(j\omega)K_2(j\omega)K_4(j\omega), \quad (26)$$

$$A(\omega) = \frac{U_2(\omega)}{U_1(\omega)} = K_3(\omega)K_1(\omega)K_2(\omega)K_4(j\omega). \quad (27)$$

На рис. 13 показана АЧХ петлевого коэффициента передачи ССМ, рассчитанная по выражению (27).



а *б*

Рис. 13. АЧХ петлевого усиления ССМ в линейном (а)
и логарифмическом (б) масштабах

Определим комплексный коэффициент передачи замкнутой системы стабилизации оптической мощности и его модуль

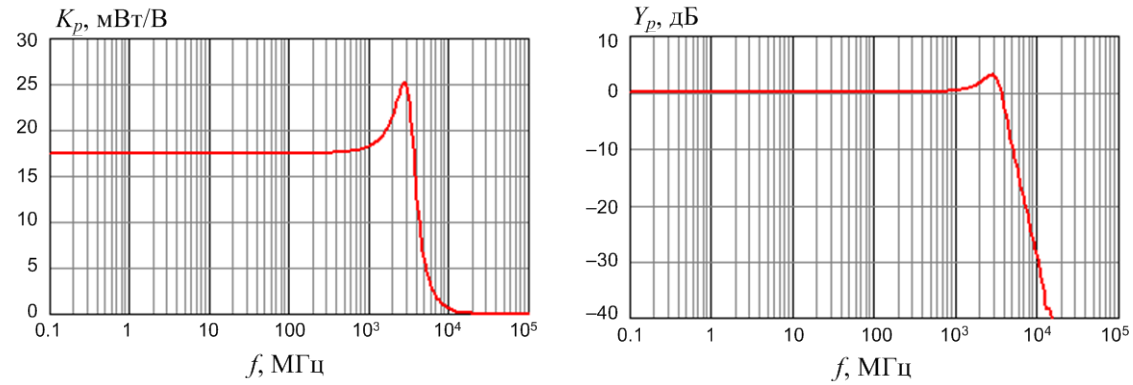
$$K(j\omega) = \frac{P(j\omega)}{U_1(j\omega)} = \frac{K_3(j\omega)K_1(j\omega)}{1+K_3(j\omega)K_1(j\omega)K_2(j\omega)} = \frac{K_{31}(j\omega)}{1+A(j\omega)}, \quad (28)$$

$$K(\omega) = \frac{P(\omega)}{U_1(\omega)} = \frac{K_{31}(\omega)}{|1+A(j\omega)|}. \quad (29)$$

На рис. 14 приведена результирующая АЧХ ССМ, рассчитанная по (29).

Определим некоторые параметры рассчитанной ССМ: модуль петлевого усиления $A_0 = 62$, Амплитуда входного напряжения $U_1 \approx 1$ В для обеспечения максимальной выходной оптической мощности $P_1 = 19$ мВт.

Сравнение рис. 13 и 14 показывает, что использование ООС в ССМ позволяет существенно повысить быстродействие ИИ. Полоса пропускания может быть увеличена с 20–30 МГц до 2–3 ГГц.



а *б*

Рис. 14. АЧХ системы стабилизации оптической мощности в линейном (а)
и логарифмическом (б) масштабах

Кроме того, существенно уменьшается влияние нестабильности параметров ИИ. Относительная погрешность поддержания оптической мощности при воздействии любого дестабилизирующего фактора уменьшается в A_0 раз.

Библиографический список

1. **Иванов А. Б.** Волоконная оптика: компоненты, системы передачи, измерения / А. Б. Иванов. – М. : Компания САЙРУС СИСТЕМС, 1999. – 672 с.

2. **Листвин В. Н.** DWDM системы: научное издание / В. Н. Листвин, В. Н. Трещиков. – М. : Издательский дом «Наука», 2013. – 300 с.

3. **Салех Б.** Оптика и фотоника. Принципы и применения. учебное пособие: пер. с англ. В 2 т. Т. 2 / Б. Салех, М. Тейх. – Долгопрудный: Издательский дом «Интеллект», 2012. – 784 с.

4. **Фриман Р.** Волоконно-оптические системы связи / Р. Фриман. – 2-е изд., доп. – М. : Техносфера, 2004. – 496 с.

References

1. **Ivanov A. B.** Volokonnaja optika: komponenty, sistemy peredachi, izmerenija / A. B. Ivanov. – M. : Kompanija SAJRUS SISTEMS, 1999. – 672 s.

2. **Listvin V. N.** DWDM sistemy: nauchnoe izdanie / V. N. Listvin, V. N. Treshhikov. – M. : Izdatel'skij dom «Nauka», 2013. – 300 s.

3. **Saleh B.** Optika i fotonika. Principy i primenenija. uchebnoe po-sobie: per. s angl. V 2 t. T. 2 / B. Saleh, M. Tejh. – Dolgoprudnyj: Izda-tel'skij dom «Intellekt», 2012. – 784 s.

4. **Friman R.** Volokonno-opticheskie sistemy svjazi / R. Friman. – 2-e izd., dop. – M. : Tehnosfera, 2004. – 496 s.

Былина Мария Сергеевна – кандидат технических наук, доцент кафедры «Фотоника и линии связи» Федерального государственного бюджетного образовательного учреждения высшего образования «Санкт-Петербургский государственный университет телекоммуникаций им. проф. М. А. Бонч-Бруевича», BylinaMaria@mail.ru

Глаголев Сергей Федорович – кандидат технических наук, доцент, профессор, заведующий кафедрой «Фотоника и линии связи» Федерального государственного бюджетного образовательного учреждения высшего образования «Санкт-Петербургский государственный университет телекоммуникаций им. проф. М. А. Бонч-Бруевича»

УДК 621.315

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

M. S. Bylina Bonch-Bruevich Saint-Petersburg State University of Telecommunication

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

P. A. Chaimardanov Bonch-Bruevich Saint-Petersburg State University of Telecommunication

КОМПЛЕКС ВИРТУАЛЬНЫХ ЛАБОРАТОРНЫХ РАБОТ ПО ИССЛЕДОВАНИЮ ПАРАМЕТРОВ ПЕРЕДАЧИ КАБЕЛЬНЫХ ЦЕПЕЙ

COMPLEX OF VIRTUAL LABORATORY WORKS FOR RESEARCH OF CABLE CIRCUITS TRANSMISSION PARAMETERS

В данной работе представлены обобщенная математическая модель однородной двухпроводной КЦ, созданная на основе известных моделей, и виртуальная лабораторная установка, разработанная на ее основе, предназначенная для выполнения комплекса лабораторных работ по дисциплинам кафедры «Фотоники и линий связи».

This paper presents a generalized mathematical model of homogeneous cable circuit, created on the basis of well-known models, and virtual laboratory setup, developed on its basis, designed to perform complex of laboratory works on the disciplines provided by on the sub-faculty of Photonics and communications lines.

двухпроводная линия, кабельная цепь, однородная кабельная цепь, первичные параметры передачи, вторичные параметры передачи, виртуальная лабораторная установка.

pair line, cable circuit, homogeneous cable circuit, primary transmission parameters, secondary transmission parameters, virtual laboratory setup.

Введение

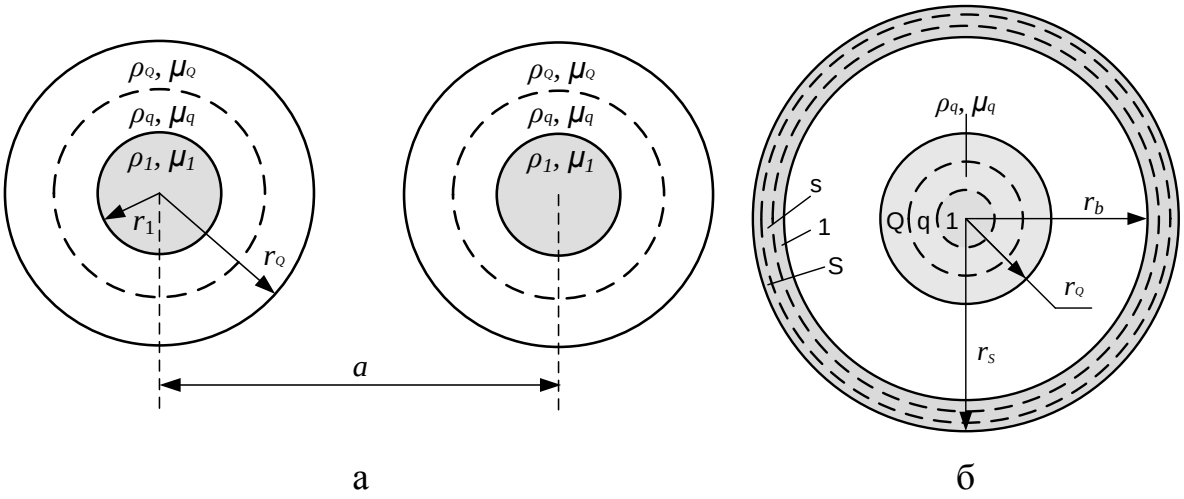
При изучении специальных дисциплин студенты Санкт-Петербургского государственного университета телекоммуникаций (СПбГУТ) им. проф. М.А. Бонч-Бруевича должны изучать свойства таких сложных объектов, как кабельные линии связи, состоящие из кабельных цепей (КЦ). К сожалению, полное обеспечение учебных лабораторий объектами исследования, а также необходимыми современными измерительными приборами и технологическим оборудованием не представляется возможным. Это обусловлено рядом причин, основными из которых явля-

ются громоздкость объектов исследования, их многообразие и распределенность в пространстве, а также высокая стоимость объектов исследования и контрольно-измерительной аппаратуры. Поэтому в большинстве случаев доступ студентов к реальным объектам исследования очень ограничен. Универсальным выходом является использование виртуальных лабораторий, позволяющих проводить лабораторные работы наиболее эффективным, с точки зрения массового обучения, фронтальным методом.

Целью работы является создание виртуальной установки для обеспечения лабораторного практикума по изучению КЦ. При создании виртуальной установки очень важен выбор математических моделей объекта исследования и используемой аппаратуры.

Математическая модель однородной двухпроводной КЦ

В работе моделируются симметричная и коаксиальная КЦ, упрощенные конструкции которых представлены на рис. 1.



а б

Рис. 1. Конструкции симметричной (а) и коаксиальной (б) кабельных цепей

Предполагается, что каждый проводник симметричной КЦ состоит из Q проводящих концентрических слоев и имеет внешний радиус r_Q, а внутренний и внешний проводники коаксиальной КЦ состоят из Q и S слоев соответственно и имеют внешние радиусы r_Q и r_S. Материалы слоев в общем случае различны. Слой q характеризуется радиусом r_q, удельным сопротивлением ρ_q, абсолютной магнитной проницаемостью μ_q и модулем коэффициента вихревых токов $k_q = \sqrt{\omega\mu_q/\rho_q}$.

Изоляция КЦ (диэлектрик) характеризуется эквивалентной диэлектрической проницаемостью $\varepsilon_{экв}$, эквивалентным тангенсом диэлектрических потерь $\mathrm{tg}\Delta_{экв}$, абсолютной магнитной проницаемостью $\mu_{диэл}$, сопротивлением R_0 и проводимостью $G_0 = 1/R_0$ на постоянном токе. Расстояние между проводниками симметричной КЦ равно a. Внутренний радиус внешнего полого проводника коаксиальной КЦ равен r_b.

Конструкция как симметричной, так и коаксиальной КЦ может включать экран с радиусом *X*.

КЦ в целом характеризуется первичными параметрами передачи – погонными сопротивлением *R*, индуктивностью *L*, емкостью *C* и проводимостью *G*, а также вторичными параметрами передачи – волновым сопротивлением $Z_в$, постоянной распространения γ, коэффициентом затухания α, коэффициентом фазы β, фазовой скоростью V_φ, длиной волны λ и удельным временем задержки τ_z сигнала в КЦ.

Электромагнитное поле (ЭМП) КЦ описывается уравнениями Максвелла, которые для изотропной среды имеют вид [1]:

$$\begin{cases} \mathrm{rot}\, H = j_{\text{пров.}} + j_{\text{смещ.}} = \sigma E + \varepsilon_a \frac{\mathrm{dE}}{\mathrm{dt}}, \mathrm{div}\, H = 0 \\ \mathrm{rot}\, E = -\mu_a \frac{dH}{dt}, \mathrm{div}\, E = \frac{\rho}{\varepsilon_a} \end{cases}, \qquad (1)$$

где *H* – напряженность магнитного поля, А / мм;

E – напряженность электрического поля, В / мм;

$j_{\text{пров.}}$ – плотность тока проводимости, А / мм^2;

$j_{\text{смещ.}}$ – плотность тока смещения, А / мм^2;

σ – удельная проводимость среды, См / мм;

ε_a – абсолютная диэлектрическая проницаемость среды, Ф / мм;

μ_a – абсолютная магнитная проницаемость среды, Гн / мм;

ρ – объемная плотность зарядов, Кл / мм^3;

t – время, с.

Полное сопротивление *Z*, а также погонные сопротивление и индуктивность проводника с радиусом r_a можно определить, используя уравнение Умова-Пойтинга:

$$I^2 Z = \int_0^{2\pi} E_z(r_a) H_\varphi^*(r_a) r_a d\varphi,\ R = Re(Z),\ L = \mathrm{Im(Z)}/(i\omega), \qquad (2)$$

где *I* – сила тока, протекающего по проводнику;

H_φ^* – комплексно сопряженное значение H_φ;

E_z – продольная составляющая электрического поля;

H_φ – тангенциальная составляющая магнитного поля.

При установившемся гармоническом воздействии с частотой ω из (1) можно получить систему уравнений для H_φ и E_z [1]:

$$H_\varphi = \frac{1}{i\omega\mu_a}\frac{\partial E_z}{\partial r},$$

$$\frac{\partial^2 E_z}{\partial r^2} + \frac{1}{r}\frac{\partial E_z}{\partial r} + \frac{1}{r^2}\frac{\partial^2 E_z}{\partial \varphi^2} + \frac{\partial^2 E_z}{\partial z^2} - ik^2 E_z = 0 \text{ – } \textit{для проводника}, \qquad (3)$$

$$\frac{\partial^2 E_z}{\partial r^2} + \frac{1}{r}\frac{\partial E_z}{\partial r} + \frac{1}{r^2}\frac{\partial^2 E_z}{\partial \varphi^2} + \frac{\partial^2 E_z}{\partial z^2} = 0 \text{ – } \textit{для диэлектрика},$$

где $k = \sqrt{\omega\mu_a/\rho}$ – модуль коэффициента вихревых токов (1 / мм).

Математическая модель симметричной КЦ

Для симметричной КЦ (рис. 1а) решение системы (3) имеет вид:

Проводник, слой q:

$$E_z(r,\varphi,q)=\sum_{n=0}^{\infty}\left(A_{q,n}\cdot I_n(m_q r)+B_{q,n}\cdot K_n(m_q r)\right)\cos(n\varphi),$$

$$H_\varphi(r,\varphi,q)=\frac{1}{m_q\rho_q}\Bigg(A_{q,0}I_1(m_q r)+0.5\sum_{n=1}^{\infty}A_{q,n}\big[I_{n-1}(m_q r)+$$

$$+I_{n+1}(m_q r)\big]\cos(n\varphi)\Big)-\frac{1}{m_q\rho_q}\Bigg(B_{q,0}K_1(m_q r)+0.5\sum_{n=1}^{\infty}B_{q,n}\big[K_{n-1}(m_q r)+$$

$$+K_{n+1}(m_q r)\big]\cos(n\varphi)\Big). \qquad (4)$$

Диэлектрик:

$$E_z(r,\varphi)=F_0\ln(r)+C_0+\sum_{n=1}^{\infty}[F_n r^n+C_n r^{-n}]\cos(n\varphi)\,,$$

$$H_\varphi(r,\varphi)=\frac{F_0}{i\omega\mu_{\text{диэл}}r}+\sum_{n=1}^{\infty}\frac{n\left[F_n r^{n-1}-C_n r^{-n-1}\right]}{i\omega\mu_{\text{диэл}}}\cos(n\varphi)\,. \qquad (5)$$

В (4) и (5) использованы следующие обозначения: I_n, K_n – модифицированные функции Бесселя n-го порядка первого и второго рода, соответственно, $m_q=\sqrt{i}k_q$, k_q – модуль коэффициента вихревых токов слоя q, $A_{q,n}$, $B_{q,n}$, C_n, F_n – постоянные интегрирования, определяемые из граничных условий.

Граничные условия, заключающиеся в непрерывности составляющих ЭМП на границах соседних слоев проводника, позволяют выразить все $A_{q,n}$ и $B_{q,n}$ через $A_{1,n}$ и $B_{1,n}$ и представить (4) в виде:

$$E_z(r_q,\varphi,q)=A_{1,0}h_{q,0}+\sum_{n=1}^{\infty}A_{1,n}h_{q,n}\cos(n\varphi),$$

$$H_\varphi(r_q,\varphi,q)=A_{1,0}z_{q,0}+\sum_{n=1}^{\infty}A_{1,n}z_{q,n}\cos(n\varphi), \qquad (6)$$

где $h_{q,0}$, $h_{q,n}$, $z_{q,0}$ и $z_{q,n}$ – константы, определяемые приведенными ниже выражениями.

Для q-го слоя (q = 1):

$$h_{1,0}=I_0(m_1r_1),\ h_{1,n}=I_n(m_1r_1), \qquad (7)$$

$$z_{1,0}=\frac{1}{m_1\rho_1}I_1(m_1r_1),\ z_{1,n}=\frac{1}{2m_1\rho_1}[I_{n-1}(m_1r_1)+I_{n+1}(m_1r_1)]. \qquad (8)$$

Для q-го слоя (q ≠ 1):

$$A_{q,0} = A_{1,0}\frac{m_q\rho_q K_0(m_q r_{q-1})z_{q-1,0}+h_{q-1,0}K_1(m_q r_{q-1})}{K_1(m_q r_{q-1})I_0(m_q r_{q-1})+K_0(m_q r_{q-1})I_1(m_q r_{q-1})}, \quad (9)$$

$$B_{q,0} = -A_{1,0}\frac{m_q\rho_q I_0(m_q r_{q-1})z_{q-1,0}-h_{q-1,0}I_1(m_q r_{q-1})}{K_1(m_q r_{q-1})I_0(m_q r_{q-1})+K_0(m_q r_{q-1})I_1(m_q r_{q-1})}, \quad (10)$$

$$A_{q,n} = A_{1,n}\frac{2m_q\rho_q K_n(m_q r_{q-1})z_{q-1,n}+h_{q-1,n}\left(K_{n+1}(m_q r_{q-1})+K_{n-1}(m_q r_{q-1})\right)}{I_n(m_q r_{q-1})\left(K_{n+1}(m_q r_{q-1})+K_{n-1}(m_q r_{q-1})\right)+K_n(m_q r_{q-1})\left(I_{n+1}(m_q r_{q-1})+I_{n-1}(m_q r_{q-1})\right)}, \quad (11)$$

$$B_{q,n} = -A_{1,n}\frac{2m_q\rho_q I_n(m_q r_{q-1})z_{q-1,n}-h_{q-1,n}\left(I_{n+1}(m_q r_{q-1})+I_{n-1}(m_q r_{q-1})\right)}{I_n(m_q r_{q-1})\left(K_{n+1}(m_q r_{q-1})+K_{n-1}(m_q r_{q-1})\right)+K_n(m_q r_{q-1})\left(I_{n+1}(m_q r_{q-1})+I_{n-1}(m_q r_{q-1})\right)}. \quad (12)$$

$$h_{q,0} = \left[A_{q,0}I_0(m_q r_q) + B_{q,0}K_0(m_q r_q)\right]/A_{1,0}, \quad (13)$$

$$z_{q,0} = \frac{1}{m_q\rho_q}\left[\frac{A_{q,0}I_1(m_q r_q)-B_{q,0}K_1(m_q r_q)}{A_{1,0}}\right], \quad (14)$$

$$h_{q,n} = \left[A_{q,n}I_n(m_q r_q) + B_{q,n}K_n(m_q r_q)\right]/A_{1,n}, \quad (15)$$

$$z_{q,n} = \frac{1}{2m_q\rho_q}\frac{\left(A_{q,n}\left(I_{n+1}(m_q r_q)+I_{n-1}(m_q r_q)\right)-B_{q,n}\left(K_{n+1}(m_q r_q)+K_{n-1}(m_q r_q)\right)\right)}{A_{1,n}}, \quad (16)$$

Выразим постоянные интегрирования $A_{1,n}$, $B_{1,n}$, и C_n через F_n, используя соотношения (5) и (6) и граничное условие, заключающееся в непрерывности составляющих ЭМП на границе внешнего Q-го слоя проводника и диэлектрика:

$$A_{1,0} = \frac{iF_0}{-z_{Q,0}\omega\mu_{\text{диэл}}r_Q}, A_{1,n} = \frac{i2nF_n r_Q^n}{-z_{Q,n}\omega\mu_{\text{диэл}}r_Q+inh_{Q,n}}, C_0 = -F_0\left(\ln(r_Q) - \chi_0\right) \quad (17)$$

$$C_n = -F_n r_Q^{2n}\chi_n, \quad \chi_0 = \frac{ih_{Q,0}}{-z_{Q,0}\omega\mu_{\text{диэл}}r_Q}, \quad \chi_n = \frac{z_{Q,n}\omega\mu_{\text{диэл}}r_Q+inh_{Q,n}}{z_{Q,n}\omega\mu_{\text{диэл}}r_Q-inh_{Q,n}},$$

Воспользовавшись законом полного тока, получим $F_0 = i\omega\mu_{\text{диэл}}I/2\pi$.

Учитывая идентичность проводников симметричной КЦ, из (5), согласно рекомендациям, предложенным в [2], можно получить уравнения для определения постоянных интегрирования F_n:

$$nF_n r_Q^n \cong \frac{iI\omega\mu_{\text{диэл}}}{2\pi}\varepsilon^n + \sum_{j=1}^{\infty}\frac{jF_j r_Q^{2j}\chi_j\varepsilon^n}{a^j}\frac{(j+n-1)!}{j!(n-1)!}, \ \varepsilon = \frac{r_Q}{a} \le 0.5. \quad (21)$$

Минимально необходимое число определяемых F_n выбирается исходя из требуемой точности расчета.

Подставляя найденные значения составляющих ЭМП в (2) , получим выражение для полного сопротивления симметричной КЦ:

$$Z = 2\left[i2\pi\omega\mu_{\text{диэл}}\chi_0 + g\frac{i\pi}{\omega\mu_{\text{диэл}}I^2}\sum_{n=1}^{\infty} nF_nF_n^*r_Q^{2n}(1-\chi_n)(1+\chi_n^*)\right] + Z_{\text{доп.}} \quad (22)$$

где g – поправочный коэффициент, учитывающий влияние окружающих металлических конструкций; $Z_{\text{доп}}$ – дополнительное сопротивление, обусловленное наличием экрана (если он есть). Параметры g и $Z_{\text{доп}}$ определяются согласно рекомендациям [1].

Для симметричной КЦ из многожильных проводников Z можно приближенно рассчитать по выражению (22) при $Q = 1$ и $r_Q = r_п \cdot \sqrt{v}$, $r_п$ – радиус одной проволоки, v – число проволок в повиве.

Погонные сопротивление, индуктивность, емкость и проводимость КЦ определяются выражениями [1]:

$$R = Re(Z), L = L_{\text{внутр.}} + L_{\text{внеш.}} = \frac{Im(z)}{i\omega} + \frac{\mu_{\text{диэл}}}{\pi}\cdot\ln\frac{a}{r_{\text{Q}}}. \quad (23)$$

$$C = \frac{\pi\varepsilon_{\text{экв}}}{\ln\frac{a}{r_{\text{Q}}} - \text{g}\left(\frac{r_Q}{a}\right)^2} - \textit{для неэкранированной цепи} \quad (24)$$

$$C = \frac{\pi\varepsilon_{\text{экв}}}{\ln\frac{a}{r_Q} - \frac{a^2}{2X^2} - \text{g}\left(\frac{r_Q}{a}\right)^2} - \textit{для экранированной цепи} \quad (25)$$

$$G = G_0 + \omega C\text{tg}\Delta_{\text{экв}}. \quad (26)$$

Предложенную методику для расчета симметричных КЦ можно использовать для анализа цепей воздушных линий связи.

Математическая модель коаксиальной КЦ

Для слоя q внутреннего проводника коаксиальной КЦ (рис. 1б) решение (3) имеет вид:

$$E_z(r,\varphi,q) = A_q\cdot I_0(m_q r) + B_q\cdot K_0(m_q r),$$

$$H_\varphi(r,\varphi,q) = \frac{1}{m_q\rho_q}\left[A_q I_1(m_q r) - B_q K_1(m_q r)\right], \quad (27)$$

где A_q, B_q – постоянные интегрирования, определяемые из граничных условий. Условия непрерывности составляющих ЭМП на границах соседних слоев проводника позволяют представить (27) в виде

$$E_z(r_q, \varphi, q) = A_1 h_q,\ H_\varphi(r_q, \varphi, q) = A_1 z_q, \tag{28}$$

где

$$h_1 = I_0(m_1 r_1),\ h_q = \frac{A_q I_0(m_q r_q) + B_q K_0(m_q r_q)}{A_1}, \tag{29}$$

$$z_1 = \frac{1}{m_1 \rho_1} I_1(m_1 r_1),\ z_q = \frac{1}{m_q \rho_q}\left[\frac{A_q I_1(m_q r_q) - B_q K_1(m_q r_q)}{A_1}\right], \tag{30}$$

$$A_q = A_1 \frac{m_q \rho_q K_0(m_q r_{q-1}) z_{q-1} + h_{q-1} K_1(m_q r_{q-1})}{K_1(m_q r_{q-1}) I_0(m_q r_{q-1}) + K_0(m_q r_{q-1}) I_1(m_q r_{q-1})}, \tag{31}$$

$$B_q = -A_1 \frac{m_q \rho_q I_0(m_q r_{q-1}) z_{q-1} - h_{q-1} I_1(m_q r_{q-1})}{K_1(m_q r_{q-1}) I_0(m_q r_{q-1}) + K_0(m_q r_{q-1}) I_1(m_q r_{q-1})}. \tag{32}$$

Константу A_1 найдем, воспользовавшись законом полного тока:

$$H_\varphi(r_Q) = A_1 z_Q = \frac{I}{2\pi r_Q},\ A_1 = \frac{I}{2\pi r_Q z_Q}. \tag{33}$$

Окончательно для полного сопротивления Z_a и погонных сопротивления R_a и индуктивности L_a внутреннего проводника получаем:

$$Z_\text{a} = i2\pi\omega\mu_{\text{диэл}}\chi_0,\ \chi_0 = \frac{i h_Q}{-z_Q \omega \mu_{\text{диэл}} r_Q},\ R_a = Re(Z_a)\ ,\ L_\text{a} = \frac{Im(Z_\text{a})}{i\omega}. \tag{34}$$

Решение (3) для диэлектрика ($r_Q \le r \le r_b$) имеет вид:

$$E_z(r) = F_a \ln(r) + C_a,\ H_\varphi(r) = \frac{F_a}{i\omega\mu_{\text{диэл}} r}. \tag{35}$$

Постоянные интегрирования F_a, C_a определим из (28), (33) и (35) с использованием граничных условий, заключающихся в непрерывности составляющих ЭМП при $r = r_Q$:

$$A_1 h_0 = F_a \ln(r_Q) + C_a,\ C_a = A_1 h_Q - F_a \ln(r_Q),\ F_a = i\omega\mu_{\text{диэл}} I/2\pi. \tag{36}$$

Окончательно для области $r_Q \le r \le r_b$ получим:

$$E_z(r) = F_a \ln\frac{r}{r_Q} + A_1 h_Q,\ H_\varphi(r) = \frac{F_a}{i\omega\mu_{\text{диэл}} r} = \frac{I}{2\pi r}, \tag{37}$$

Решение (3) для составляющих ЭМП во внешнем проводнике ($r \geq r_b$) имеет вид (27). С учетом граничных условий, состоящих в непрерывности составляющих ЭМП на границах соседних слоев, а также требования равенства нулю напряженности магнитного поля при $r = r_S$ это решение можно представить через константу A_S:

$$H_\varphi(r,q) = A_S z_q,\ E_z(r,q) = A_S h_q, \tag{38}$$

где

Для S-го слоя (q = S):

$$h_S = I_0(m_S r_{S-1}) + \frac{I_1(m_S r_S)}{K_1(m_S r_S)} K_0(m_S r_{S-1}) \tag{39}$$

$$z_S = \frac{1}{m_S p_S} \cdot \left[I_1(m_S r_{S-1}) - \frac{I_1(m_S r_S)}{K_1(m_S r_S)} K_1(m_S r_{S-1}) \right] \tag{40}$$

Для q-го слоя ($q \neq S$):

$$h_{q-1} = \frac{A_{q-1} I_0(m_{q-1} r_{q-2}) + B_{q-1} K_0(m_{q-1} r_{q-2})}{A_S}, \tag{41}$$

$$z_{q-1} = \frac{1}{m_{q-1}\rho_{q-1}} \left[\frac{A_{q-1} I_1(m_{q-1} r_{q-2}) - B_{q-1} K_1(m_{q-1} r_{q-2})}{A_S} \right], \tag{42}$$

$$A_{q-1} = A_S \frac{m_{q-1}\rho_{q-1} K_0(m_{q-1} r_{q-1}) z_q + h_q K_1(m_{q-1} r_{q-1})}{K_1(m_{q-1} r_{q-1}) I_0(m_{q-1} r_{q-1}) + K_0(m_{q-1} r_{q-1}) I_1(m_{q-1} r_{q-1})}, \tag{43}$$

$$B_{q-1} = -A_S \frac{m_{q-1}\rho_{q-1} I_0(m_{q-1} r_{q-1}) z_q - h_q I_1(m_{q-1} r_{q-1})}{K_1(m_{q-1} r_{q-1}) I_0(m_{q-1} r_{q-1}) + K_0(m_{q-1} r_{q-1}) I_1(m_{q-1} r_{q-1})}. \tag{44}$$

Для внутреннего слоя (q = 1) из (41)–(44) получаем:

$$h_1 = \frac{A_1 I_0(m_1 r_b) + B_1 K_0(m_1 r_b)}{A_S},\ z_1 = \frac{1}{m_1 \rho_1} \left[\frac{A_1 I_1(m_1 r_b) - B_1 K_1(m_1 r_b)}{A_S} \right]. \tag{45}$$

Воспользовавшись законом полного тока, получим $A_s = I/2\pi r_b z_1$. Окончательно для полного сопротивления Z_b и погонных сопротивления R_b и индуктивности L_b внешнего проводника получаем:

$$Z_b = -\frac{1}{2\pi r_b} \cdot \frac{h_1}{z_1},\ R_b = Re(Z_b),\ L_b = \frac{Im(Z_b)}{i\omega}. \tag{46}$$

Погонные сопротивление, индуктивность и емкость коаксиальной КЦ определяются выражениями [3]

$$R = R_a + R_b,\ L = L_a + L_b + L_{\text{внешн.}} = L_a + L_b + \frac{\mu_{\text{диэл}}}{2\pi} \cdot \ln\frac{r_b}{r_Q},\ C = \frac{2\pi\varepsilon_{\text{экв}}}{\ln\frac{r_b}{r_Q}}. \quad (47)$$

Для погонной проводимости *G* справедливо выражение (26).

Математическая модель процессов распространения сигналов по КЦ

Рассмотрим однородную КЦ длиной l, подключенную к источнику напряжения, изменяющегося по гармоническому закону, с внутренним сопротивлением Z_0 и нагруженную на сопротивление Z_l. В общем случае КЦ является несогласованной, то есть $Z_0 \neq Z_l \neq Z_в$, а Z_0 и Z_l – комплексными. Передаточная характеристика КЦ по напряжению с учетом многократных отражений определяется выражением [4]:

$$K_U(i\omega) = \frac{U_l}{U_0} = \frac{Z_{\text{в}}}{Z_0+Z_в}\frac{1+\Gamma_l}{1-\Gamma_0\Gamma_l\exp(-2\gamma l)}\exp(-\gamma l),\ \Gamma_0 = \frac{Z_в-Z_0}{Z_в+Z_0},\ \Gamma_l = \frac{Z_l-Z_в}{Z_l+Z_в}, \quad (48)$$

где U_0 и U_l – напряжения на входе и выходе КЦ, Γ_0 и Γ_l – коэффициенты отражения от входа и выхода КЦ.

Передаточная характеристика $K_U(j\omega)$ позволяет рассчитать форму сигнала на выходе КЦ $u_2(t)$ при любом входном воздействии $u_1(t)$ по выражению:

$$u_2(t) = \mathcal{F}^{-1}[\mathcal{F}[u_1(t)] \cdot K_U(i\omega)], \quad (49)$$

где $\mathcal{F}$ и $\mathcal{F}^{-1}$ прямое и обратное преобразование Фурье.

Сравнение результатов с экспериментальными данными

Для проверки правильности предложенных математических моделей было проведено сравнение рассчитанных параметров КЦ с экспериментальными данными, приведенными в [5, 6]. На рис. 2 и 3 представлены некоторые результаты сравнения. Из рисунков видно, что рассчитанные параметры хорошо описывают имеющиеся экспериментальные данные.

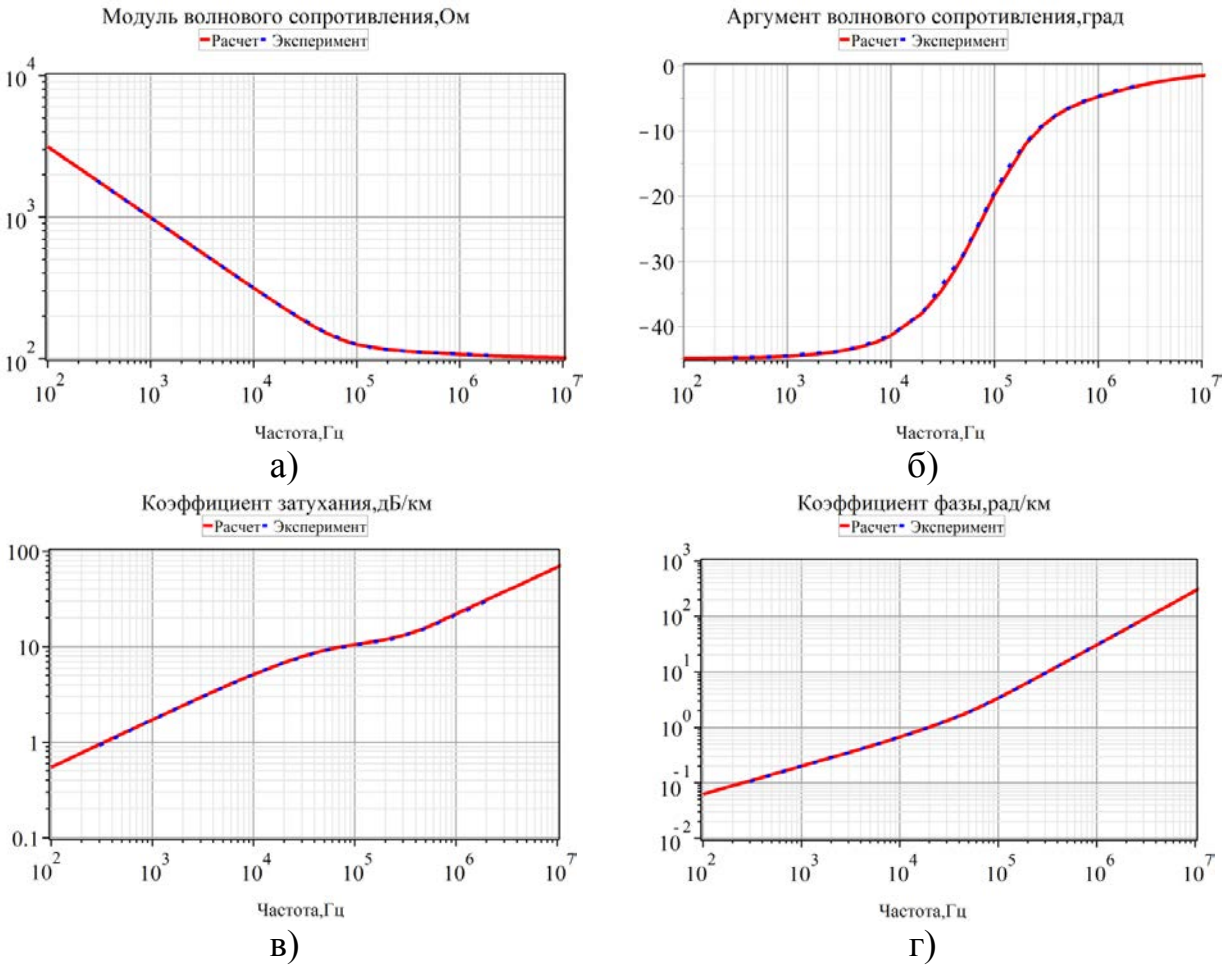


Рис. 2. Сопоставление рассчитанных
и экспериментально определенных параметров КЦ ТПП-0.4

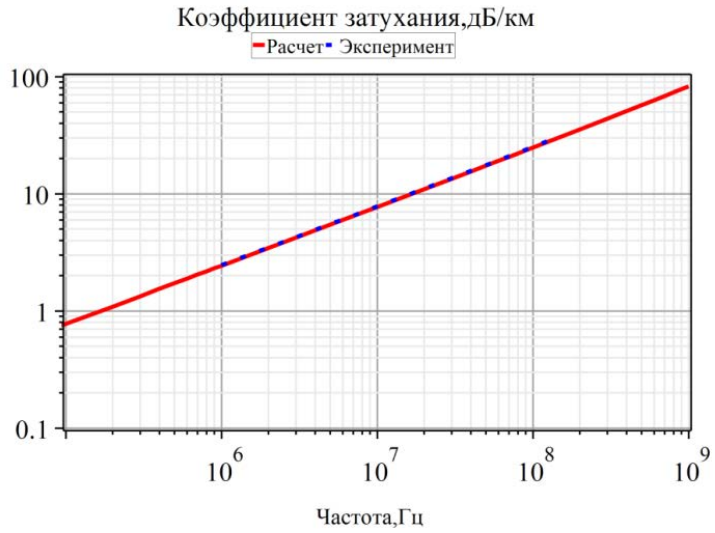


Рис. 3. Сопоставление рассчитанного и экспериментально определенного
коэффициента затухания коаксиальной КЦ кабеля КМГ-4

Виртуальная лабораторная установка по исследованию параметров КЦ

В основу разрабатываемой лабораторной установки положена математическая модель однородной КЦ, предложенная в п. 2. Исходными данными для моделирования являются конструктивные параметры КЦ и параметры материалов ее конструктивных элементов.

Виртуальная лабораторная установка позволяет проводить исследования цепей коаксиальных и симметричных кабелей, а также воздушных линий связи. Она обеспечивает следующие основные возможности:

– расчет первичных параметров КЦ;

– расчет вторичных параметров КЦ;

– расчет распределения плотности тока проводимости и тангенциальной составляющей напряженности магнитного поля КЦ;

– анализ процессов распространения различных сигналов по КЦ в частотной и временной областях с учетом возможного нарушения условий согласования линии с источником и/или приемником.

Для удобства использования интерфейс виртуальной лабораторной установки разделен на пять вкладок.

Вкладка «Цепи». Интерфейс данной вкладки (рис. 4) состоит из элементов управления, позволяющих задавать вид и параметры исследуемых КЦ. Параметры основных конструктивных элементов КЦ разделены на три группы – проводник, изоляция и экран. Одновременно можно задать параметры и провести расчеты для трех разных КЦ. Любое изменение параметров исследуемой КЦ отражается на чертеже справа.

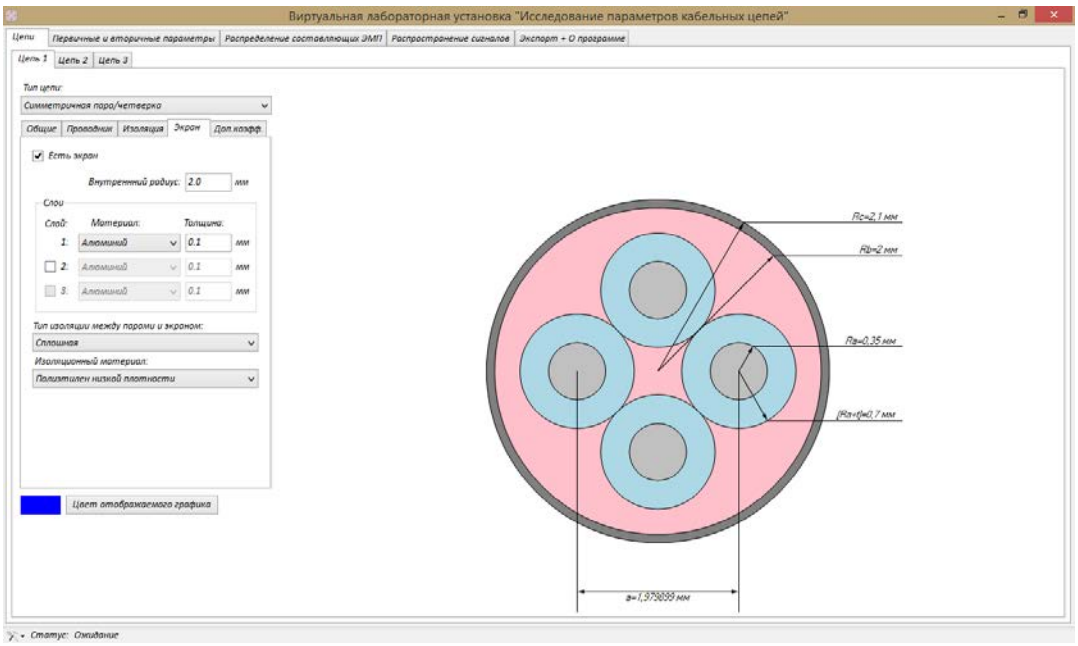


Рис. 4. Вкладка «Цепи». Выбор исходных данных.
Моделирование экранированной симметричной четверки

Вкладка «Первичные и вторичные параметры». На данной вкладке в виде графиков отображаются результаты расчета зависимостей первичных и вторичных параметров выбранных цепей от частоты (рис. 5)

Управление отображением зависимостей осуществляется с помощью меню, расположенного в левой части окна виртуальной лабораторной установки. Выбор отображаемого параметра осуществляется с помощью выпадающего списка, расположенного вверху справа. Четыре кнопки вверху слева позволяют изменять масштаб осей графика (линейный/логарифмический).

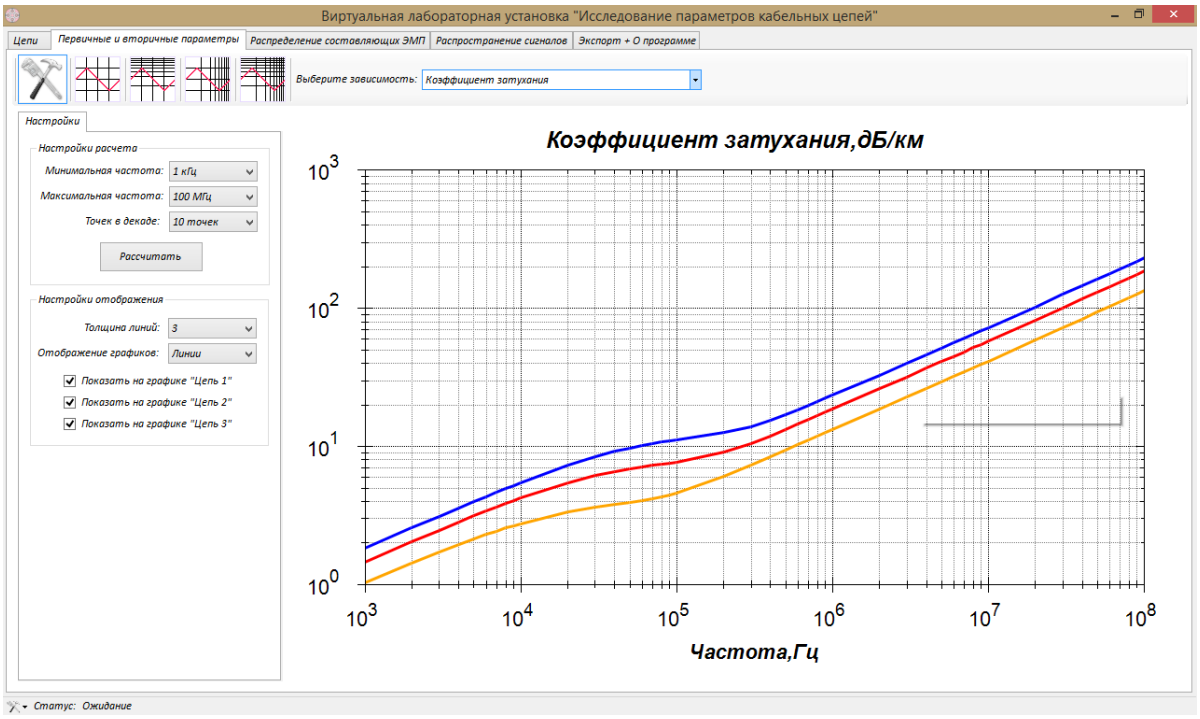


Рис. 5. Вкладка «Первичные и вторичные параметры».
Результаты расчета коэффициентов затухания КЦ ТПП-0.4 (син.), ТПП-0.5 (красн.) и ТПП-0.7 (желт.)

Вкладка «Расчет составляющих ЭМП». Данная вкладка позволяет рассмотреть распределение модуля плотности тока проводимости в проводниках цепи, а также тангенциальную составляющую магнитного поля цепи (рис. 6). Все зависимости нормируются к максимальному значению.

Интерфейс данной вкладки состоит из бокового меню и области из двух графиков. В меню имеются поля для выбора частоты и количества точек, список с выбором рассматриваемой цепи и кнопка расчета.

В качестве начала отсчета расстояния на графиках для коаксиальных КЦ используется точка, соответствующая центру внутреннего проводника, а для симметричных КЦ – соответствующая центру левого проводника.

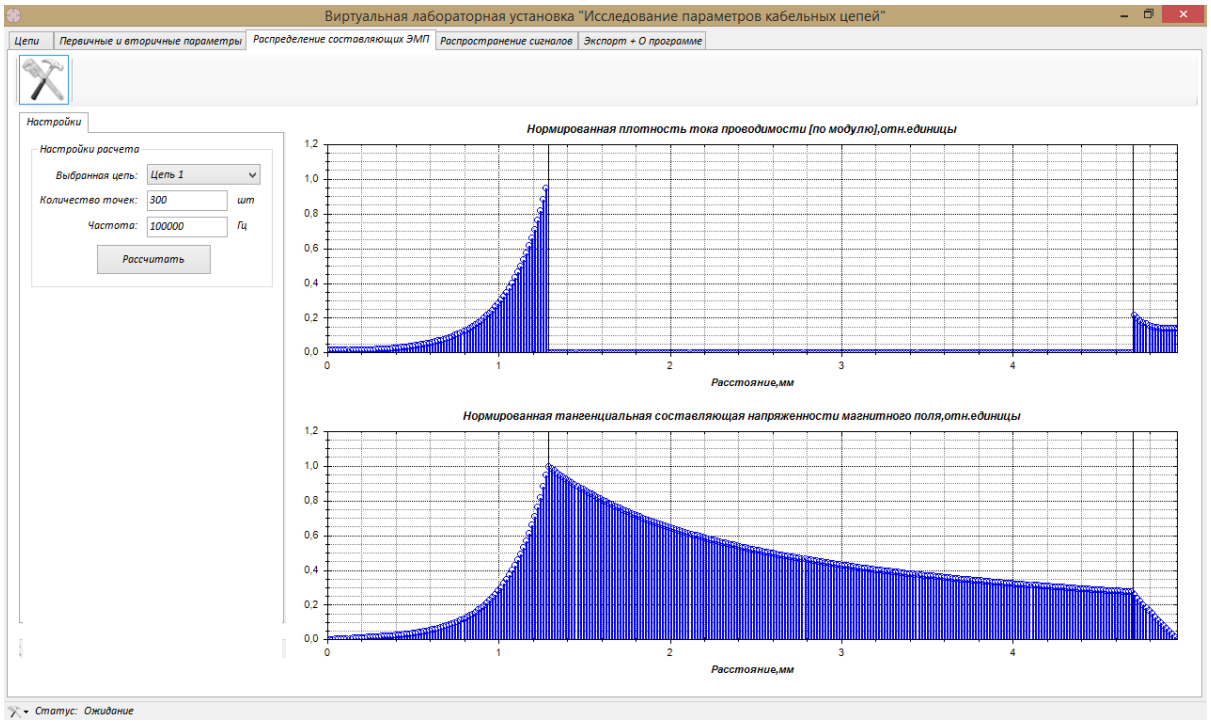


Рис. 6. Вкладка «Расчет составляющих ЭМП».
Результаты расчета параметров КЦ КМГ-4 на частоте 100 кГц

Вкладка «Распространение сигналов». Данная вкладка позволяет рассмотреть распространение сигналов различного вида во временной и частотной области по выбранной цепи с учетом согласования/рассогласования линии с источником и приемником (рис. 7).

Интерфейс данной вкладки состоит из меню и области отображения зависимостей. Верхнее меню состоит из меню выбора вида зависимостей.

В качестве сигналов в виртуальной лабораторной установке используются:

– одиночный импульс: трапецеидальный или гауссовский;

– последовательность импульсов, представляющих некоторую кодовую комбинацию и сформированную в соответствии с двоичным или квазитроичным линейным кодом (NRZ, дифференциальный NRZ, RZ, дифференциальный RZ, NRZI, Манчестерский, Манчестерский дифференциальный, AMI, MLT-3, HDB-2, HDB-3).

– произвольно заданный сигнал, загружаемый из внешнего файла

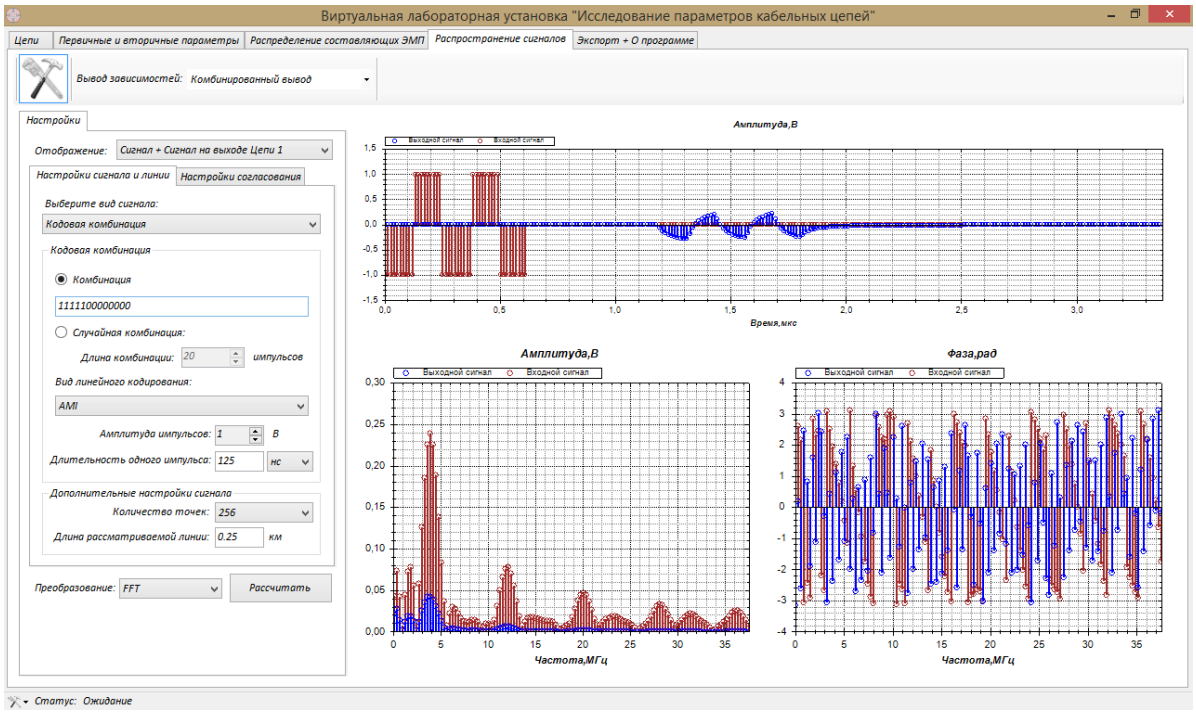


Рис. 7. Вкладка «Распространение сигналов».
Анализ распространения последовательности импульсов по согласованной КЦ ТПП-0.4 длиной 0,25 км. Длительность одного импульса 125 нс

В меню настроек можно изменять Z_0 и/или Z_l. В качестве Z_0 и/или Z_l в лабораторной установке можно выбрать активное сопротивление, индуктивность, емкость, а также различные их сочетания. Меню *«Вывод зависимостей»* позволяет выбрать, как отображать полученные зависимости во временной и частотной области (совместно или раздельно). Меню *«Рассматриваемые сигналы»* позволяет выбрать для рассмотрения либо только исходный сигнал, либо исходный сигнал вместе с сигналом на выходе какой-либо цепи.

Вкладка «Экспорт». Данная вкладка позволяет экспортировать все результаты расчетов в файлы, которые сохраняются в указанный пользователем каталог. Отметим, что графики, представленные во вкладках, можно сохранить или распечатать отдельно, не заходя на вкладку «Экспорт» путем выбора в выпадающем контекстном меню под графиком соответствующего действия.

Заключение

В рамках данной работы создана и внедрена в учебный процесс СПбГУТ им. проф. М. А. Бонч-Бруевича виртуальная лабораторная установка, реализующая комплекс лабораторных работ по изучению направляющих систем связи на основе двухпроводных линий.

Виртуальная лабораторная установка сочетает в себе функции обучения и контроля полученных знаний и позволяет преподавателю задавать уровень сложности лабораторной работы от ознакомительного до научно-исследовательского.

Библиографический список

1. **Каден Г.** Электромагнитные экраны в высокочастотной технике и технике электросвязи / Г. Каден. – М. : Государственное энергетическое издательство, 1957. – 165 с.

2. **Кулешов В. Н.** Теория кабелей связи: учеб. пособие / В. Н. Кулешов; под ред. В. А. Новикова. – М. : Связьиздат, 1950. – 420 с.

3. **Гроднев И. И.** Коаксиальные кабели связи / И. И. Гроднев, П. А. Фролов. – М. : Радио и связь, 1983. – 196 с.

4. **Андреев В. А.** Временные характеристики кабельных линий связи / В. А. Андреев. – М. : Радио и связь, 1986. – 105 с.

5. **Брискер А. С.** Городские телефонные кабели: справочник / А. С. Брискер, А. Д. Руга, Д. Л. Шарле; под ред. Д. Л. Шарле. – 2-е изд., перераб. и доп. – М. : Радио и связь, 1984. – 304 с.

6. **ГОСТ 10971-78.** Кабели коаксиальные магистральные с парами типа 2,6/9,4 и 2,6/9,5. – Введ. 1980-01-01. – М.: Госкомитет СССР по стандартам, 1978. – 51 с.

References

1. **Kaden G.** Jelektromagnitnye jekrany v vysokochastotnoj tehnike i tehnike jelektrosvjazi / G. Kaden. – M. : Gosudarstvennoe jenergeticheskoe iz-datel'stvo, 1957. – 165 s.

2. **Kuleshov V. N.** Teorija kabelej svjazi: ucheb. posobie / V. N. Kuleshov; pod red. V. A. Novikova. – M. : Svjaz'izdat, 1950. – 420 s.

3. **Grodnev I. I.** Koaksial'nye kabeli svjazi / I. I. Grodnev, P. A. Frolov. – M. : Radio i svjaz', 1983. – 196 s.

4. **Andreev V. A.** Vremennye harakteristiki kabel'nyh linij svjazi / V. A. Andreev. – M. : Radio i svjaz', 1986. – 105 s.

5. **Brisker A. S.** Gorodskie telefonnye kabeli: spravochnik / A. S. Brisker, A. D. Ruga, D. L. Sharle; pod red. D. L. Sharle. – 2-e izd., pererab. i dop. – M. : Radio i svjaz', 1984. – 304 s.

6. **GOST 10971-78.** Kabeli koaksial'nye magistral'nye s parami tipa 2,6/9,4 i 2,6/9,5. – Vved. 1980-01-01. – M.: Goskomitet SSSR po standar-tam, 1978. – 51 s.

Былина Мария Сергеевна – кандидат технических наук, доцент кафедры «Фотоника и линии связи» Федерального государственного бюджетного образовательного учреждения высшего образования «Санкт-Петербургский государственный университет телекоммуникаций им. проф. М. А. Бонч-Бруевича», BylinaMaria@mail.ru

Чаймарданов Павел Александрович – аспирант кафедры «Фотоника и линии связи» Федерального государственного бюджетного образовательного учреждения высшего образования «Санкт-Петербургский государственный университет телекоммуникаций им. проф. М. А. Бонч-Бруевича»

УДК 004.07

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

Yu. V. Voevodin Bonch-Bruevich Saint-Petersburg State University of Telecommunication

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

R. V. Kirichek Bonch-Bruevich Saint-Petersburg State University of Telecommunication

ОБЗОР УНИКАЛЬНЫХ ПРОГРАММНО-АППАРАТНЫХ ПАРАМЕТРОВ РАЗЛИЧНЫХ ТЕХНОЛОГИЙ ИНТЕРНЕТА ВЕЩЕЙ

OVERVIEW UNIQUE HARDWARE-SOFTWARE PARAMETERS OF DIFFERENT TECHNOLOGIES INTERNET OF THINGS

В данной статье освещены проблемы идентификации устройств Интернета Вещей, возможные способы идентификации и их влияние на безопасность устройств. Проанализированы преимущества и недостатки предлагаемых решений.

This paper highlights the problems of identification of the Internet of Things devices, identification of possible ways and their impact on safety devices. The advantages and disadvantages of the proposed solutions.

Internet of Things, identification, RFID, NFC, Z-Wave, IPv6, 6LowPAN.

Интернет Вещей, идентификация, RFID, NFC, Z-Wave, IPv6, 6LowPAN.

Введение

С развитием мира Интернета Вещей, устройства, подключаемые к глобальной сети, становятся значительно разнообразней. Помимо уже подключаемых, наподобие бытовой техники, датчиков или автомобилей, вполне реальным стало подключение, казалось бы, таких простейших вещей, как ламп освещения, мебели, одежды, лекарств, автомобильных шин и много другого [1]. Стремительное увеличение числа таких подключённых устройств ставит очень важную и не простую задачу: как гарантированно отличить одну Интернет Вещь от всех остальных? Технология точной идентификации и контроля доступа IoT-устройств должна давать гарантию, что взаимодействие происходит однозначно с одним конкретным устройством [2]. Создание подобной технологии, некого стандарта, позволит не только решить вопрос идентификации IoT-устройств, но и решить

задачу надёжной защиты IoT-устройств от несанкционированного доступа или от подмены на копию. Низкий уровень безопасности негативно влияет на распространение Интернета Вещей и создаёт высокий риск увеличения киберугроз. Риск настолько серьёзный, что FBI вообще не рекомендует предоставлять доступ IoT-устройствам в глобальную сеть.

Возможность подделки IoT-устройств напрямую угрожает искажением или подменой полученных данных [3]. И если подмена данных датчиков на складах приведет к воровству товаров без серьёзных последствий, то подмена данных с датчиков техногенного предприятия уже рискует привести к катастрофе [4].

Проблема использования существующих решений

Малая вычислительная мощность и высокая зависимость от экономии энергии не позволяют в полной мере многим IoT-устройствам полноценно использовать уже существующие протоколы для идентификации, создание защищённых каналов связи, передачи атрибутов, паролей и другой зашифрованной информации. Такие протоколы как SAML, OpenID и им подобные оказываются слишком ресурсоёмкими, а протоколы KNX и EnOcean используют при передачи данных всего несколько байт, которых недостаточно для реализации механизмов безопасности.

Из существующих уже решений по идентификации, предложены такие как:

- идентификация объекта (OID) для обозначения физических объектов с использованием баз управляющей информации (MIB) через протокол SNMP;
- идентификация Интернет Вещей через URL или URI;
- использование EPC (Electronic Product Code) – в радиочастотных метках (Например, RFID);
- использование MAC-адреса.

Данные способы идентификации могут быть использованы для идентификации IoT-устройств, однако, они не являются достаточно надёжными и не гарантируют защиту от подмены устройства.

Идентификация по маршруту в сети

Представляет интерес получившееся решение компании Sigma Designs.

Проприетарный протокол Z-Wave, разработан для домашней автоматизации и реализует ячеистую сеть. Особенностью формирования сети для взаимодействия с одним из устройств является запоминание через какие узлы будет проходит соединение [5]. При этом маршрут остается статичным в памяти и будет изменен лишь в двух случаях:

- если устройство будет недоступно (произойдет поиск новых маршрутов до искомого узла);
- если администратор сети сам решит обновить маршруты.

Наличие статических маршрутов в сети может принести пользу: необходимость строгого соблюдения маршрута для взаимодействия с устройством позволяет использовать сам маршрут (ID маршрутных узлов, характеристики оборудования и т. п.), как один из способов идентификации устройств.

Передача данных между узлами в сети с помощью статичных маршрутов может быть не всегда эффективной, поэтому подобный метод идентификации стоит использовать в сетях с невысокой нагрузкой на каналы связи между узлами. Неподвижность устройств также накладывает ограничения.

Использование подобной статической адресации сужает возможные решения по организации сети, и с практической точки зрения статическая адресация может служить дополнительным компонентом в идентификации вещей [6].

Идентификация с помощью сервера сертификации

Криптографическая система с открытым ключом обеспечивает надёжную защиту информации при обмене зашифрованных данных между двумя устройствами. Однако такой метод идентификации не подразумевает проверку источника (или автора) открытого ключа. Для подтверждения отсутствия подмены открытого ключа предлагается подписывать каждый открытый ключ цифровым сертификатом с помощью третьей стороны: сервера сертификации. Такой метод обеспечивает защиту от подмены ключа.

Аналогично можно использовать центр сертификации не только для обеспечения криптозащиты канала обмена информации, но и для идентификации IoT-устройств. По сути, вместо подписи открытого ключа, сервер будет подписывать само устройство. Однако, вся надёжность такого метода упирается в способность сервера отличить устройство злоумышленника, пытающегося подписать его, от остальных устройств.

Идентификация устройства с помощью IMEI

IMEI представляет собой уникальный идентификатор, который используются в мобильных телефонах во всём мире. В случае использования IMEI для идентификации устройств Интернета Вещей, вместо SIM-карты, в которой хранится номер IMSI, будет встроен чип. Таким образом можно обеспечить уникальную идентификацию, на основе уже разработанных стандартов для мобильных телефонов.

Идентификация с помощью IPv6

Отсутствие свободного адресного пространства по протоколу IPv4 в конечном итоге приведет к массовому переходу сетевых устройств на использование протокола IPv6. IPv6 позволяет использовать $3{,}4\times10^{38}$ адресов. Огромный запас адресного пространства даёт возможность предоставить уникальный идентификатор в виде сетевого адреса каждому устройству вплоть до 2100 года, используя при этом всего 51 бит вместо возможных 128 [7]. Учитывая подобную избыточность, возможно использование незанятой части адресного пространства для какой-либо другой служебной информации, тем самым открывая возможности для создания более «легких» протоколов для IoT-устройств или для внедрения каких-либо криптографических решений.

Стандарт 6LowPAN

Относительно новый стандарт, созданный специально для работы в сетях, где идёт активное взаимодействие Интернет Вещей. Использование 6LowPAN позволяет снизить необходимое количество бит для записи адреса протокола IPv6 с 128 до 64. Это может быть очень полезным при экономии места, если каким-либо образом диапазон в 51 бит всё же будет занят. 6LowPAN также обеспечивает различную степень сжатия заголовка IP – до 50 %, что положительно сказывается по нагрузке на сеть [8].

Радиочастотная идентификация

Те или иные определения Интернета Вещей в конечном итоге сводятся к интеграции физических вещей с цифровым миром Интернета. Среди примеров грузовые контейнеры, станки, транспорт, продукты, животные и люди. Технология RFID (Radio Frequency IDentification) – наиболее подходящая технология для взаимодействия с физическими вещами или их отслеживания [9].

Использование RFID-меток положительно сказывается на экономии энергии: устройству не нужно отправлять данные о себе, считыватель получит всю необходимою информацию из RFID-метки, расположенной на корпусе. В метку можно записать служебную информацию о функционировании устройства или сетевой адрес. В современных радиочастотных метках достаточно места для хранения информации о сетевом адресе. Это особенно актуально с постепенным переходом от протокола IPv4 на IPv6. Использование RFID-идентификации положительно сказывается на удобстве считывания. В отличии от QR-кода и штрих-кода, при работе с RFID нет необходимости в точном позиционировании метки: достаточно находиться в пределах работы Устройства Записи и Считывания (далее УЗС) на расстоянии до 20 метров.

После начала массового внедрения RFID технологий, цена производства меток значительно снизилась и продолжает падать. Разница в стоимости приобретения радиочастотных меток и печати штрих-кодов постепенно нивелируется, и экономическое преимущество RFID-меток будет очевидно в тех областях, где важна скорость работы со считываемыми данными.

Серьёзной преградой для программной реализации защиты устройства с помощью RFID-меток является крайне невысокая вычислительная мощностью чипа в метке. Это значительно снижает диапазон криптографических решений и не позволяет внедрить приемлемую защиту без удорожания производства. Необходимо учесть, что вся вычислительная работа остается на стороне УЗС, а в память RFID-метки можно записать относительно небольшой объём данных. Поэтому среди перспективных решений точной идентификации устройств и защитой от копирования можно выделить следующие:

- Постоянная перезапись служебного поля данных при каждом обращении к устройству. Результат записи формируется по закрытому ключу, который известен будет только той группе УЗС, которой будет происходить считывание меток. Такой способ не решает проблему копирования RFID-метки, но позволяет выявить устройство, которое было скопировано или изменено.
- Использование RFID-меток с уникальным «Железным» ID. Является уже аппаратным решением от копирования. Например, метки Gen2 содержат уникальный ID-идентификатор. Успешность подделки зависит от аппаратного реверс-инжиниринга. Если производитель не уделил должного внимания защите метки от подделки, то через некоторое время на рынке появляются точно такие же метки, но уже с чистым полем уникального ID.

Наиболее эффективным решением обеспечения уникальной идентификацией с помощью RFID-меток является комбинация различных способов защиты данных от копирования.

В вышеупомянутой метке Gen2 существует следующая реализация работы с данными:

- Поле Reserved Memory используется для хранения пароля самоуничтожения и пароля доступа, каждое занимает 32 бита данных. Взаимодействие с данными метки возможно после введения корректного пароля, а введения пароля самоуничтожения приведёт к потере всех данных и выводу метки из строя.
- EPC поле (Electronic Product Code) хранит уникальный идентификатор метки, по которому они отличаются от остальных RFID-меток. Размер поля составляет от 96 до 240 бит, что позволяет реализовать запись сетевого адреса.

- TID поле (Transponder ID) хранит данные о производителе и модели чипа метки. Это поле защищено от перезаписи и является гарантированно уникальным.
- User Memory – поле данных пользователя. Принимает размер от 32 до 512 бит.

Исходя из полученных данных, можно увидеть, что в метке Gen2 возможно использование несколько технологий: реализованных компанией и тех, что были предложены ранее. Комбинация этих решений позволяет значительно увеличить уникальность идентификации и обеспечивает базовый контроль доступа к данным.

Однако стоит учесть, что RFID-метку легко уничтожить мощной атакой электромагнитного излучения: некоторые компоненты чипа будут выжжены, и это нельзя определить лишь по внешнему виду метки. Также метку, использующую в качестве доступа пароль можно взломать обычным осциллографом. Аналитики выявляли на экране пики, соответствующие неверным битам и повторяли процедуру аутентификации с модификацией пароля [10]. Создание программы подбора пароля самоуничтожения и использование её в обычном телефоне представляет большую угрозу меткам, с подобной функциональностью.

Использование радиочастотной связи ближнего действия (NFC) позволяет обезопасить метку от атак на расстоянии. Из-за малого радиуса действия (до 20 см) злоумышленник будет вынужден находится непосредственно рядом с атакованным устройством. Это усложняет процесс атаки и увеличивает шанс обнаружения атакующего.

Устройства NFC способны принимать и передавать данные одновременно, что позволяет контролировать радиочастотное поле и выявлять несоответствия при обмене данными. В случае обнаружения попытки взлома устройство может сбросить соединение.

Сравнение обозреваемых вариантов радиочастотной идентификации IoT-устройств

Учитывая ограниченную вычислительную мощность устройств Интернета Вещей, необходимость увеличения продолжительности работы за счёт экономии потребления энергии, крайне желательно использовать простые и компактные методы идентификации. Среди аппаратных решений наиболее лидирующее положение у технологии радиочастотной идентификации. Ниже в таблице приводится сравнение двух технологий радиочастотной идентификации: RFID и NFC.

ТАБЛИЦА. Сравнение технологий радиочастотной идентификации: RFID и NFC

Характеристики технологии	RFID	NFC
Дальность сигнала	До 20 м	До 20 см
Двусторонняя связь	Крайне ограничена, зависит от модели метки	Возможна.
Взаимодействие с устройствами	Ограничено пассивным поведением RFID-метки	Используется NFC-совместимыми устройствами (мобильные телефоны, планшеты) для передачи данных/эмуляции RFID
Объем передачи данных	Ограничен памятью метки	Зависит от используемого устройства.
Шифрование	Отсутствует	Уровень шифрования зависит от вычислительной мощности IoT-устройства

NFC в связке с совместимым устройством представляет собой более гибкий инструмент для реализации уникальной идентификации IoT-устройств в сравнении с технологией RFID. RFID дешевле, чем NFC и рекомендуется к использованию в тех системах, где охрана безопасности данных не является критически важным элементом.

Заключение

В данной статье были рассмотрены различные способы идентификации IoT-устройств. Раскрыты положительные и отрицательные стороны некоторых технологий. Можно сказать, что для достаточно надёжной, уникальной идентификации в критически важных областях, где защита данных является первоочередной задачей, желательно комплексное использование различных способов идентификации, рассмотренных в статье.

Библиографический список

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

2. **Кучерявый А. Е.** Интернет Вещей / А. Е. Кучерявый // Электросвязь. – 2013. – № 1. – С. 21–24.

3. **Киричек Р. В.** Ложные облака для интернета вещей. Методы защиты / Р. В. Киричек, В. А. Кулик, А. Г. Владыко, И. А. Богданов, А. Е. Кучерявый // Информационные технологии и телекоммуникации. – 2015. – № 3 (11). – С. 27–39.

4. **Cruz L.** Securing of Internet of Things [Электронный ресурс] / L. Cruz. – Режим доступа: http://newsroom.cisco.com/press-release-content?type=webcontent& articleId= 1158640

5. **Loughlin T.** Z-Wave Christmas Lights / T. Loughlin, 22 ноября 2012.

6. **Stollman J.** Concepts of Identity within the Internet of Things [Электронный ресурс] / J. Stollman, I. Friese. – Режим доступа: https://kantarainitiative.org/ confluence/display/IDoT/Concepts+of+Identity+within+the+Internet+of+Things

7. **Salman M.** On Identification of Internet of Things / M. A. Salman // International Journal of Sciences: Basic and Applied Research, 2014

8. **Олссон Д.** Раскрываем тайны 6LOWPAN / J. Olsson // НОВОСТИ ЭЛЕКТРОНИКИ. – 2015. – № 11.

9. **Stephan H.** The Things in the Internet of Things / H. Stephan. – SAP Research Center Zurich.

10. **Roberti M.** RFID Security: a Reality Check [Электронный ресурс] / M. Roberti. – Режим доступа: http://www.rfidjournal.com/articles/view?2170

References

1. **Kucherjavyj A. E.** Samoorganizujushhiesja seti / A. E. Kucherjavyj, A. V. Prokop'ev, E. A. Kucherjavyj. – SPb. : Ljubavich, 2011. – 311 s.

2. **Kucherjavyj A. E.** Internet Veshhej / A. E. Kucherjavyj // Jelektrosvjaz'. – 2013. – № 1. – S. 21–24.

3. **Kirichek R. V.** False clouds for Internet of Things. Methods of protection / R. V. Kirichek, V. A. Kulik, A. G. Vladyko, I. A. Bogdanov, A. E. Koucheryavy // IT&Telecom. – 2015. – № 3 (11). – PP. 27–39.

4. **Cruz L.** Securing of Internet of Things [Electronic resource] / L. Cruz. – Access mode: http://newsroom.cisco.com/press-release-content?type=webcontent&articleId=1158640

5. **Loughlin T.** Z-Wave Christmas Lights / T. Loughlin, 22. 11.2012.

6. **Stollman J.** Concepts of Identity within the Internet of Things [Electronic resource] / J. Stollman, I. Friese. – Access mode: https://kantarainitiative.org/confluence/display/IDoT/Concepts+of+Identity+within+the+Internet+of+Things

7. **Salman M.** On Identification of Internet of Things / M. A. Salman // International Journal of Sciences: Basic and Applied Research, 2014.

8. **Olsson D.** Raskryvaem tajny 6LOWPAN / J. Olsson // NOVOSTI ELEKTRONIKI. – 2015. – № 11.

9. **Stephan H.** The Things in the Internet of Things / H. Stephan. – SAP Research Center Zurich.

10. **Roberti M.** RFID Security: a Reality Check [Electronic resource] / M. Roberti. – Access mode: http://www.rfidjournal.com/articles/view?2170

Воеводин Юрий Витальевич – студент группы СП-21 Федерального государственного бюджетного образовательного учреждения высшего образования «Санкт-Петербургский государственный университет телекоммуникаций им. проф. М. А. Бонч-Бруевича»

Киричек Руслан Валентинович – кандидат технических наук, доцент кафедры «Сети связи и передача данных» Федерального государственного бюджетного образовательного учреждения высшего образования «Санкт-Петербургский государственный университет телекоммуникаций им. проф. М. А. Бонч-Бруевича», kirichek@sut.ru

УДК 004.414.22

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

K. N. Danilov Bonch-Bruevich Saint-Petersburg State University of Telecommunication

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

R. V. Kirichek Bonch-Bruevich Saint-Petersburg State University of Telecommunication

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

V. A. Kulik Bonch-Bruevich Saint-Petersburg State University of Telecommunication

МЕТОДЫ ОБНАРУЖЕНИЯ ИНТЕРНЕТ ВЕЩЕЙ В ГЛОБАЛЬНОЙ СЕТИ

METHODS FOR DETECTION OF INTERNET OF THINGS IN THE GLOBAL NETWORK

В данной статье рассматриваются методы обнаружения на основе анализа сетевого трафика и на основе сканирования открытых сетевых портов. Проводится ряд экспериментов по подтверждению возможности применения данных методов обнаружения на практике.

This paper discusses the methods of detection based on analysis of network traffic based on the scanning open network ports. It held a series of experiments to confirm the possibility of using these detection methods in practice.

Интернет Вещей, интернет вещь, анализ трафика, сетевой порт, сканирование, тестирование.

Internet of Things, the Internet thing, traffic analysis, network port scanning, testing.

Введение

В настоящее время, Интернет Вещей является одним из актуальнейших направлений в развитии телекоммуникаций [1, 2]. Разнотипность Интернет Вещей и отсутствие единого стандарта по межмашинному взаимодействию поднимет проблему безопасности передачи пользовательских данных в сетях пост-NGN.

Одной из проблем является взаимодействие Интернет Вещей по открытому каналу связи, что предоставляет возможность перехвата пользова-

тельских данных злоумышленниками. Именно поэтому тестирование Интернет Вещей на наличие уязвимостей безопасности, в частности передачи конфиденциальных данных, является важной исследовательской задачей [3, 4].

В данной статье будет рассмотрены методы обнаружения Интернет Вещей на основе захвата и анализа машинного трафика и сканирования открытых сетевых портов.

1 Обнаружение Интернет Вещей на основе анализа сетевого трафика

Одним из методов обнаружения Интернет Вещи является анализ сетевого трафика на промежуточном узле в сети связи (например, маршрутизатор) [3]. Данный метод заключается в перехвате и анализе трафика, идущего от локальной подсети, имеющей в своем составе Интернет Вещи.

Сетевой трафик, создаваемый Интернет Вещью имеет ряд параметров, позволяющих отличить устройства Интернета Вещей от других устройств, подключенных к сети связи общего пользования [5], таких как:

- длина пакетов;
- интервалы времени между отправляемыми пакетами;
- определенные сетевые порты, используемые в ИВ;
- информацию, находящуюся в поле данных.

Данные параметры будут отличаться для различных типов Интернет Вещей. На данный момент, основными типами Интернет Вещей являются [6]:

1) Сенсор – Интернет Вещь, собирающая показания с различных датчиков и отправляющая ее в сеть Интернет [7]. ИВ данного типа, характеризуются:

- большим размером заголовка, по сравнению с размером поля данных;
- периодичными интервалами времени отправки данных (самоподобный трафик) для контроля состояния датчиков в режиме реального времени (далее самоподобный сценарий) и интенсивной непериодичной отправкой данных (антиперсистентный трафик), начинаемой по определенному условию, параметром которого являются снимаемые с датчиков показания (антиперсистентный сценарий);
- стандартными сетевыми портами, используемыми протоколами передачи данных Интернета Вещей. Например, протокол CoAP – порт 5683, протокол MQTT – порты 1883, 8883, 8884, протокол HTTP – порт 80, протокол HTTPS – порт 8080, протокол XMPP – порты 5222, 5269;
- информация, находящейся в поле данных пакета может содержать идентификационный номер Интернет Вещи на сервере (или адрес, закрепленный за данной ИВ на сервере), тип отправляемых данных,

тип устройства и т. д. Формат поля данных определяет используемый протокол прикладного уровня.

2) Актуатор – Интернет Вещь, отправляющая сигналы управления на устройство воздействия на окружающий мир (например, звуковая и световая сигнализация), по сигналу, полученному из сети Интернет. ИВ данного типа имеют схожие параметры с ИВ типа Сенсор, но имеют следующие отличия:

- устройство не отправляет какие-либо данные, за исключением служебного трафика, используемого для поддержания сеанса связи и подтверждения функционирования устройства на удаленном сервере управления;
- стандартные протоколы прикладного уровня, используемые ИВ для обмена информацией в сети стандарта IPv4, в большинстве случаев, основываются на транспортном протоколе TCP. Данный протокол используется для организации сеанса связи между устройством ИВ (в случае, если оно не имеет внешнего IPv4 адреса) и удаленным сервером управления.

3) Шлюз – Интернет Вещь, преобразующая пакеты, полученные от Интернет Вещей, в формат пакетов, используемых в сети общего пользования [2]. ИВ данного типа имеют схожие параметры с ИВ типа Сенсор, но имеют следующие отличия:

- все пакеты, отправляемые устройствами, подключенными к шлюзу в поле IP-адрес источника, будут иметь IP-адрес шлюза. В связи с этим время отправки пакетов Интернет Вещью данного типа недетерминируемо. Для определения сценария работы ИВ, необходимо обнаружить пакеты, принадлежащие отдельным Интернет Вещам и далее провести анализ трафика для определения сценария взаимодействия. Пакеты можно обнаружить методом анализа поля данных на дублирующуюся информацию в различных пакетах.
- сетевые порты, в зависимости от алгоритма работы устройства, могут использоваться для возможности обращения к конкретной Интернет Вещи, подключенной к шлюзу, путем назначения данной ИВ определенного порта.

Также Интернет Вещи делятся, как было сказано выше, по типам сценариям работы, на ИВ с самоподобным сценарием и ИВ с антиперсистентным сценарием.

На основе модельной сети лаборатории Интернета Вещей СПбГУТ [8] был разработан экспериментальный стенд с функцией обнаружения Интернет Вещей на основе анализа трафика, который изображен на рисунке.

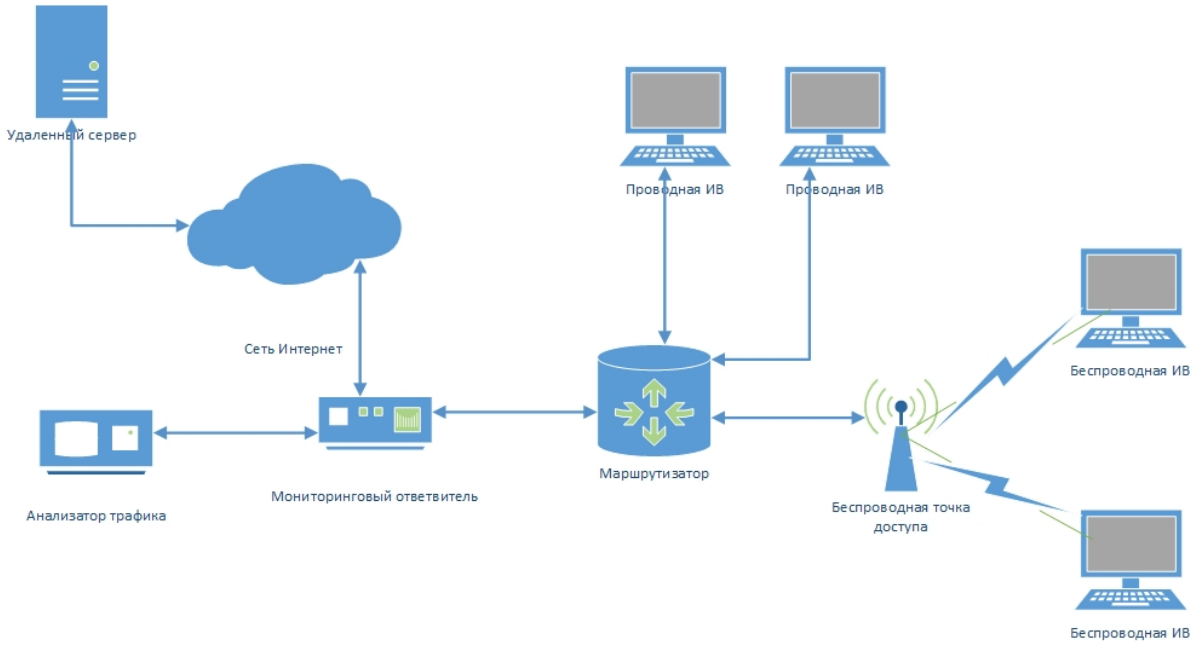


Рисунок. Схема сети с функцией обнаружения Интернета Вещей на основе анализа трафика

Мониторинговый ответвитель и анализатор трафика изображенные на схеме в совокупности представляют собой систему обнаружения Интернет Вещей в локальной подсети. В частности, мониторинговый ответвитель отвечает за дублирование трафика, идущего к удаленному серверу, а анализатор трафика отвечает за обнаружение пактов, идущих от Интернет Вещей.

Данная система обнаружения Интернет Вещей позволяет опознавать любой из наиболее используемых типов Интернет Вещей, вне зависимости от протокола ее функционирования, но в тоже время для обнаружения Интернет Вещей, функционирующий в какой-либо подсети, необходимо иметь доступ к каналу связи, по которому данные из подсети поступают в глобальную сеть, доступ к которому, чаще всего, ограничен. Данная проблема поднимает вопрос возможности обнаружения устройств Интернета Вещей удаленным узлом, не имеющим доступ к каналу связи, по которому проходит трафик из исследуемой подсети.

2 Обнаружение Интернет Вещей на основе сканирования открытых сетевых портов

Для решения проблемы обнаружения Интернет Вещей без доступа к каналу связи, по которому проходит трафик искомых ИВ, предлагается использовать существующие методы сканирования устройств, подключенных к сети Интернет, на наличие открытых портов сетевого взаимодействия. В связи с тем, что для организации сетевого взаимодействия в Интернете Вещей чаще всего используются протоколы транспортного уровня

TCP [9] и UDP [10], то и сканирование будет проводиться для обнаружения портов TCP и UDP.

Существует несколько способов выполнения сканирования TCP-портов. Наиболее быстрый и легко реализуемый способ использует сетевые функции операционной системы, где находится виртуальное сканирующие устройство. Виртуальное сканирующее устройство проводит анализ наличия на сканируемом узле сети открытых сетевых портов методом последовательного перебора портов. Если порт исследуемого устройства открыт, то операционная система совершает трёхэтапную процедуру установления соединения, после которой подтверждается доступность порта для соединения, затем соединение закрывается. Для ускорения процесса последовательного перебора портов, используется метод параллельного сканирования, когда одновременно, с различных портов виртуального сканера, происходит сканирование двух и более портов исследуемого узла сети.

Сканирование UDP-портов более трудоемкий и ресурсозатратный процесс, так как для протокола UDP отсутствует понятие сеанса связи, и нет гарантии, что данные дойдут до порта анализируемого устройства. Несмотря на это, сканирование возможно, потому что большинство узлов связи отвечают на прибывший, на закрытый UDP-порт, пакет – отправкой ICMP сообщения, в котором говорится о недоступности данного сетевого порта, а отсутствие данного сообщения говорит о том, что порт UDP открыт. В связи с тем, что при передачи данных с помощью протокола UDP нет гарантии их доставки, был сделан вывод, что при сканировании UDP-портов данным методом, необходимо отправлять множество запросов на каждый порт сканируемого устройства.

Большинство интернет вещей используют определенные протоколы для передачи данных, которые, как было сказано выше, занимают определенные сетевые порты. Примером могут послужить *CoAP* [11], *MQTT* [12], *HTTP* [13], *HTTP/2* [14], *RTMP* [15], *RTSP* [16] и другие. Номера данных фиксированных портов определяет некоммерческая организация «*Internet Assigned Numbers Authority*» (далее «*IANA*»), которые используются для определенных целей, и устанавливает соответствие между ними и используемыми протоколами прикладного уровня. С помощью сопоставления списка обнаруженных сетевых портов на сканируемом устройстве и базы данных «*IANA*» можно определить используемый на данном сетевом порту прикладной протокол передачи данных.

Другие порты, не занесенные в базу данных «*IANA*» и использующие для передачи данных протокол *TCP*, как правило, на любой запрос отправляют ответ. Благодаря ответу, поступившему от устройства, можно определить по какой протокол прикладного уровня использует порт.

Для определения типа Интернет Вещи необходимо провести анализ поля данных поступившего на запрос ответа. Например, ответы на HTTP-

запросы могут содержать информацию об устройстве, например, название операционной системы или производителя.

Отличным примером может послужить следующий HTTP-заголовок:

- *HTTP/1.1 200 OK;*
- *Date: Wed, 26 Jan 2016 11:06:42 GMT;*
- *Server: Linux/2.x UPnP/1.0 Avtech/1.0;*
- *Connection: close;*
- *Last-Modified: Wed, 08 Jan 2014 09:36:39 GMT;*
- *Content-Type: text/html.*

Заголовок «*Server*» содержит следующую полезную информацию:

- *Linux/2.x* – ядро операционной системы, которая используется устройством;
- *UPnP* – технология, включающая в себя набор сетевых протоколов, предназначена для объединения устройств в домашней или корпоративной среде;
- *Avtech* – производитель видеокамер.

В данном случае можно сделать вывод, что устройство, от которого получен ответ, является видеокамерой.

Множество устройств, которые используются в Интернете Вещей (особенно серийные, такие как видеокамеры, бытовая техника и т. д.) имеют интерфейс веб-взаимодействия. Анализ информации с веб-страниц таких устройств может позволить определить его тип. Стоит отметить, что такой способ определения типа Интернет Вещи становится более актуальным, в связи с появлением концепции *Web of Things* [17], которая говорит о том, что каждое устройство Интернет Вещей должно иметь интерфейс веб-взаимодействия.

Однако, отсутствие веб-страницы на устройстве или отсутствие открытых сетевых портов, работающих по протоколам *HTTP, HTTPS, HTTP/2*, не означает, что устройство не является интернет вещью. Существует множество других протоколов взаимодействия Интернета Вещей, которые не поддерживают концепцию Web of Things, но также подключены к сети Интернет. В связи с этим сканирующему устройству, для анализа информации, содержащийся в поле данных полученных пакетов, необходимо иметь в своей базе данных форматы ответов для каждого из популярных протоколов для Интернета Вещей.

Анализ всей доступной об устройстве информации, по определенным алгоритмам, позволяет определить является ли оно Интернет Вещью, его тип, а также получить доступ к нему для взаимодействия.

Для исследования возможности обнаружения Интернет Вещей на основе сканирования открытых сетевых портов, с помощью языка программирования *Java* и принципов сканирования открытых сетевых портов, описанных выше, было разработано программное обеспечение для обна-

ружения Интернет Вещей и определения их типа на, указанном в параметрах приложения *IP*-адресу, узле связи.

Алгоритм работы программы состоит из последовательности шагов, приведенных ниже.

Шаг 1. Определяется доступность удаленного узла, а затем происходит поиск открытых портов. Сканирование всех портов проводится одновременно. Таким образом скорость сбора информации зависит от времени ожидания ответа каждого из портов

Шаг 2. Если сканируемый порт является открытым, то происходит определение протокола, который он использует в своей работе. Для увеличения быстродействия программы мы ограничились лишь списком протоколов прикладного уровня, используемых в Интернете Вещей. Данный список сопоставлялся со списком обнаруженных открытых сетевых портов на исследуемом узле связи.

Шаг 3. Производится поиск дополнительной информацию об устройстве, которую мы можем получить, анализируя ответ, приходящий на запрос подключения. В качестве примера можно привести информацию, полученную с заголовка *HTTP*-ответа, или список опций, содержащихся в заголовке RTSP-ответа.

Таким образом, в ходе вышеописанного эксперимента, удалось подтвердить возможность обнаружения ИВ методом сканирования открытых сетевых портов. В частности, удалось определить номера открытых сетевых портов, протоколы взаимодействия, использующие данный сетевой порт, а также некоторую дополнительную информация о самой Интернет Вещи.

Заключение

В данной статье были рассмотрены два метода обнаружения Интернет Вещей, подключенных к глобальной сети и проведены эксперименты, подтвердившие их работоспособность практически. С помощью метода обнаружения Интернет Вещей на основе анализа сетевого трафика, в большинстве случаев система обнаружения может определить саму Интернет Вещь и ее тип (в зависимости от сложности алгоритма анализа трафика), но данный метод работоспособен только лишь в случае, когда имеется доступ к каналу связи, по которому проходит трафик Интернета Вещей, что делает невозможным их обнаружение устройством в сети Интернет, не имеющим доступ к нему. Второй метод – метод обнаружения Интернет Вещей на основе сканирования открытых сетевых портов, в случае с сетевыми портами, использующими протокол транспортного уровня *UDP*, не позволяют определить тип устройства, но второй метод позволяет обнаружить устройства Интернета Вещей из любой точки сети Интернет, не имея доступа к генерируемому ею трафику.

Библиографический список

1. **Кучерявый А. Е.** Интернет Вещей / А. Е. Кучерявый // Электросвязь. – 2013. – № 1. – С. 21–24.

2. **Кучерявый А. Е.** Самоорганизующиеся сети / А. Е. Кучерявый, А. В. Прокопьев, Е. А. Кучерявый. – СПб. : Любавич, 2011. – 311 с.

3. **Богданов И. А.** Характеристики жизненного цикла мобильной сенсорной сети при различных потоках ложных событий / И. А. Богданов, А. И. Парамонов, А. Е. Кучерявый // Электросвязь. – 2013. – № 1. – С. 32–33.

4. **Васильев А. Б.** Тестирование сетей связи следующего поколения / А. Б. Васильев, Д. В. Тарасов, Д. В. Андреев, А. Е. Кучерявый. – М. : ФГУП ЦНИИС, 2008. – 144 с.

5. **Киричек Р. В.** Ложные облака для интернета вещей. Методы защиты / Р. В. Киричек, В. А. Кулик, А. Г. Владыко, И. А. Богданов, А. Е. Кучерявый // Информационные технологии и телекоммуникации. – 2015. – № 3 (11). – С. 27–39.

6. **Peter Waher** // Learning Internet of Things. – Birmingham, UK, Packt Publishing Ltd. // Jan 2015.

7. **Кучерявый А. Е.** Эволюция исследований в области беспроводных сенсорных сетей / А. Е. Кучерявый, Р. В. Киричек, А. И. Парамонов, А. В. Прокопьев // Информационные технологии и телекоммуникации. – 2014. – № 4 (8). – С. 29–41.

8. **Kirichek R.** Internet of Things Laboratory Test Bed / R. Kirichek, A. Koucheryavy // International Conference on Wireless Communication, Networking and Application. WCNA 2014. – LNEE. – Vol. 348. – Heidelberg: Springer, 2016.

9. **Postel J.** RFC: 793. Transmission Control Protocol / J. Postel // Information Sciences Institute University of Southern California // September 1981

10. **Postel J.** RFC: 768. User Datagram Protocol / J. Postel // ISI // 28 August 1980

11. **Shelby Z.** RFC: 7252. The Constrained Application Protocol (CoAP) / Z. Shelby, K. Hartke, C. Bormann // Internet Engineering Task Force (IETF) // Universitaet Bremen TZI June 2014.

12. **Cohn Raphael J.** MQTT Version 3.1.1 / Raphael J. Cohn, Richard J. Coppen (IBM) // OASIS Standard // Oct 2014.

13. **Fielding R.** RFC: 2616. Hypertext Transfer Protocol -- (HTTP/1.1) / R. Fielding, J. Gettys, J. Mogul // Network Working Group // UC Irvine, Compaq, W3C // June 1999.

14. **Belshe M.** RFC: 7540. Hypertext Transfer Protocol Version 2 (HTTP/2) / M. Belshe, R. Peon // Internet Engineering Task Force (IETF) // BitGo, Google Inc. // May 2015.

15. **Parmar H.** Adobe's Real Time Messaging Protocol / H. Parmar, M. Thornburgh // Adobe // December 21, 2012.

16. **Schulzrinne H.** RFC: 2326. Real Time Streaming Protocol (RTSP) / H. Schulzrinne, A. Rao, R. Lanphier // Network Working Group // Columbia U., Netscape, RealNetworks // April 1998.

17. **Guinard Dominique** From the Internet of Things to the Web of Things: Resource Oriented Architecture and Best Practices / Dominique Guinard, Vlad Trifa, Friedemann Mattern, Erik Wilde // Springer. – PP. 97–129.

References

1. **Kucherjavyj A. E.** Internet Veshhej / A. E. Kucherjavyj // Jelektrosvjaz'. – 2013. – № 1. – S. 21–24.

2. **Kucherjavyj A. E.** Samoorganizujushhiesja seti / A. E. Kucherjavyj, A. V. Prokop'ev, E. A. Kucherjavyj. – SPb. : Ljubavich, 2011. – 311 s.

3. **Bogdanov I. A.** Harakteristiki zhiznennogo cikla mobil'noj sensornoj seti pri razlichnyh potokah lozhnyh sobytij / I. A. Bogdanov, A. I. Paramonov, A. E. Kucherjavyj // Jelektrosvjaz'. – 2013. – № 1. – S. 32–33.

4. **Vasil'ev A. B.** Testirovanie setej svjazi sledujushhego pokolenija / A. B. Vasil'ev, D. V. Tarasov, D. V. Andreev, A. E. Kucherjavyj. – M. : FGUP CNIIS, 2008. – 144 s.

5. **Kirichek R. V.** False clouds for Internet of Things. Methods of protection / R. V. Kirichek, V. A. Kulik, A. G. Vladyko, I. A. Bogdanov, A. E. Koucheryavy // IT&Telecom. – 2015. – № 3 (11). – PP. 27–39.

6. **Peter Waher** // Learning Internet of Things. – Birmingham, UK, Packt Publishing Ltd. // Jan 2015.

7. **Koucheryavy A. E.** The Investigation evolution in the wireless sensor networks area / A. E. Koucheryavy, R. V. Kirichek, A. I. Paramonov, A. V. Prokopiev // IT&Telecom. – 2014. – № 4 (8). – PP. 29–41.

8. **Kirichek R.** Internet of Things Laboratory Test Bed / R. Kirichek, A. Koucheryavy // International Conference on Wireless Communication, Networking and Application. WCNA 2014. – LNEE. – Vol. 348. – Heidelberg: Springer, 2016.

9. **Postel J.** RFC: 793. Transmission Control Protocol / J. Postel // Information Sciences Institute University of Southern California // September 1981

10. **Postel J.** RFC: 768. User Datagram Protocol / J. Postel // ISI // 28 August 1980

11. **Shelby Z.** RFC: 7252. The Constrained Application Protocol (CoAP) / Z. Shelby, K. Hartke, C. Bormann // Internet Engineering Task Force (IETF) // Universitaet Bremen TZI June 2014.

12. **Cohn Raphael J.** MQTT Version 3.1.1 / Raphael J. Cohn, Richard J. Coppen (IBM) // OASIS Standard // Oct 2014.

13. **Fielding R.** RFC: 2616. Hypertext Transfer Protocol -- (HTTP/1.1) / R. Fielding, J. Gettys, J. Mogul // Network Working Group // UC Irvine, Compaq, W3C // June 1999.

14. **Belshe M.** RFC: 7540. Hypertext Transfer Protocol Version 2 (HTTP/2) / M. Belshe, R. Peon // Internet Engineering Task Force (IETF) // BitGo, Google Inc. // May 2015.

15. **Parmar H.** Adobe's Real Time Messaging Protocol / H. Parmar, M. Thornburgh // Adobe // December 21, 2012.

16. **Schulzrinne H.** RFC: 2326. Real Time Streaming Protocol (RTSP) / H. Schulzrinne, A. Rao, R. Lanphier // Network Working Group // Columbia U., Netscape, RealNetworks // April 1998.

17. **Guinard Dominique** From the Internet of Things to the Web of Things: Resource Oriented Architecture and Best Practices / Dominique Guinard, Vlad Trifa, Friedemann Mattern, Erik Wilde // Springer. – PP. 97–129.

Данилов Кирилл Николаевич – студент группы СП-21 Федерального государственного бюджетного образовательного учреждения высшего образования «Санкт-Петербургский государственный университет телекоммуникаций им. проф. М. А. Бонч-Бруевича»

Киричек Руслан Валентинович – кандидат технических наук, доцент кафедры «Сети связи и передача данных» Федерального государственного бюджетного образовательного учреждения высшего образования «Санкт-Петербургский государственный университет телекоммуникаций им. проф. М. А. Бонч-Бруевича», kirichek@sut.ru

Кулик Вячеслав Андреевич – студент группы ИКТИ-53м Федерального государственного бюджетного образовательного учреждения высшего образования «Санкт-Петербургский государственный университет телекоммуникаций им. проф. М. А. Бонч-Бруевича», vslav.kulik @gmail.com

УДК 621.396

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

Ch. Z. Dinh Bonch-Bruevich Saint-Petersburg State University of Telecommunications

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

A. I. Paramonov Bonch-Bruevich Saint-Petersburg State University of Telecommunications

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

R. V. Kirichek Bonch-Bruevich Saint-Petersburg State University of Telecommunications

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

A. E. Koucheryavy Bonch-Bruevich Saint-Petersburg State University of Telecommunications

МЕТОДЫ ИНСТАЛЛЯЦИИ СЕНСОРНЫХ УЗЛОВ С КВАДРОКОПТЕРА ОБЩЕГО ПОЛЬЗОВАНИЯ

METHODS OF INSTALLATION SENSOR NODES WITH PUBLIC QUADROCOPTERS

В статье представлено сравнение способов инсталляции сенсорных узлов для покрытия заданной области при использование различных способов: случайного размещения и детерминированного размещения. Рассмотрены методы повышения энергоэффективности сенсорных узлов и квадрокоптера.

The paper compares the methods of installation of sensor nodes to cover a given area with the use of various methods: random and deterministic placement offering. The methods of increasing energy efficiency of sensor nodes and quadrocopters.

беспроводная сенсорная сеть, сенсорные узлы, инсталляция, случайный метод, детерминированный метод, энергоэффективности, БПЛА, квадрокоптер.

wireless sensor network, sensor nodes, installation, random method, deterministic method, energy efficiency, UAVs, quadrocopter.

В последние годы исследования в области беспроводных сенсорных сетей (БСС) пополнились новым направлением – летающими сенсорными сетями (ЛСС). В качестве летающих узлов используются общедоступные

беспилотные летающие аппараты (БПЛА) общего назначения – квадрокоптеры [1, 2]. Использование квадрокоптеров в качестве временного головного узла в БСС – это новый поход, который улучшает качество сбора данных, а также продлевает жизненный цикл сенсорных узлов. Использование квадрокоптера, в ряде случаев, позволяет не только расширить возможности по организации связи между узлами, но и произвести физическую инсталляцию узлов. В данной работе, будем рассматривать квадрокоптер как средство инсталляции беспроводных сенсорных узлов на заданной области с целью последующего сбора данных.

В статье рассмотрены два аспекта функционирования БСС: во-первых, обеспечение покрытия территории, для чего используется алгоритм случайной инсталляции сенсорных узлов с применением квадрокоптера и последующей оценкой качества покрытия заданной области. Во-вторых, повышение энергоэффективности сети, для чего использован метод повышения энергоэффективности сенсорных узлов и квадрокоптера.

Как известно, существует два основных способа инсталляции узлов в беспроводной сенсорной сети: случайное размещение и детерминированное размещение [3]. Случайное размещение обычно используются для крупномасштабных БСС не только потому, что это требует меньших затрат, но также и потому, что в ряде случаев, такой способ может быть единственно возможным. Однако случайное размещение сенсорных узлов может привести к появлению неконтролируемых зон; поэтому, в большинстве случаев, случайное размещение, не будет эффективно для достижения максимального покрытия [4].

В статье, рассмотрена вероятность покрытия при случайном размещении сенсорных узлов на заданной территории. Мы использовали двоичную модель, которая рассмотрена в [5]. В этой модели, каждый сенсорный узел имеет одинаковый и постоянный радиус действия сенсора. Область обслуживания накроем сеткой линий n x m, с размером каждой ячейки сетки равен 1. Двоичная модель предполагает, что доля покрытия области в границах обслуживания аппроксимируется долей покрытых узлов сетки. Покрытие всей области пропорционально числу покрытых узлов решетки. Для описания покрытия узлов сетки $G(x, y)$ введем двоичную функцию, значение которой равно 1, если узел попадает в зону покрытия сенсора $s_i(x_i, y_i)$ и 0, в противном случае

$$I(x, y, s_i) = \begin{cases} 1 & \text{, если } \sqrt{(x - x_i) + (y - y_i)} < R_s \\ 0 & \text{, в ином случае} \end{cases}.$$

Рис. 1 иллюстрирует приведенное выражение.

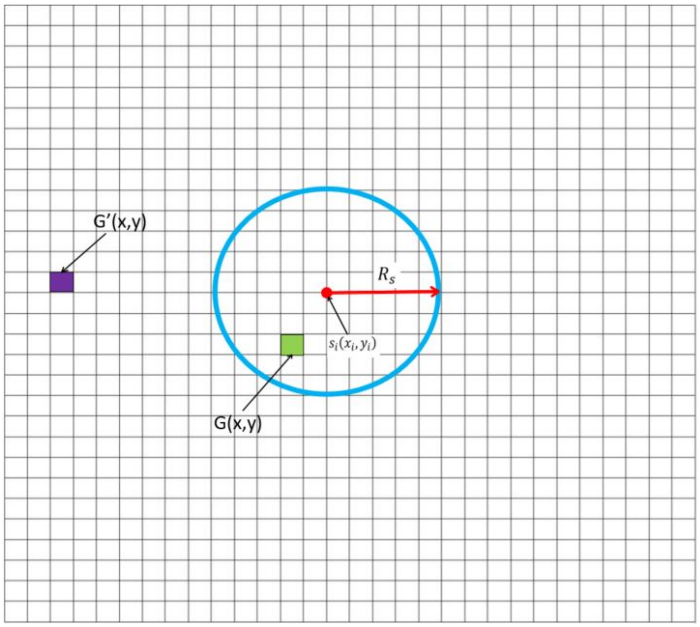


Рис. 1. Покрытие узлов сетки сенсорным узлом

$$\mathrm{A}_{\text{пок}}(S) = \cup_{i=1}^{N} A_{s_i} \cong \frac{A}{m \cdot n} \sum_{x=1}^{m} \sum_{y=1}^{n} I(x, y, S),$$

где A – общая область с размером n (м) на m (м).

Площадь непокрытой области составит:

$$\mathrm{A}_{\text{не пок}}(S) = A - \mathrm{A}_{\text{пок}}(S).$$

Вероятность покрытия может быть определена как:

$$P_{\text{вер}} = \frac{\mathrm{A}_{\text{пок}}(S)}{\mathrm{A}} \cong \frac{\sum_{x=1}^{m} \sum_{y=1}^{n} I(x,y,S)}{m * n},$$

где A – общая область с размером n (м) на m (м).

Для анализа зависимости доли покрытия зоны обслуживания от числа сенсорных узлов была разработана имитационная модель.

В области с размером 100×100 м размещено k = 0...200 узлов с радиусом покрытия R = 10 м. Точки размещения узлов определяются координатами (x_i, y_i), i = 1…k, где x_i и y_i случайные числа, имеющие равномерное распределение в интервале от 0 до 100. Результат моделирования приведен на рис. 2.

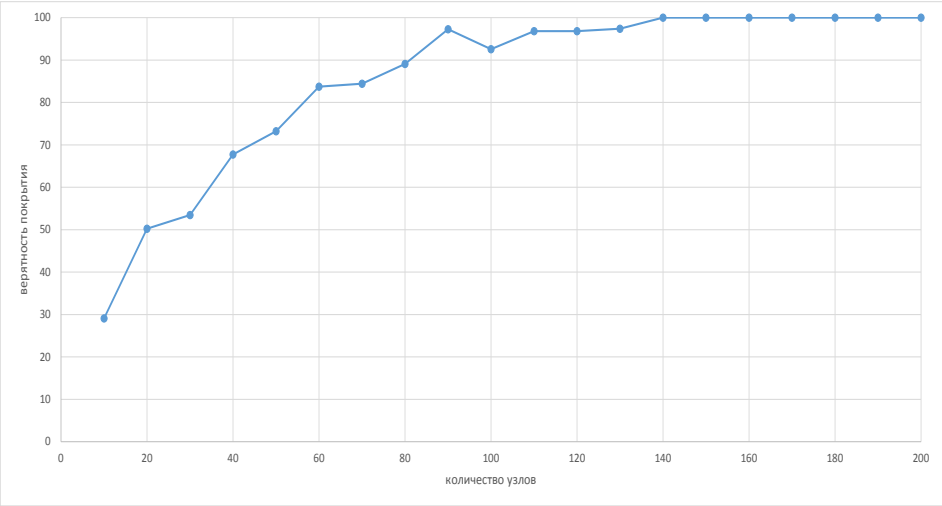


Рис. 2. Зависимость между количеством узлов и вероятностью покрытия (долей покрытой области)

Как видно из приведенных результатов моделирования вероятность покрытия возрастаем с ростом числа сенсорных узлов, а при значениях 140 и более узлов (более 0,014 узлов на м^2), близка к единице.

Сравнивая полученные результаты с детерминированным размещением узлов [6], можно заметить, что для обеспечения полного (100 %) покрытия аналогичной области требуется всего 58 сенсорных узлов (рис. 3).

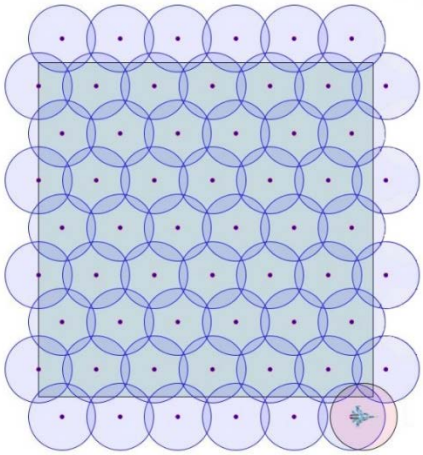


Рис. 3. Детерминированное размещение сенсорных узлов с использованием квадрокоптера общего пользования

Из сравнения видно, что при случайном размещении, для обеспечения близкого к 100 % покрытия требуется более, чем вдвое больше узлов, чем при их детерминированном размещении. Однако, стоит отметить, что при том же числе узлов (58) при случайном их распределении обеспечивается более 80 % покрытия территории. При детерминированном размещении узлов 100 % покрытие достигается лишь в идеальном случае, на практике имеет место ошибка их позиционирования, которая приводит к уменьшению доли покрытия. С учетом последнего можно полагать, что оба метода

сопоставимы по эффективности и должны выбираться исходя из конкретных условий.

Наряду с задачей покрытия территории актуальной задачей построения БСС является задача повышения эффективности энергопотребления. При использовании квадрокоптеров, необходимо обеспечить экономию не только энергии наземного сегмента сети, но и также энергию квадрокоптера. Полагаем, что квадрокоптер является элементом сети связи и выполняет облет узлов для сбора информации от сенсорных узлов наземного сегмента сети. Для экономии энергии квадрокоптера необходимо использовать некоторый алгоритм, позволяющий уменьшить время взаимодействия с узлами наземного сегмента ЛСС.

Кластерная организация сети считается эффективной и масштабируемой для решения подобных задач, но лишь при условии рационального выбора головного узла в кластерной сети в конкретный момент времени. При кластерной организации сети роли узлов периодически изменяются в соответствие и используемым алгоритмом кластеризации [8]. На основе работ [4, 6] был разработан алгоритм выбора головных узлов кластеров при детерминированном размещении сенсорных узлов в области обслуживания и съеме информации с них с помощью квадрокоптера. Данный алгоритм предполагает, что каждый из узлов сети может выполнять функции головного узла. Эти функции делегируются ему периодически, так чтобы каждый из узлов сети периодически становился головным узлом. Работа алгоритма проиллюстрирована на рис. 4. Головной узел кластера выделен красным цветом, члены кластера связаны с ним оранжевыми линиями. На рисунке приведены 4 раунда работы сети (смены роли узлов). За 4 раунда каждый из узлов сети единожды выполняет роль головного узла.

Экономия энергии расходуемой сетью достигается за счет того, что расстояния между головными узлами кластеров и узлами членами кластеров меньше расстояний между узлами сети и квадрокоптером, производящим сбор данных, а расход энергии на передачу данных пропорционален квадрату расстояния. Передача же данных на квадрокоптер осуществляется только головными узлами кластеров.

Согласно [7, 9] энергия, расходуемая каждым сенсорным узлом, будет равна:

$$E = E_{\text{прием}} + E_{\text{пер}},$$

$$E_{\text{пер}} = E_{\text{обр}} \cdot k + E_{\text{усил}} \cdot k \cdot d^2,$$

$$E_{\text{према}} = E_{\text{обр}} \cdot k,$$

где E – энергия затрачиваемая каждым сенсорным узлом, Дж;

$E_{\text{прием}}$ – энергия, затрачиваемая на прием информации, Дж;

$E_{\text{пер}}$ – энергия, затрачиваемая на передачу информации, Дж;
$E_{\text{обр}}$ – энергия затрачиваемая на обработку 1 бита информации, Дж;
k – размер сообщения, бит;
d – расстояние между узлами и квадракоптером, м.

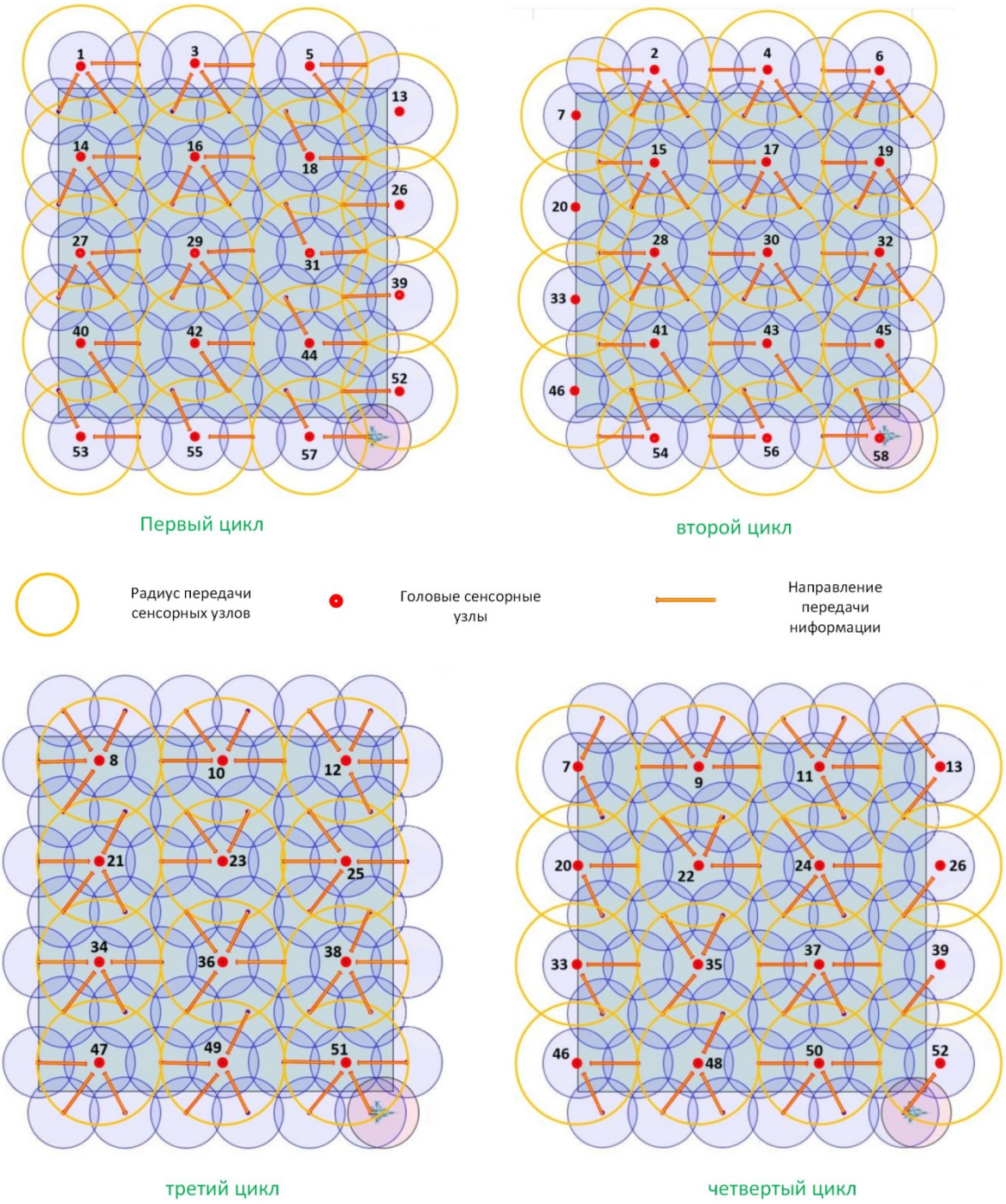


Рис. 4. Алгоритм выбора головных узлов
для детерминированного размещения сенсорных узлов в сенсорной области
с использованием квадрокоптера общего пользования

Энергия, затрачиваемая квадракоптером определяется как:

$$E_{\text{квад}} = N \cdot E_{\text{обр}} \cdot k + N \cdot \frac{d_k}{v} \cdot E_0 \,,$$

где $E_{\text{квад}}$ – энергия, затрачиваемая квадрокоптером на прием информации, Дж;

k – размер сообщения, бит;

d_k – расстояние между головными узлами кластеров (полагаем, что траектория движения квадрокоптера проходит над головными узлами кластеров), м;

N – количество головных узлов;

v – средняя скорость движения квадрокоптера, м/с;

E_0 – энергия, затрачиваемая квадрокоптером за единицу времени полета, Дж/с.

На рис. 5 приведены результаты моделирования расхода энергии при опросе каждого из узлов сети и при использовании алгоритма кластеризации и опросе только головных узлов кластеров.

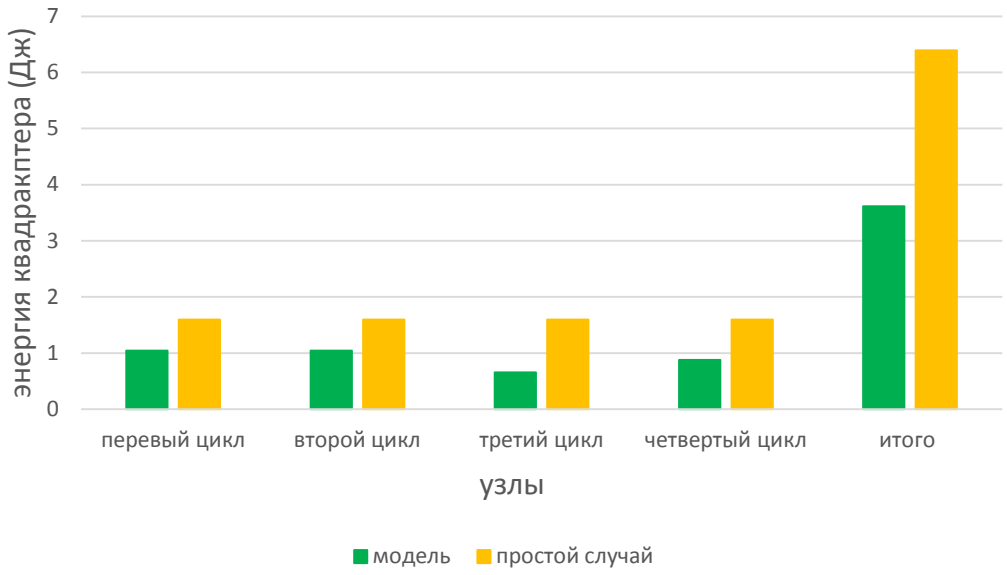


Рис. 5. Результаты моделирования расхода энергии квадрокоптера

Результаты получены для следующих исходных данных: $E_{\text{обр}} = 50$ нДж, $E_{\text{пер}} = 100$ пДж, $k = 200$ бит (длина сообщений от узлов к головным узлам), $k' = 6400$ бит (длина сообщений от головных узлов к квадрокоптеру), $d_k = 20$ м, $d = 10\sqrt{3}$ м. При использовании квадрокоптера 3D Robotics Iris+ [10], который оснащен аккумулятором емкостью 5100 мАч, 11,1 В, и способен работать в течение 20 минут (начальная энергия

квадрокоптера $E_0 = \frac{5100}{11.1*1000} * \frac{20}{60} =$ 18,87 Дж), при скорости полета v = 10 м/с.

Как видно из представленных результатов, предлагаемая модель обеспечивает снижение затрачиваемой на каждом цикле движения квадрокоптера энергии почти вдвое.

Выводы

- В результате данной работы получена сравнительная характеристика случайного и детерминированного методов размещения узлов сенсорной сети с целью обеспечения покрытия зоны обслуживания. Было показано, что детерминированный способ размещения узлов, при условии достаточно точного размещения узлов обеспечивает большую эффективность.
- Результаты проведенного анализа показали, что при ограниченной точности размещения узлов, а также при менее жестких требованиях к доле покрытия, случайное размещение узлов может быть сопоставимо по эффективности с детерминированным.
- Разработан метод организации беспроводной сенсорной сети при детерминированном размещении узлов и использовании квадрокоптера для выполнения операций сбора данных.
- Предложенный метод кластерной организации сети позволяет существенно снизить энергозатраты квадракоптера на работу по сбору данных.

В дальнейших исследованиях, предполагается исследовать модели случайного размещения сенсорных узлов, обеспечивающие покрытие заданной области наименьшим количеством узлов и методы минимизации расхода энергии в таких сетях.

Библиографический список

1. **Кучерявый А. Е**. Летающие сенсорные сети / А. Е. Кучерявый, А. Г. Владыко, Р. В. Киричек, А. И. Парамонов, А. В. Прокопьев, А. И. Богданов, А. А. Дорт-Гольц // Электросвязь. – 2014. – № 9. – С. 2–5.

2. **Киричек Р. В.** Эволюция исследований в области беспроводных сенсорных сетей // А. Е. Кучерявый, Р. В. Киричек, А. И. Парамонов, А. В. Прокопьев // Информационные технологии и телекоммуникации. – 2014. – № 4. – С. 29–41.

3. **Мочалов В. А.** Стратегии размещения узлов сенсорной сети / В. А. Мочалов, Е. Н. Турута // VII Международной научно-технической конференции, 23–27 ноября 2010 г, Москва.

4. **Динь Ч. З.** Обзор методов инсталляции сенсорных узлов с квадрокоптера / Ч. З. Динь, Р. В. Киричек, А. Е. Кучерявый // Информационные технологии и телекоммуникации. – 2015. – № 1 (9). – С. 51–63.

5. **Abo-Zahhad M.** Coverage maximization in mobile Wireless Sensor Networks utilizing immune node deployment algorithm / Mohammed Abo-Zahhad, Sabah M. Ahmed and

Nabil Sabor // Electrical and Computer Engineering (CCECE), 2014 IEEE 27th Canadian Conference on.

6. **Динь Ч. З.** Имитационная модель инсталляции сенсоров с квадрокоптера на заданной территории / Ч. З. Динь, Р. В. Киричек, А. И. Парамонов, А. Е. Кучерявый // Информационные технологии и телекоммуникации. – 2015. – № 2 (10). – С. 93–100.

7. **Heinzelman W. R.** Energy-Efficient Communication Protocol for Wireless Microsensor Networks / Wendi Rabiner Heinzelman, Anantha Chandrakasan, and Hari Balakrishnan // System Sciences, 2000. Proceedings of the 33rd Annual Hawaii International Conference on.

8. **Салим А.** Выбор головного узла кластера в однородной беспроводной сенсорной сети / А. Е. Кучерявый, А. Салим // Электросвязь. – 2009. – № 8. – С. 32–36.

9. **Sharawi M.** WSN's Energy-Aware Coverage Preserving Optimization Model based on Multi-Objective Bat Algorithm / M. Sharawi, E. Emary, I. A. Saroit, H. El-Mahdy // Evolutionary Computation (CEC), 2015 IEEE Congress on.

10. **Киричек Р. В.** Модельные сети для Интернета Вещей и программируемых сетей / Р. В. Киричек, А. Г. Владыко, М. В. Захаров, А. Е. Кучерявый // Информационные технологии и телекоммуникации. – 2015. – № 3 (11). – С. 17–26.

References

1. **Kucherjavyj A. E.** Letajushhie sensornye seti / A. E. Kucherjavyj, A. G. Vladyko, R. V. Kirichek, A. I. Paramonov, A. V. Prokop'ev, A. I. Bogdanov, A. A. Dort-Gol'c // Jelektrosvjaz'. – 2014. – № 9. – S. 2–5.

2. **Kirichek R. V.** The Investigation evolution in the wireless sensor networks area / A. E. Koucheryavy, R. V. Kirichek, A. I. Paramonov, A. V. Prokopiev // IT&Telecom. – 2014. – № 4. – PP. 29–41.

3. **Mochalov V. A.** Strategii razmeshhenija uzlov sensornoj seti / V. A. Mochalov, E. N. Turuta // VII Mezhdunarodnoj nauchno-tehnicheskoj kon-ferencii, 23–27 nojabrja 2010 g, Moskva.

4. **Dinh Ch. Z.** Review of methods of installation sensor nodes with quadrocopter / Ch. Z. Dinh, R. V. Kirichek, A. E. Koucheryavy // IT&Telecom. – 2015. – № 1 (9). – PP. 51–63.

5. **Abo-Zahhad M.** Coverage maximization in mobile Wireless Sensor Networks utilizing immune node deployment algorithm / Mohammed Abo-Zahhad, Sabah M. Ahmed and Nabil Sabor // Electrical and Computer Engineering (CCECE), 2014 IEEE 27th Canadian Conference on.

6. **Dinh Ch. Z.** Simulation models installation sensor with quadrocopters in a given area / Ch. Z. Dinh, R. V. Kirichek, A. I. Paramonov, A. E. Koucheryavy // IT&Telecom. – 2015. – № 2 (10). – PP. 93–100.

7. **Heinzelman W.R** Energy-Efficient Communication Protocol for Wireless Microsensor Networks / Wendi Rabiner Heinzelman, Anantha Chandrakasan, and Hari Balakrishnan // System Sciences, 2000. Proceedings of the 33rd Annual Hawaii International Conference on.

8. **Salim A.** Vybor golovnogo uzla klastera v odnorodnoj besprovodnoj sensornoj seti / A. E. Kucherjavyj, A. Salim // Jelektrosvjaz'. – 2009. – № 8. – S. 32–36.

9. **Sharawi M.** WSN's Energy-Aware Coverage Preserving Optimization Model based on Multi-Objective Bat Algorithm / M. Sharawi, E. Emary, I. A. Saroit, H. El-Mahdy // Evolutionary Computation (CEC), 2015 IEEE Congress on.

10. **Kirichek R. V.** Model networks for Internet of Things and SDN / R. V. Kirichek, A. G. Vladyko, M. V. Zaharov, A. E. Koucheryavy // IT&Telecom. – 2015. – № 3 (11). – PP. 17–26.

Динь Чон Зуи – студент магистратуры кафедры «Сети связи и передача данных» Федерального государственного бюджетного образовательного учреждения высшего образования «Санкт-Петербургский государственный университет телекоммуникаций им. проф. М. А. Бонч-Бруевича», duydthiph@gmail.com

Парамонов Александр Иванович – кандидат технических наук, доцент кафедры «Сети связи и передача данных» Федерального государственного бюджетного образовательного учреждения высшего образования «Санкт-Петербургский государственный университет телекоммуникаций им. проф. М. А. Бонч-Бруевича», alex-in-spb@yandex.ru

Киричек Руслан Валентинович – кандидат технических наук, доцент кафедры «Сети связи и передача данных» Федерального государственного бюджетного образовательного учреждения высшего образования «Санкт-Петербургский государственный университет телекоммуникаций им. проф. М. А. Бонч-Бруевича», kirichek@sut.ru

Кучерявый Андрей Евгеньевич – доктор технических наук, профессор, заведующий кафедрой «Сети связи и передача данных» Федерального государственного бюджетного образовательного учреждения высшего образования «Санкт-Петербургский государственный университет телекоммуникаций им. проф. М. А. Бонч-Бруевича», akouch@mail.ru

УДК 004.415.538

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

V. A. Kulik Bonch-Bruevich Saint-Petersburg State University of Telecommunication

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

R. V. Kirichek Bonch-Bruevich Saint-Petersburg State University of Telecommunication

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

A. E. Koucheryavy Bonch-Bruevich Saint-Petersburg State University of Telecommunication

ПРОГРАММНО-АППАРАТНЫЙ КОМПЛЕКС ДЛЯ ТЕСТИРОВАНИЯ УСТРОЙСТВ ИНТЕРНЕТА ВЕЩЕЙ

HARDWARE-SOFTWARE COMPLEX FOR TESTING INTERNET OF THINGS DEVICES

В данной статье будут рассмотрены модели тестирования устройств Интернета Вещей, в частности тестирование сетевой безопасности, нагрузочное тестирование и удаленное тестирование. Каждая из моделей рассматривается в контексте ее реализации в программно-аппаратном комплексе.

This paper will address Internet devices testing models of Things, in particular network security testing, stress testing and remote testing. Each of the models discussed in the context of its implementation in the software and hardware complex.

Интернет Вещей, интернет вещь, тестирование, сетевая безопасность, нагрузочное тестирование, облако, анализ трафика.

Internet of Things, thing, testing, network security, load testing, cloud, traffic analysis.

Введение

В последнее время, в связи с значительным удешевлением производства микропроцессорной техники и интенсивным развитием технологий передачи данных для сетей связи общего пользования, все более актуальной становится тема Интернета Вещей [1, 2]. Количество устройств, подключенных к сети Интернет, в настоящее время превышает количество людей пользующихся глобальной сетью связи Интернет и, согласно оценке главного футуролога компании *Cisco* Дэйва Эванса, к 2020 году достигнет

отметки 50 миллиардов устройств, подключенных к сети Интернет [3]. Такое огромное число устройств, подключенных к сети Интернет, ставит перед исследователями совершенно новые задачи, связанные с рядом серьезных проблем, возникающих в сетях связи общего пользования при их взаимодействии с устройствами Интернета Вещей. В частности, на текущий момент, не существует единого подхода к тестированию устройств Интернета Вещей, которые существуют для узлов сети связи следующего поколения [4].

В данной статье будет рассмотрен ряд методов по тестированию Интернет Вещей, в частности методы тестирования сетевой безопасности, нагрузочного тестирования и удаленного тестирования. Данные методы, в дальнейшем, предлагается использовать для разработки программно-аппаратного обеспечения для тестирования устройств Интернета Вещей.

1 Тестирование сетевой безопасности

Отсутствие общих стандартов сетевой безопасности для Интернет Вещей, в совокупности с их ограниченной вычислительной мощностью, выявляют новые угрозы безопасности для устройств Интернета Вещей. Данные угрозы создают потребность в тестировании Интернет Вещей на наличие уязвимостей сетевой безопасности.

Одной из распространенных уязвимостей Интернет Вещей является перехват конфиденциальных данных, идущих от Интернет Вещи к удаленному облачному серверу. В случае, если для данных отсутствует криптографическая защита злоумышленник получает полный доступ к данным, отправляемых устройством [5].

В связи с этим предлагается проводить тестирование Интернет Вещей на уязвимость сетевой безопасности методом перехвата и анализа сетевого трафика. Метод заключается в подключении к каналу связи, по которому идет трафик Интернета Вещей, устройства перехвата и анализа трафика, которое захватывает и обнаруживает, по характерным свойствам, трафик ИВ [5]. В случае если не используются алгоритмы шифрования возможно провести анализ информации, находящейся в поле данных перехваченных пакетов. Если в процессе выявления Интернет Вещи удалось определить, используемый ИВ протокол обмена, выполняется выделение ключевых полей в пакете. Например, в протоколе *MQTT* присутствует поле *topic*, в котором находится информация о брокере на который подписано устройство, т. е. фактически – это адрес приложения, которое отвечает за взаимодействие ИВ и *MQTT*-сервера. В случае, если протокол взаимодействия не определен, устройство тестирования определяет изменяемые биты в поле данных пакета, путем анализа множества пакетов, полученных от ИВ. После этого устройство на основе полученных данных определяет тип устройства Интернета Вещей.

Таким образом, после определения формата сообщения, возможна фальсификация данных, получаемых сервером от ИВ типа «сенсор» [6], путем отправки «ложного» пакета, дублирующего перехваченные от ИВ пакеты, но с необходимым изменением поля данных, на удаленный облачный сервер, связанный с атакуемой ИВ. Точно таким же образом возможно воздействие на интернет вещь типа «актуатор» [6] путем анализа данных и отправки «ложного» пакета на ИВ.

В случае успешного проведения тестирования ИВ считается уязвимой для атаки, при условии возможности доступа злоумышленника к каналу связи, по которому ИВ передает данные удаленному облачному серверу.

2 Нагрузочное тестирование

Помимо проблемы обеспечения сетевой безопасности, не менее важной задачей является задача проведения нагрузочного тестирования узлов сети связи, в первую очередь маршрутизаторов и коммутаторов, на предмет устойчивости к трафику Интернета Вещей. Необходимость создание методики для такого тестирования связано с тем, что трафик Интернет Вещей отличается от классического трафика конвергентных сетей связи, в связи с чем возникает вопрос устойчивости существующего оборудования сетей связи к трафику подобного типа.

В первую очередь, для генерации трафика Интернет Вещей необходимо определить его свойства. Трафик Интернет Вещей характеризуется:

- малым размером пакетов. Поле данных в большинстве случаев имеет меньший размер чем заголовок пакета;
- большое количество пакетов, в связи с большим числом Интернет Вещей, подключенных к сети;
- иными законами временного распределения. Помимо свойств самоподобия, которое наблюдалось в сетях связи следующего поколения, Интеренет Вещи могут создавать антиперсистентный трафик [7, 8].

Таким образом, при создании потока данных Интернет Вещей, для тестирования узлов связи следует учитывать все вышеперечисленные свойства.

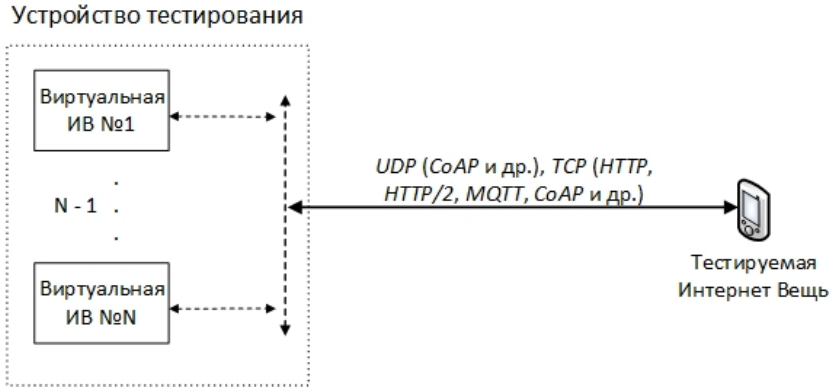


Рис. 1. Модель нагрузочного тестирования Интернет Вещей

Для реализации устройства нагрузочного тестирования предлагается модель (рис. 1), обладающая следующими функциями:

1) Возможность параллельной генерации трафика от виртуальных Интернет Вещей. Т. е. возможность создания на устройстве тестирования множества виртуальных Интернет Вещей, имеющих уникальные параметры (уникальный *MAC, IP*, идентификационный номер и т. д.);

2) Каждая виртуальная интернет вещь, работающая на устройстве, при этом должна иметь один их основных типов устройств ИВ [6], например:

- сенсор (устройство, преобразующее и отправляющее данные, получаемые от датчиков. Датчик – это электронное устройство, которое измеряет физическое состояние или химический состав и доставляет электронный сигнал, соответствующий наблюдаемой характеристике [9]);
- актуатор (устройство, которое инициирует физическое действие после возбуждения входным сигналом [9]);
- мультимедиа устройство (устройство отправляющее мультимедийную информацию. Мультимедийная информация – это цифровая информация, в которой для информирования или развлечения пользователей используется много видов информационного контента и обработки информации, например, текст, изображения, аудио, видео, трехмерные панорамные изображения и цифровые карты [9]);

3) Поддержка основных сценариев работы ИВ. Каждая интернет вещь обладает уникальным алгоритмом работы, заложенным в нее разработчиком, но существуют следующие основные типы сценариев работы ИВ:

- Постоянная отправка данных. Каждое устройство периодично отправляет данные на удаленный облачный сервер. В данном случае, устройство может иметь 2 типа данных – сенсор, мультимедиа устройство. Генерирует самоподобный трафик. Для данного сценария чаще всего используются протоколы транспортного уровня без установления соединения (например, *UDP*), реже используются протоколы, поддерживающие установление соединение (например, *TCP*).
- Отправка данных по запросу. В данном случае, устройство может иметь 2 типа данных – сенсор, мультимедиа устройство. Может генерировать, как самоподобный трафик, так и антиперсистентный, в зависимости от алгоритма, прописанного на удаленном управляющем сервере. Для данного сценария чаще всего используются протоколы транспортного уровня с установлением соединения (например, *TCP*), в некоторых случаях, например, в случаях, когда и ИВ, и облачный сервер имеют адрес в глобальной сети, возможно использование протоколов без установления соединения (например, *UDP*).

− Воздействие на окружающий мир устройством, по управляющему сигналу. В данном случае, устройство может иметь тип актуатор. Может генерировать, как самоподобный трафик, так и антиперсистентный, в зависимости от алгоритма, прописанного на удаленном управляющем сервере. Для данного сценария чаще всего используются протоколы транспортного уровня с установлением соединения (например, *TCP*), в некоторых случаях, возможно использование протоколов без установления соединения (например, *UDP*).

4) Возможность генерации различных типов трафика от каждой Интернет Вещи по определенному закону распределения [7, 8].

5) Связь с удаленным тестовым сервером, необходимым для тестирования сценариев, в которых необходимо использование протоколов транспортного уровня с поддержкой соединения. Также данный сервер, необходим для измерения уровня задержки при высоких уровнях нагрузки оборудования трафиком Интернета Вещей.

Также помимо поддержки возможностей вышеуказанной модели нагрузочного тестирования, устройство должно поддерживать все основные типы физических интерфейсов передачи данных. Т. е. устройство должно поддерживать: интерфейс *PON*, интерфейс *Ethernet*, интерфейс *IEEE 802.11*.

3 Удаленное тестирование

Еще одной проблемой при организации тестирования Интернет Вещей является удаленное тестирование Интернет Вещей. Удаленное тестирование ИВ необходимо в случае необходимости тестирования уже подключенных и функционирующих в глобальной сети ИВ. При этом удаленное тестирование подразумевает полную автоматизацию процесса, что позволит обеспечить низкую стоимость процесса тестирования для конечного пользователя – обладателя тестируемой ИВ.

Для реализации программно-аппаратного комплекса удаленного тестирования Интернет Вещей предлагается модель (рис. 2) состоящая из:

1) Удаленного сервера тестирования (*Cloud testing server*). Сервер отвечающий за контроль процесса тестирования, путем отправки управляющих команд устройству тестирования, собирающего статистику, полученную в ходе тестирования и проводящего анализ полученных данных.

2) Маршрутизатор (*Switch*). Отвечает за соединения локального сегмента на стороне пользователя, включающего устройство тестирования и само тестируемое устройство Интернет Вещей с сетью связи общего пользования.

3) Устройство тестирования (*Testing device*). Устройство, находящейся в одной локальной сети с тестируемой интернет вещью и имеющее доступ к среде передачи данных Интернет вещи.

4) Удаленный облачный сервер (*Cloud server*). Сервер, с которым происходит взаимодействие устройства Интернет Вещей.

5) Тестируемое устройство Интернет Вещей (*Internet of Thing device under testing*). Тестируемое устройство, находящейся в одной локальной сети с тестирующим устройством и взаимодействующее с удаленным облачным сервером по определенному протоколу взаимодействия.

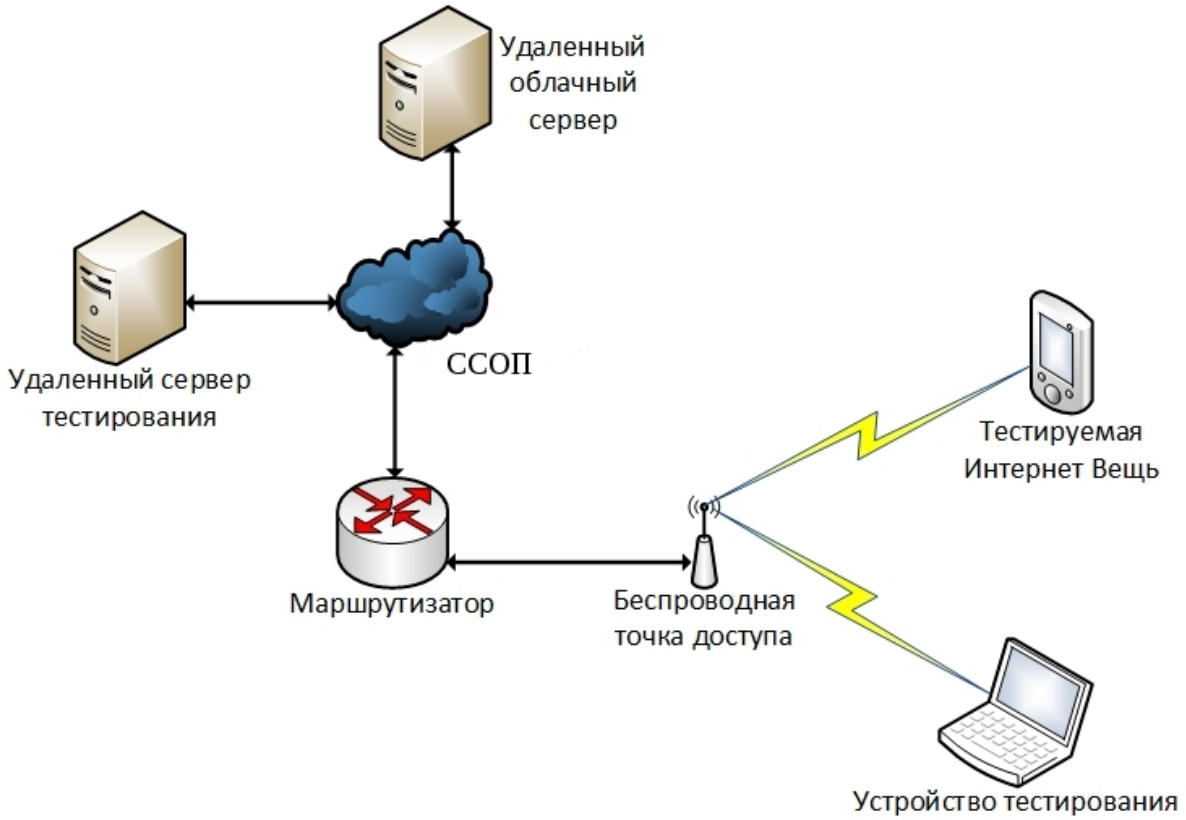


Рис. 2. Пример модели удаленного тестирования с доступом к беспроводному каналу связи

Такой программно-аппаратный комплекс возможно организовать на основе модельной сети лаборатории Интернета Вещей СПбГУТ им. М. А. Бонч-Бруевича [11].

Тестирование Интернет Вещи, на основе вышеприведенной модели рекомендуется проводить по следующему алгоритму (рис. 3):

1) Тестируемая интернет вещь и устройство тестирования подключаются к одной локальной сети.

2) На устройство тестирования устанавливается программное обеспечение, отвечающее за взаимодействие с удаленным сервером тестирования. Данное приложение активируется в режиме фоновой работы.

3) Предоставление устройству тестирования доступа к каналу связи, по которому передаются данные от Интернет Вещи, либо с использованием интерфейса беспроводной связи, либо с использованием мониторингого

ответвителя, для дублирования, идущего по проводному каналу связи трафика.

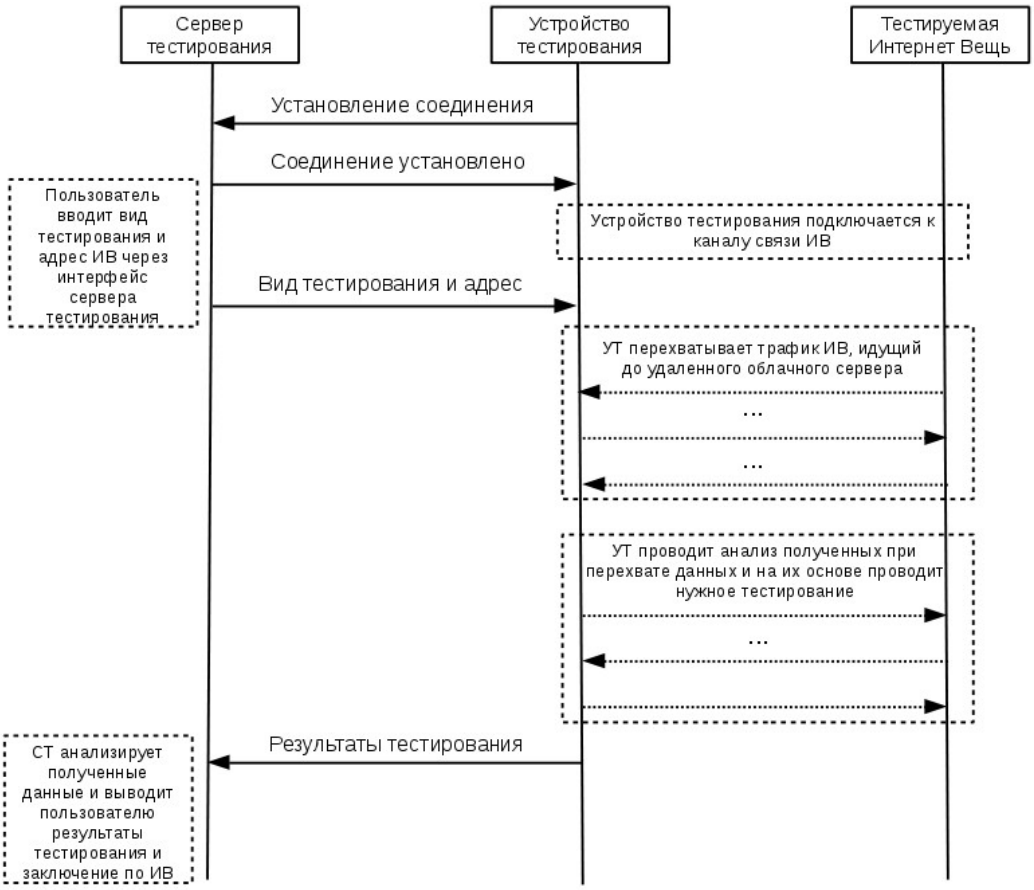


Рис. 3. Модель взаимодействия устройств, при проведении удаленного тестирования

4) Пользователь, через интерфейс взаимодействия с удаленным сервером тестирования, выбирает вид тестирования Интернет Вещи.

5) Далее облачный сервер отправляет управляющие сигналы на устройство тестирования в локальной сети. Устройство тестирование переключается в режим ожидания.

6) Тестируемая интернет вещь активируется и начинает взаимодействие с удаленным облачным сервером, по заранее прописанному в ИВ сценарию.

7) Устройство тестирования перехватывает трафик, идущий от Интернет Вещи, и производит его анализ, с помощью заранее указанного пользователем IP-адресом Интернет Вещи.

8) Устройство тестирования, по определенным критериям (например, коэффициент Хёрста, протокол взаимодействия транспортного уровня, порт взаимодействия и др.) определяет тип Интернет Вещи и протокол ее взаимодействия. Если же используется нестандартный протокол взаимодействия, то проводится поиск неизменяемой части и граничных значений

для изменяемой частей пакета, с помощью сравнения множества сходных пакетов, полученных от Интернет Вещи, для поля данных пакета, при условии того что данные незашифрованны, или данные поддаются расшифровке (в случае предварительного перехвата ключа шифрования для симметричного шифрования).

9) Далее проводится одно из возможных видов тестирования [5, 10], в зависимости от того какой вид был выбран пользователем в интерфейсе взаимодействия с удаленным сервером.

10) Устройство тестирование отправляет данные о результатах тестирования на удаленный сервер тестирования.

11) Сервер тестирования, на основе анализа полученных данных, выдает пользователю заключение о Интернет Вещи, по выбранному виду тестирования.

Заключение

В данной статье были рассмотрены три модели тестирования Интернет Вещей. Каждая из них решает определенный круг задач по исследованию корректности работы устройств Интернета Вещей. На основе рассмотренных методов предлагается разработать программно-аппаратный комплекс для комплексного тестирования Интернет Вещей, как удаленно из глобальной сети, так и из локального сегмента. Методы нагрузочного тестирования и тестирования сетевой безопасности могут быть реализованы в программно-аппаратной реализации предложенной модели удаленного тестирования.

Библиографический список

1. **Кучерявый А. Е.** Интернет Вещей / А. Е. Кучерявый // Электросвязь. – 2013. – № 1. – С. 21–24.

2. **Кучерявый А. Е.** Самоорганизующиеся сети / А. Е. Кучерявый, А. В. Прокопьев, Е. А. Кучерявый. – СПб. : Любавич, 2011. – 311 с.

3. **Evans Dave** The Internet of Things How the Next Evolution of the Internet Is Changing Everything / Dave Evans // CISCO White Papers // April 2011.

4. **Васильев А. Б.** Тестирование сетей связи следующего поколения / А. Б. Васильев, Д. В. Тарасов, Д. В. Андреев, А. Е. Кучерявый. – М. : ФГУП ЦНИИС, 2008. – 144 с.

5. **Киричек Р. В.** Ложные облака для интернета вещей. Методы защиты / Р. В. Киричек, В. А. Кулик, А. Г. Владыко, И. А. Богданов, А. Е. Кучерявый // Информационные технологии и телекоммуникации. – 2015. – № 3 (11). – С. 27–39.

6. **Peter Waher** / Learning Internet of Things. – Birmingham, UK, Packt Publishing Ltd. // Jan 2015.

7. **Vybornova Anastasia** Traffic Analysis in Target Tracking Ubiquitous Sensor Networks / Anastasia Vybornova, Andrey Koucheryavy // 14th International Conference, NEW2AN 2014 and 7th Conference, ruSMART 2014 vol. 8638 // Springer International Publishing // August 27–29, 2014.

8. **Парамонов А. И.** Разработка и исследование комплекса моделей трафика для сетей связи общего пользования : автореферат дис. … канд. техн. наук, Санкт-Петербург: СПбГУТ, 2014.

9. **Y.2069.** Terms and definitions for the Internet of things // Recommendation ITU-T // Jul 2012.

10. **Киричек Р. В.** Методы исследования беспроводных каналов связи Интернета Вещей в условиях совместной работы / В. А. Кулик, Р. В. Киричек, А. Н. Бондарев // Информационные технологии и телекоммуникации. – 2015. – № 2 (10). – С. 106–114.

11. **Kirichek R.** Internet of Things Laboratory Test Bed / R. Kirichek, A. Koucheryavy // International Conference on Wireless Communication, Networking and Application. WCNA 2014. – LNEE. – Vol. 348. – Heidelberg: Springer, 2016.

References

1. **Kucherjavyj A. E.** Internet Veshhej / A. E. Kucherjavyj // Jelektrosvjaz'. – 2013. – № 1. – S. 21–24.

2. **Kucherjavyj A. E.** Samoorganizujushhiesja seti / A. E. Kucherjavyj, A. V. Prokop'ev, E. A. Kucherjavyj. – SPb. : Ljubavich, 2011. – 311 s.

3. **Evans Dave** The Internet of Things How the Next Evolution of the Internet Is Changing Everything / Dave Evans // CISCO White Papers // April 2011.

4. **Vasil'ev A. B.** Testirovanie setej svjazi sledujushhego pokolenija / A. B. Vasil'ev, D. V. Tarasov, D. V. Andreev, A. E. Kucherjavyj. – M. : FGUP CNIIS, 2008. – 144 s.

5. **Kirichek R. V.** False clouds for Internet of Things. Methods of protection / R. V. Kirichek, V. A. Kulik, A. G. Vladyko, I. A. Bogdanov, A. E. Koucheryavy // IT&Telecom. – 2015. – № 3 (11). – PP. 27–39.

6. **Peter Waher** / Learning Internet of Things. – Birmingham, UK, Packt Publishing Ltd. // Jan 2015.

7. **Vybornova Anastasia** Traffic Analysis in Target Tracking Ubiquitous Sensor Networks / Anastasia Vybornova, Andrey Koucheryavy // 14th International Conference, NEW2AN 2014 and 7th Conference, ruSMART 2014 vol. 8638// Springer International Publishing // August 27–29, 2014.

8. **Paramonov A. I.** Razrabotka i issledovanie kompleksa modelej trafika dlja setej svjazi obshhego pol'zovanija : avtoreferat dis. … kand. tehn. nauk, Sankt-Peterburg: SPbGUT, 2014.

9. **Y.2069.** Terms and definitions for the Internet of things // Recommendation ITU-T // Jul 2012.

10. **Kirichek R. V.** Software development for servers wirelesssensor networks / R. V. Kirichek, V. A. Kulik, A. N. Bondarev // IT&Telecom. – 2015. – № 2 (10). – PP. 106–114.

11. **Kirichek R.** Internet of Things Laboratory Test Bed / R. Kirichek, A. Koucheryavy // International Conference on Wireless Communication, Networking and Application. WCNA 2014. – LNEE. – Vol. 348. – Heidelberg: Springer, 2016.

Кулик Вячеслав Андреевич – магистр, инженер кафедры «Сети связи и передача данных» Федерального государственного бюджетного образовательного учреждения высшего образования «Санкт-Петербургский государственный университет телекоммуникаций им. проф. М. А. Бонч-Бруевича», vslav.kulik @gmail.com

Киричек Руслан Валентинович – кандидат технических наук, доцент кафедры «Сети связи и передача данных» Федерального государственного бюджетного образовательного учреждения высшего образования «Санкт-Петербургский государственный университет телекоммуникаций им. проф. М. А. Бонч-Бруевича», kirichek@sut.ru

Кучерявый Андрей Евгеньевич – доктор технических наук, профессор, заведующий кафедрой «Сети связи и передача данных» Федерального государственного бюджетного образовательного учреждения высшего образования «Санкт-Петербургский государственный университет телекоммуникаций им. проф. М. А. Бонч-Бруевича», akouch@mail.ru

УДК 004.7

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

R. V. Kirichek Bonch-Bruevich Saint-Petersburg State University of Telecommunications

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

D. K. Nguen Bonch-Bruevich Saint-Petersburg State University of Telecommunications

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

E. M. Gerasimova Bonch-Bruevich Saint-Petersburg State University of Telecommunications

СРАВНИТЕЛЬНЫЙ ОБЗОР ТЕХНОЛОГИИ LI-FI И ПЕРСПЕКТИВА ПРАКТИЧЕСКОГО ИСПОЛЬЗОВАНИЯ ДЛЯ ИНТЕРНЕТА ВЕЩЕЙ

COMPARATIVE REVIEW OF TECHNOLOGIES LI-FI AND OUTLOOK FOR THE PRACTICAL USE OF THE INTERNET OF THINGS

В настоящее время *Li-Fi* технология является новым и актуальным направлением исследований в области инфокоммуникаций. В конце 2015, в одной лаборатории в Эстонии, проведено испытание, в котором смог получить очень высокую скорость передачи 224 Гбит/с в лабораторных условиях, а во время тестов в офисах – до 1 Гбит/с. Тем не менее, из-за некоторых ограничений, что существующая технология может быть применена только в определенных специализированных областях. В этой статье представлены особенности этой технологии, сравнение с известной технологией Wi-Fi и перспективы применения *Li-Fi* для сети IoT.

At present, Li-Fi technology is a new and urgent direction in infocommunications research. At the end of 2015 in a laboratory in Estonia, carried out the test, which was able to get a very high transmission rate of 224 Gb/s in the lab and during tests in the office – up to 1 Gbit/s. However, due to certain limitations that the present technology can be applied only at certain specific areas. This paper presents the features of this technology, compared to known Wi-Fi technology and perspectives of Li-Fi network for the IoT.

Li-Fi технология, Интернет Вещей, светодиодная лампа, технология VLC.

Li-Fi technology, the Internet of Things, LED lamp, the VLC technology.

1 Введение

Одним из основоположников технологии *Li-Fi* является профессор Харальд Хаас из Эдинбургского университета. Именно он инициировал создание проекта *D-Light* и коммерческого проекта *PureVLC* [11]. Он занимается разработкой технологии *Li-Fi* уже более десяти лет и является автором название технологии *VLC* (*Visible Light Communication* – связь по видимому свету) на светодиодах – технология *Li-Fi* (аббревиатура в названии составлена из английских слов "light" (свет) и "fidelity" (точность)). В июне 2011 года доктор Харальд Хаас продемонстрировал, что светодиодная лампа, оснащенная модулятором для кодирования сигнала, может передавать на компьютер видеоизображение высокой четкости (*HD*, аббревиатура от английских слов *high-definition*) [6].

Технология *Li-Fi* способна обеспечить надежный и дешевый способ подключения к Интернету практически из любого места с помощью специальных светодиодов.

При финансировании британским Советом по исследованиям в области инженерных и физических наук (*Engineering and Physical Sciences Research Council*), университетами Эдинбурга, Оксфорда и Кэмбриджа был инициирован проект изучения передачи данных с помощью ультрапараллельного видимого света (*Ultra-parallel visible light communications project*). Микросветодиоды могут, создавать параллельные потоки света и таким образом, в разы, увеличивать количество данных, которое может быть передано за единицу времени. "Представьте себе головку душа, которая направляет воду строго параллельными струями, – а мы таким же образом заставили вести себя свет", – объясняет профессор Харальд Хаас [6].

Согласно стандарту *IEEE* 802.15.7, вышедшему в декабре 2012 года для *VLC*-технологий, пропускная способность технологии *Li-Fi* предписана в пределах 96 Мбит/с [9]. С помощью микросветодиодной лампы, можно достигать скорости передачи данных 3,5 Гб/с через каждый из трех цветов – красный, зеленый и синий, – которые вместе составляют белый свет [8]. Это значит, что, сложив спектральные каналы, можно передавать данные с общей скоростью 10 Гб/с. Сброс сигнала у использующихся светодиодов и фотодиодов происходит достаточно быстро для того, чтобы не выдерживать паузу для его надёжного затухания.

Видимое излуче́ние является той частью электромагнитного спектра, которая расположена в диапазоне между 385 ТГц и 790 ТГц. Эта часть электромагнитного спектра, в 10 тысяч раз более широкая, чем спектр радиоизлучения. Поэтому потенциально свет может обеспечить практически неограниченную широту канала передачи данных, и имеет более широких возможностях технологий *VLC*. Для того, чтобы передать обратно данные на базе технологии *Li-Fi* сеть требует комбинированного использования с другими технологиями передачи данных, такими как *PLC* (*Power Line Communication*), в которой данные передаваемые по силовым проводам или высокоскоростная

инфракрасная передача данных данных (*VFIR* или *UFIR – Very Fast Infrared* и *Ultra Fast Infrared*) [10].

На рис. 1 показано локальная сеть передачи данных на базе комбинации технологии *Li-Fi* и технологии *VFIR* для обратной связи, в которой *Li-Fi*-трансмиттер представлен в себе фотодиодный инфракрасный излучатель, приёмник, декодер, а также *USB*-интерфейс.

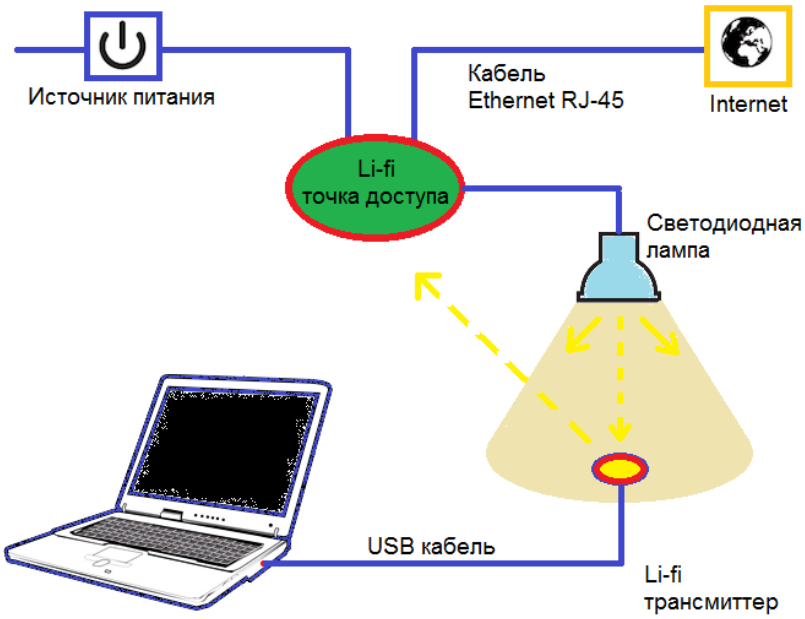


Рис. 1. Схематичное представление локальной сети *Li-Fi*

В технологии *Li-Fi* используется свет от светодиодов в качестве среды для доставления доступа к сети, мобильной и высокоскоростной передачи. Данные передаются посредством модуляции интенсивности света с наносекундными интервалами, которые слишком быстры, чтобы не удалось обнаружить человеческим глазом. Эти данные затем принимается светочувствительным детектором. После этого световой сигнал демодулируется в электронном виде.

2 *Li-Fi* и сравнение с известной технологией Wi-fi

Самая большая разница между *Li-Fi* и *Wi-fi*, это при передаче данных *Li-Fi* использует видимый свет, как канал связи (в отличие от радиоволн в *Wi-Fi*). Из этого, по сравнению с *Wi-fi*, технология *Li-Fi* имеет несколько преимуществ и недостатков.

2.1 Преимущества

В первый очередь, в настоящее время *Li-Fi* позволяет передать данные в сети с скоростью до 1 Гбит/с, значит в 100 раз быстрее, чем скорость пере-

дачи в *Wi-Fi*. Даже, в лабораторных условиях, можно получить высокую скорость передачи – 224 Гбит/с, значит можно скачать 20 фильмов в качестве *HD* только в секунду. По мнению Хааса, *Li-Fi* может достичь скорости передачи данных в более 100 раз, чем *Wi-Fi*, потому что *Li-Fi* содержится в небольшом районе, а в то время радиосигналы распространяются.

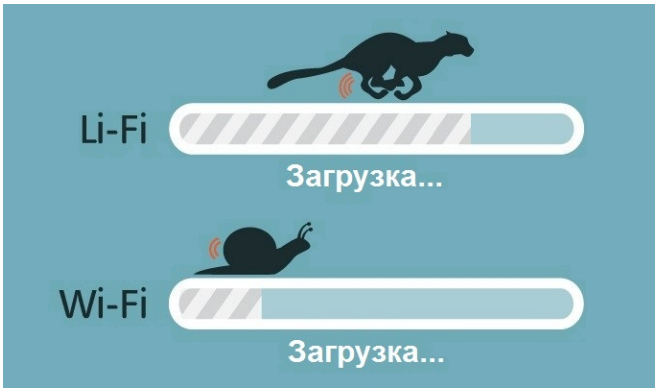


Рис. 2. Разница между скоростями передачи данных в *Li-Fi* и Wi-fi

В сетях *Wi-Fi* для передачи данных необходимо расширить допустимую полосу частот, которая ограничена и платна, а в сетях *Li-Fi*, дополнительная полоса выделится бесплатно и не требует процедуры лицензирования, что позволит упрощать использование технологии *Li-Fi*.

Вместе с этим, радиочастотные технологии *RFID* для передачи данных могут вызвать негативные последствия на организм человека, и, несмотря на последствия *Li-Fi* сети не известно, есть исследования, показывающие, что свет *LED* является наиболее удобным для человеческого глаза [2].

Видимый свет не проходит сквозь стены, поэтому технология *VLC* потенциально более надежна, чем традиционный *Wi-fi*, с точки зрения сохранения конфиденциальности передачи данных. В отличие от радиочастотных технологий, радиус сети с использованием технологии *Li-Fi* позволяет полностью покрыть сигналом закрытое целевое помещение (например: комната, кабинет, зал, офис...) и не будет выходить за его пределы [3, 8]. Это значит, что возможно более обеспечение высокого уровня конфиденциальности данных, более простой способ, чтобы защитить их от несанкционированного доступа. В зоне 10 кв. метров, по технологии *Li-Fi* исследователи института телекоммуникаций Фраунгофера уже передали данные со скоростью 800 Мбит/сек [12]. Это позволяет технологию *Li-Fi* стать отличным решением для создания и использвания беспроводной сети в домашних условиях.

Кроме этого, низкая цена микросветодиодной лампы, в сочетании с возможностями энергосбережения позволяют построение сети *Li-Fi* стать более дешевым и энергоэффективным.

По словам профессора Хааса, еще одно преимущество новой технологии заключается в том, что для равномерного распределения светодиодного передатчика возможно получить подключение к интернету гораздо более точ-

ную и стабильную внутри здания [6]. Недостатком традиционного маршрутизатора *Wi-Fi* всегда существовал, что с увеличением расстояния от передатчика сигнал ослабевается, а также в домах и офисах с областью, где связь настолько слаба, что подсоединение к интернету становится нестабильным или вовсе прерывается.

2.2. Недостатки

Несмотря на то, что существуют многие преимущества, в настоящее время *Li-Fi* технология является еще новой технологией, которая находится в начале исследования. Поэтому, эта технология также имеет некоторые недостатки, позволяющие препятствовать применению *Li-Fi* на практике.

В первый очередь, это изменение в инфраструктуре. Известные технологии беспроводной передачи данных сегодня как *Wi-Fi, Bluetooth, LTE* широко применяются на основе солидной инфраструктуры, и хорошо работают, удовлетворяют большинство потребностей пользователей. Для того, чтобы *Li-Fi* становилась популярным, требует изменение от производителя вспомогательного оборудования, единство в строительстве соответствующей инфраструктуры. Этот процесс требует много времени и денег.

Как показано выше, в технологии *Li-Fi* используется свет для передачи данных. А свет передается только прямо и не может пройти через препятствия, что говорит о более высокой уязвимости к перебоям [7]. Это значит в домашних условиях, такие предметы, как шторы, растения или сами пользователь... могут стать препятствиями к процессам передачи информации между использователем и сетью Интернета.

Кроме этого, при условии существования солнечного света, или там, где есть смешанные среды для свет, как в тумане, невозможно использовать технологию *Li-Fi*. В таких средах, помеха формируется, препятствует светопропускание, свет ослабевается, что ведет к ощибки и потере информации при передачи.

ТАБЛИЦА. Преимущества и недостатки технологии *Li-Fi*

Преимущества:	**Недостатки:**
− высокая скорость передачи данных; − высокий уровень безопасности; − малое потребление энергии и дешево; − не влияет на организм человека, комфортно для человеческих глаз.	− уязвимость к перебоям; − невозможно использовать в темноте, в смешанных средах; − изменение в инфраструктуре.

В частности, самый большой недостаток технологии *Li-Fi*, это проблема при использовании в темноте. Во многих случаях пользователи, которые хотят подключиться к Интернету в темноте, например перед сном [13]. Тогда использование света для передачи информации вызывает ощущение дискомфорта для пользователей.

Чтобы стать неотъемлемой частью жизни, технология *Li-Fi* необходимо преодолеть существующие барьеры. Тем не менее, ученые говорят, что в будущее *Li-Fi* не может полностью заменить традиционные технологии, только сосуществовать и использоваться в специализированных областях.

3 Перспектива практического использования *Li-Fi* для *IoT*

В настоящее время, технология беспроводной оптической передачи данных *Li-Fi* изучается для использования в узкоспециализированных областях, развертывания в медицинских учреждениях и предприятиях, в космических шаттлах и станциях, на борту самолётов [9], на которых производственные процессы связаны с радиопередачами. Однако, ученые прогнозируют, что появление Интернета Вешей может привести к явлению “хруст спектр” (*spectrum crunch*), в котором радиочастотные сети передачи данных перегружаются. С помощью использования технологии *Li-Fi*, можно отказаться от этой проблемы, и передать сигнал на неограниченное количество устройств в зоне видимости, как показано на рис. 3.

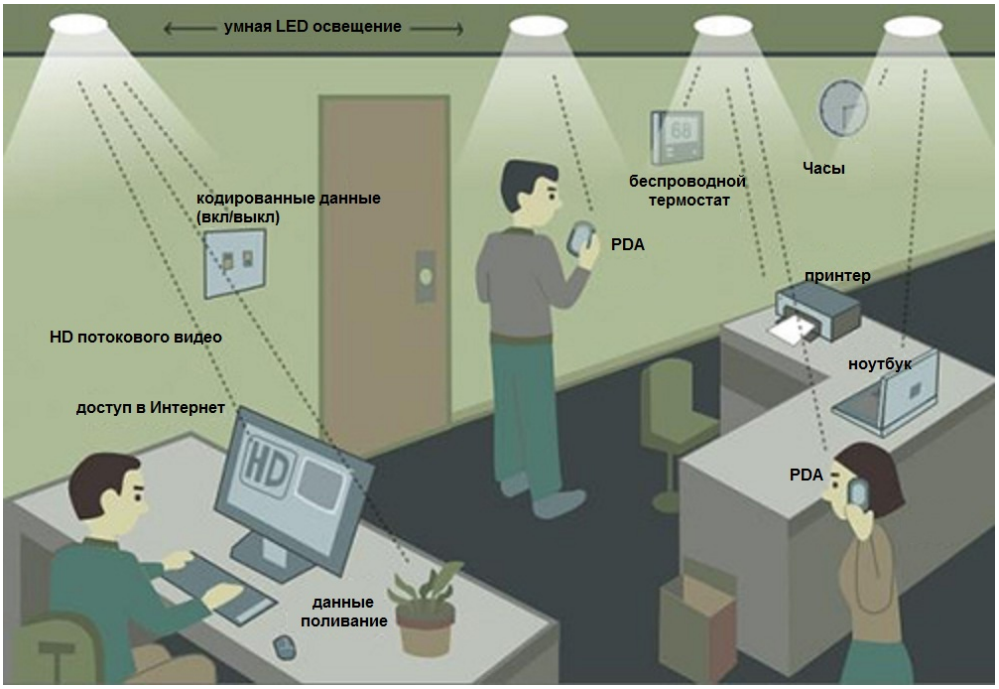


Рис. 3. Практическое использование технологии *Li-Fi*

Известно, что Интернет вещей, это понятие, используемое для описания сети, в которой все физические объекты, оснащённых встроенными технологиями для взаимодействия друг с другом или с внешней средой, могут подключаться к Интернету [1, 5]. Такие средства, как средства идентификации, средства измерения, средства передачи данных, и средства обработки данных. Средства измерения играют особую роль, отвечают за взаимодействия с внешней средой, и обеспечивают преобразование о внешней среде в понятный вид данных для машины, и тем самым напол-

няющие вычислительную среду значимой информацией. Сеть, состоящая из этих средств и самая популярная на сегодняшний день – это беспроводная сенсорная сеть, работающая на базе технологий *Zigbee, 6LoWPAN, IEEE 802.15.4, BLE…* С своими преимуществами, технология *Li-Fi* в полной мере может конкурировать с упомянутой выше технологии, технология, и широко использоваться в Интернете Вещей. Большинство современных устройств оснащены по меньшей мере 1 LED. Поэтому, чтобы эти устройства смогли подключаться к сети, мы просто добавляем дополнительный набор *Li-Fi*-трансмиттер. Это можно рассматривать как большое преимущество в применении *Li-Fi* для *IoT*.

Еще одно практическое применение *Li-Fi* в жизни это для сети *VANET (Vehicular ad hoc network)*, в которой машины могут общаться друг с другом с помощью автомобильных фар; а фонарики как станции управления – *RSU* (*Road Side Unit*). Это показано на рис. 4.

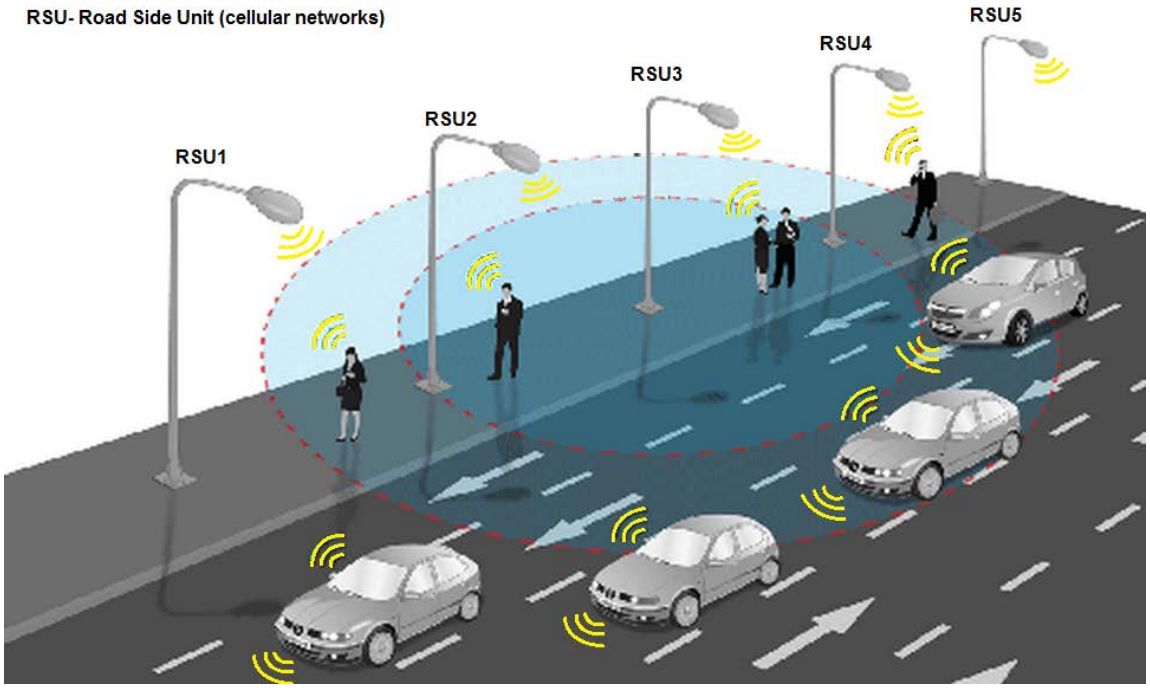


Рис. 4. Применение технологии *Li-Fi* для *VANET*

4 Подход совместного использования технологии *Li-Fi* вместе с традиционными технологиями *Wi-Fi, LTE, Bluetooth, Zigbee, …*

В цели преодоления недостаток технологии *Li-Fi*, мы предлагаем решения с комбинированным использованием технологии *Li-Fi* вместе с традиционными технологиями беспроводной передачи данных. Для этого мы используем специальный трансмиттер, который состоит из нескоторых частьей. Первая часть, это обычный *Li-Fi*-трансмиттер, представлен в себе фотодиодный инфракрасный излучатель, приёмник и декодер. Вторая часть состоит из сборщика энергии и батарея. Последнная часть, это мо-

дуль *Zigbee/Wi-fi/BLE*… В нормальных условиях, устройства работают в режиме передачи с использованием технологии *Li-Fi*, одновременно сборщик энергии заряжает батарей. В неблагоприятных условиях, батарей будет предоставляет энергию модули *Zigbee/Wi-fi/BLE,* тогда устройство работает по базе традиционной технологии. Принцип этого подхода, показанный на рис. 5.

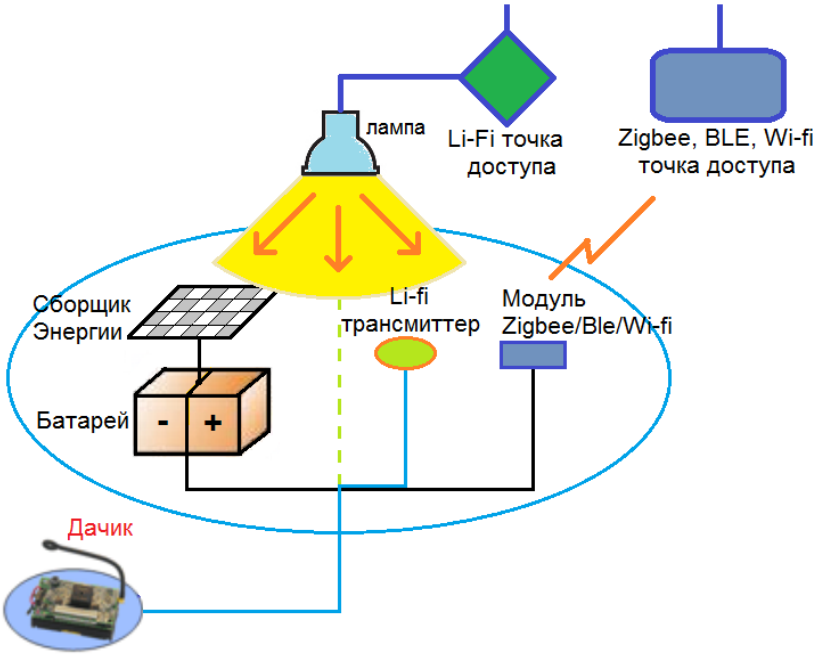


Рис. 5. Подходы совместного использования технологии *Li-Fi* вместе с традиционными технологиями

5 Заключение

Сегодня наука и технология быстро меняются, чтобы удовлетворить требования человека в жизни. Появление технологии *Li-Fi* позволяет людям решить проблему ограниченного спектра радиочастот традиционных технологий, и предоставляет возможность передачи данных с очень высокой скоростью. Несмотря на некоторые ограничения, технология *Li-Fi* все еще находится в стадии исследования и разработки. В следующее время, наряду с развитием IoT, *Li-Fi* будет достигать определенный успех.

Библиографический список

1. **Киричек Р. В.** Эволюция исследований в области беспроводных сенсорных сетей / А. Е. Кучерявый, Р. В. Киричек, А. И. Парамонов, А. В. Прокопьев // Информационные технологии и телекоммуникации. – 2014. – № 4. – С. 29–41.

2. **Никифоров С. Г.** Теперь электроны можно увидеть: светодиоды делают электрический ток очень заметным / С. Г. Никифоров // Компоненты и технологии. – 2006. – № 3. – С. 20–27.

3. **Петрусь И. П.** Аспекты практического использования беспроводной оптической технологии передачи данных [Электронный ресурс] / И. П. Петрусь, Е. А. Гузенкова // Интернет-журнал Науковедение. – 2014. – № 2 (21). – Режим доступа: http://cyberleninka.ru/ article/n/aspekty-prakticheskogo-ispolzovaniya-besprovodnoy-opticheskoy-tehnologii-peredachi-dannyh

4. **Кучерявый А. Е.** Интернет вещей / А. Е. Кучерявый // Электросвязь. – 2013. – № 1. – С. 21–24.

5. **Кучерявый А. Е.** Самоорганизующиеся сети / А. Е. Кучерявый, А. В. Прокопьев, Е. А. Кучерявый. – СПб. : Любавич, 2011. – 311 с.

6. **Хаас Х.** Беспроводная информация из каждой лампочки [Электронный ресурс] / Х. Хаас. – Режим доступа: http://www.ted.com/talks/harald_haas_wireless_data_from_every_ light_bulb.htm

7. **Алексеев В.** Что в будущем заменит сети Wi-Fi? [Электронный ресурс] / В. Алексеев. – Режим доступа: http://xn--d1aw.xn--p1ai/a/2015/11/30/So_skorostju_ot_ sveta/? articlepage=2

8. **Haas H.** Air–Interface Requirements for Mobile Data Services, chapter in. The Handbook of Information Security / H. Haas; ed. by H. Bidgoli. – New York, John Wiley & Sons, 2006. – Vol. 1. – P. 712–731.

9. **IEEE 802.15.7** [Электронный ресурс]. – Режим доступа: http://standards.ieee.org/ findstds/ standard/802.15.7-2011.html

10. **Panchal Akshay** *Li-Fi* (Light Fidelity)-The future technology In Wireless communication / Akshay Panchal, Santosh Ladani // International Journal of Information & Computation Technology. – 2014. – Vol. 4, Number 16.

11. **Povey G.** What is Visible Light Communication? [Электронный ресурс] / G. Povey. – Режим доступа: http://visiblelightcomm.com/what-is-visible-light-communication-vlc/

12. **Paraskevopoulos A.** Data are traveling by light [Электронный ресурс] / A. Paraskevopoulos. – Режим доступа: https://www.fraunhofer.de/en/press/research-news/ 2011/august/data-traveling.html

13. **Sharma Rahul R.** *Li-Fi* Technology Transmission of data through light / Rahul R. Sharma, Raunak, Akshay Sanganal // Int.J.Computer Technology & Applications. – 2014. – Vol. 5 (1). – PP. 150–154.

References

1. **Kirichek R. V.** The Investigation evolution in the wireless sensor networks area / A. E. Koucheryavy, R. V. Kirichek, A. I. Paramonov, A. V. Prokopiev // IT&Telecom. – 2014. – № 4. – PP. 29–41.

2. **Nikiforov S. G.** Teper' jelektrony mozhno uvidet': svetodiody de-lajut jelektricheskij tok ochen' zametnym / S. G. Nikiforov // Komponenty i tehnologii. – 2006. – № 3. – S. 20–27.

3. **Petrus' I. P.** Aspekty prakticheskogo ispol'zovanija besprovodnoj opticheskoj tehnologii peredachi dannyh [Electronic resource] / I. P. Petrus', E. A. Guzenkova // Internet-zhurnal Naukovedenie. – 2014. – № 2 (21). – Access mode: http://cyberleninka.ru/article/n/ aspekty-prakticheskogo-ispolzovaniya-besprovodnoy-opticheskoy-tehnologii-peredachi-dannyh

4. **Kucherjavyj A. E.** Internet veshhej / A. E. Kucherjavyj // Jelektrosvjaz'. – 2013. – № 1. – S. 21–24.

5. **Kucherjavyj A. E.** // Samoorganizujushhiesja seti / A. E. Kucherjavyj, A. V. Prokop-'ev, E. A. Kucherjavyj. – SPb. : Ljubavich, 2011. – 311 s.

6. **Haas H.** Besprovodnaja informacija iz kazhdoj lampochki [Electronic resource] / H. Haas. – Access mode: http://www.ted.com/talks/harald_haas_wireless_data_ from_every_light_ bulb.htm

7. **Alekseev V.** Chto v budushhem zamenit seti Wi-Fi? [Electronic resource] / V. Alekseev. – Access mode: http://xn--d1aw.xn--p1ai/a/2015/11/30/ So_skorostju_ot_sveta/ ?articlepage=2

8. **Haas H.** Air–Interface Requirements for Mobile Data Services, chapter in. The Handbook of Information Security / H. Haas; ed. by H. Bidgoli. – New York, John Wiley & Sons, 2006. – Vol. 1. – P. 712–731.

9. **IEEE 802.15.7** [Electronic resource]. – Access mode: http://standards.ieee.org/ findstds/ standard/ 802.15.7-2011.html

10. **Panchal Akshay** *Li-Fi* (Light Fidelity)-The future technology In Wireless communication / Akshay Panchal, Santosh Ladani // International Journal of Information & Computation Technology. – 2014. – Volume 4, Number 16.

11. **Povey G.** What is Visible Light Communication? [Electronic resource] / G. Povey. – Access mode: http://visiblelightcomm.com/what-is-visible-light-communication-vlc/

12. **Paraskevopoulos A.** Data are traveling by light [Electronic resource] / A. Paraskevopoulos. – Access mode: https://www.fraunhofer.de/en/press/research-news/2011/ august/data-traveling.html

13. **Sharma Rahul R.** *Li-Fi* Technology Transmission of data through light / Rahul R. Sharma, Raunak, Akshay Sanganal // Int.J.Computer Technology & Applications. – 2014. – Vol. 5 (1). – PP. 150–154.

Киричек Руслан Валентинович – кандидат технических наук, доцент кафедры «Сети связи и передача данных» Федерального государственного бюджетного образовательного учреждения высшего образования «Санкт-Петербургский государственный университет телекоммуникаций им. проф. М. А. Бонч-Бруевича», kirichek@sut.ru

Нгуен Дак Кы – студент группы ИКТИ-53м Федерального государственного бюджетного образовательного учреждения высшего образования «Санкт-Петербургский государственный университет телекоммуникаций им. проф. М. А. Бонч-Бруевича»

Герасимова Екатерина Михайловна – аспирант кафедры информатики и компьютерного дизайна Федерального государственного бюджетного образовательного учреждения высшего образования «Санкт-Петербургский государственный университет телекоммуникаций им. проф. М. А. Бонч-Бруевича»

УДК 121.391

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

R. V. Kirichek Bonch-Bruevich Saint-Petersburg State University of Telecommunications

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

P. A. Shilin Bonch-Bruevich Saint-Petersburg State University of Telecommunications

АНАЛИЗ ИСПОЛЬЗОВАНИЯ БПЛА КАК УЗЛА СЕТИ VANET

ANALYSIS OF THE USE OF UAV AS NETWORK NODE VANET

Беспроводные самоорганизующейся сети связи VANET обеспечивают связь между транспортными средствами, транспортом и стационарной инфраструктурой. Однако есть несколько проблем, связанных с их использованием – это частые разрывы между узлами, невозможность долгое время одному узлу выступать в роли главного узла кластера и т. д.

Одним из вариантов решения данных проблем, является возможность использования специальных БПЛА, которые могут встраиваться в инфраструктуру сети VANET, обеспечивая необходимую поддержку работы служб и организуя устойчивую связью между узлами сети.

Wireless ad hoc network connection VANET provide communication between vehicles, transport and stationary infrastructure. However, there are several problems associated with with their use – a frequent breaks between nodes, the impossibility for a long time one node act as the master node of the cluster, and so on.

One solution to these problems is the ability to use special UAV, which can be built in infrastructure VANET network, providing the necessary support services and work by organizing a stable connection between network nodes.

VANET, летающие сенсорные сети, квадрокоптер, связность.

VANET, ubiquitous flying sensor networks, quadcopter, connectivity.

Введение

Интеллектуальные Транспортные Системы (ИТС) [1] являются одним из перспективных направлений, исследуемых в нашей стране последние 5 лет. Одним из мотивирующих факторов для исследователей, послуживший всплеску работы в этом направлении является появление перового стандарта ГОСТ Р ИСО 14813-1 «Рекомендуемая модель архитектуры для сектора ИТС». В зарубежных источниках также присутствует термин

Intelligent Transport System (ITS). ИТС постоянно развиваются, приобретая в свой состав все новые и новые технологии, повышая тем самым уровень интеллектуализации. Одной из предлагаемых учеными частью ИТС должны стать беспроводные самоорганизующейся сети связи Vehicular Ad Hoc Network (VANET) [2], обеспечивающие связь между транспортными средствами, транспортом и стационарной инфраструктурой. Основной проблемой таких сетей являются частые разрывы между узлами. Другой проблемой такой сети является невозможность долгое время одному узлу выступать в роли главного узла кластера. Кроме того, есть некоторые трудности в поддержании работы служб организации дорожного движения. Одним из вариантов решения данных проблем, является возможность использования специальных БПЛА, которые могут встраиваться в инфраструктуру сети VANET, обеспечивая необходимую поддержку работы служб и организуя устойчивую связью между узлами сети.

Интеллектуальные транспортные системы постоянно развиваются. Разрабатываются и принимаются новые стандарты сетей такие как: DSRC [3] и более поздний стандарт IEEE 802.11p [4]; в первую очередь предназначаются для повышения эффективности и безопасного дорожного движения. Альтернативным источником развития этого направления является современные тенденции в мире взаимодействия цифровых устройств и интернета вещей, взаимодействия мобильных и носимых устройств с различными другими устройствами, принадлежащими человеку. Производители транспортных средств уже сейчас интегрируют в состав автомобиля системы, которые расширяют возможности взаимодействия человека и автомобиля, а также постоянно исследуют на предмет новых возможностей. Уже не новость что некоторые автомобили могут самостоятельно находить свободное место на парковке, предотвращать ДТП, сообщать о неисправности и др. Для появления новых горизонтов, дополнительных возможностей требуется развертывание дополнительной инфраструктуры сети, которую порой развернуть очень сложно и экономически не выгодно.

Беспилотные летательные аппараты (БПЛА) является еще одним популярным направлением для исследователей в последние годы. Автономные или полуавтономные БПЛА, самостоятельно организующие сети между собой и инфраструктурой, оснащенные различными датчиками, камерами, оборудованием связи, позволяют решать широкий спектр задач, а потому интересны как для гражданского, так и для военного применения. Кроме того, БПЛА применяются для организации временных узлов связи, что дает возможный способ улучшения и эффективности связи сетей. На текущий момент самым доступным вариантом БПЛА являются квадрокоптеры, используются как гражданскими, так и военными, они легко управляемы, устойчивы и недороги. Производитель автомобилей Renault в этом году предложил концепт-кар KWID в составе которого используется квадрокоптер, который делает разведку дорожного траффика, сканирует

ландшафт и определяет препятствия [5]. Такие БПЛА будут стимулировать разработчиков придумывать новые решения и приложения.

На текущий момент, научные работы по теме VANET решают огромный спектр задач, предлагают новые виды всевозможных приложений, но некоторые проблемы до сих пор так и небыли решены, в частности вопросы соединения и организации качественной связи. Высокая мобильность узлов сети VANET приводит к тому что топология крайне динамичная, связь не устойчивая. Использование придорожных станций RSU позволяет в какой-то мере решить эти проблемы, но необходимость разворачивать и стоимость накладывают свои ограничения.

В данной статье мы предлагаем новый вариант инфраструктуры сети VANET с использованием БПЛА, а также проанализируем спектр задач, который может быть решен.

Анализ работ по теме

Обзор публикаций показывает, что исследуемая проблема в российском научном сегменте не изучена вовсе. Основной причиной отсутствия исследований является новизна способа решения проблем для сетей VANET. Также существенное влияние оказывает тот факт, что исследованием проблем сетей VANET стандарта IEEE 802.11p занимается узкий круг специалистов, компаний, которые не взаимодействуют между собой и не делятся результатами наработок в этой области. Большая часть работ по теме VANET и ИТС посвящены общим вопросам организации ИТС, терминологии, исследованиям протоколов передачи данных, пропускных характеристик каналов связи между автомобилями. Полученные результаты натурных исследований зачастую неверны, по причине того, что оборудование, поддерживающее стандарт IEEE 802.11p выпускается несколькими компаниями в мире, и не доступно большинству исследователей, что вынуждает использовать методы имитационного моделирования, которые как правило имеют большие неточности, либо оборудование, работающее в рамках стандарта IEEE 802.11 предназначенное для стационарных беспроводных сетей таких как Wi-Fi , но не предназначенное для автомобильного сегмента.

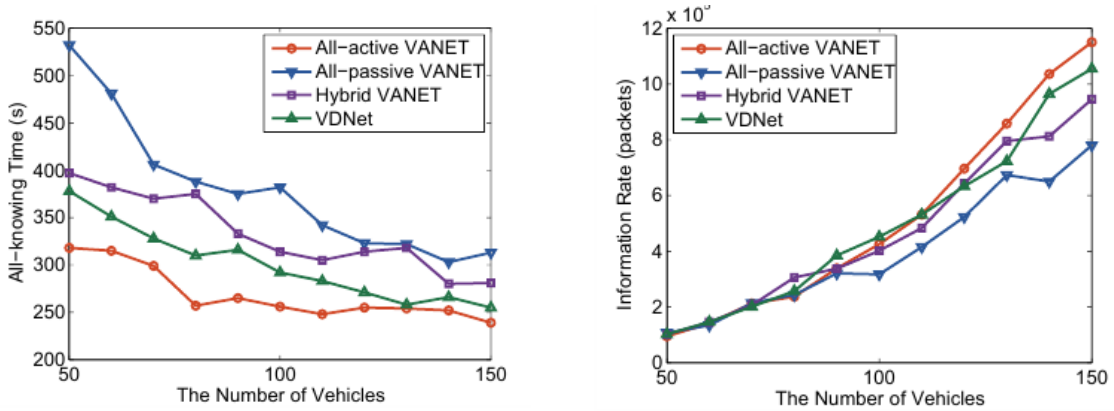
Для того чтобы все выяснить мы попробуем во всем разобраться более подробнее исходя из научных статей доступных автору.

В российском научном сегменте первыми, кто предложил использовать БПЛА для организации сети связи между собой и сбора данных были А. Е. Кучерявый, А. Г. Владыко, Р. В. Киричек, А. И. Парамонов, А. В. Прокопьев, И. А. Богданов, А. А. Дорт-Гольц в статье «Летающие сенсорные сети» за 2014 г. [6]. Более приближенной к исследуемой теме имеется статья за 2015 г. «Исследование возможности применения беспилотного летательного аппарата в качестве временного головного узла кластеров наземной сенсорной сети» за авторством А. Е. Кучерявого,

А. В. Прокопьева, А. Д. Вырелкина [7]. В рамках описанных статей указывается возможность сенсорных сетей к сбору информации с различных наземных устройств, которые находятся на пуассоновском сенсорном поле, и полностью автономны, организуется сбор информации об их состоянии и др. параметры, с целью доставки информации до сервера и дальнейшей обработки. Также рассматривается возможность организации временного головного узла на базе БПЛА. В последствии проведенное моделирование авторами этих статей показывает возможность организации подобной сети.

В статье [8] автор рассматривает задачу организации сбора данных наземной сети с использованием БПЛА применительно к приложениям мониторинга в реальном времени. В рамках данной статьи автором предлагается несколько сценариев сбора данных с помощью БПЛА с последующей передачей данных шлюзу. Эффективность тех или иных сценариев сбора данных зависит от соотношения числа узлов сети к количеству БПЛА. Также определен тип целевой функции, для приложений мониторинга в реальном времени.

В статье [9] Yang Zhang рассматриваются задачи организации механизма передачи данных в сети VANET помощью БПЛА, предлагается метод эффективной маршрутизации траффика, предлагаются новые методы и алгоритмы выбора головного узла среди нескольких БПЛА, рассчитывается эффективность использования такого подхода. В качестве термина обозначающей подобную сеть, автор использует термин VDNet. На рис. 1 (а, б) представлены результаты симуляции производительности сети VANET при использовании БПЛА.



а) б)

Рис. 1. Результаты симуляции производительности сети VANET при использовании БПЛА: а) зависимость времени опознавания (all-knowing time) ТС от числа автомобилей (the number of Vehicles); б) зависимость количества пакетов (information rate) от числа автомобилей (the number of Vehicles).
Обозначения: All-active – для активной сети, All-passive – для пассивной сети, Hybrid – для гибридной сети, VDNet – для сети с применением БПЛА

Также автором исследуется вероятность доставки пакета (delivery ratio), и задержка (end-to-end delay) в зависимости от вероятности выбора БПЛА в качестве головного узла сети VANET. На рис. 2 представлен график этих зависимостей.

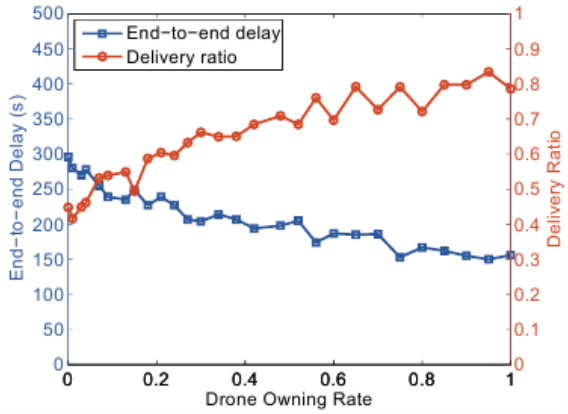


Рис. 2. Эффективность доставки пакетов

Как видно из графика, вероятность доставки пакета увеличивается, задержка уменьшается в тех случаях, когда БПЛА является головным узлом сети.

Кроме того, автор исследует три варианта эксплуатации сети в различные условия с помощью моделей. Такими моделями являются: модель закрытого типа, приближенно напоминающую город, модель разгруженного района, приближенно напоминающую сельскую местность, и модель открытого мира, где узлы могут двигаться в любом направлении. Автор указывает что точность работы системы VDNet возрастает при приеме качественного сигнала GPS, что зачастую бывает недоступно в условиях города.

В ходе анализа существующих работ было косвенно подтверждена возможность создания сетей VANET в качестве узлов которой используются БПЛА. Также стоит выделить ряд проблем, которые были не затронуты в рамках рассмотренных статей. Так в работах [6–9] предлагается обобщенная модель летающей сенсорной сети, не учитывающей особенности сети VANET, а именно высокую динамичность узлов, и высокую изменчивость топологии сети. Так же в работах не описаны альтернативные сценарии использования БПЛА, помимо сбора и мониторинга, существует целый спектр альтернативных задач, который может применяться в VANET. Кроме этого при исследовании передачи данных по сети не учитывается тип данных, тип сервиса, от которых будет завесить как нагрузка на сеть, время доставки, вероятность доставки и другие, качественные и количественные характеристики.

Проделанная работа

Первоначально организациями ETSI (www.etsi.org), Car-to-Car Consortium (www.car-to-car.org), IEEE (www.ieee.org) и др., предложено несколько вариантов архитектур сети VANET [10–13]. После изучения материалов становится понятно, что есть устройства двух типов: (On Board Unit или OBU), которые интегрируется в состав электроники автомобиля и (Roadside Unit или RSU) придорожные базовые станций. На рис. 3 представлена предлагаемая модель сети VANET с использованием беспилотной летающей станции (Unmanned Station Unit или USU).

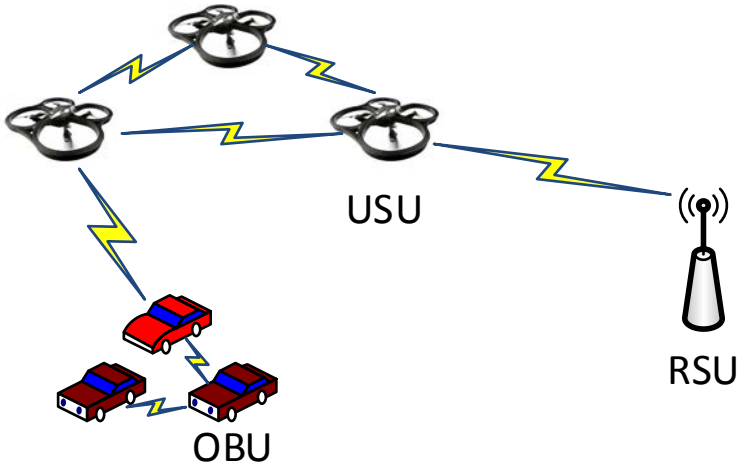


Рис. 3. Модель сети VANET с использованием БПЛА

В данной модели USU является таким же узлом сети, как и другие участники дорожного движения. USU формирует каналы связи как с автомобилями (OBU) так и придорожной станциями (RSU). Такое использование USU позволяет значительно увеличить радиус взаимодействия узлов сети, а также организовать возможность связи устройств с RSU, где прямая связь типа автомобиль-придорожная станция невозможна. Такое увеличение радиуса взаимодействия обусловлено тем что приемо-передающее оборудование USU находится значительно выше над землей чем оборудование OBU, а значит сигнал менее затухает, менее поглощается окружающими предметами и ландшафтом.

Рассмотрим также возможные преимущества на основе анализа сервисов сети VANET.

VANET предоставляет своим пользователям различные службы такие как: доступ в интернет, мультимедиа, телефония и т. д. Список служб, расширяется с появлением новых исследований в этой области. Разрабатывается группа стандартов IEEE 1609 [14] описывающих в частности службы и приложения, управление службами, взаимодействие подсистем на различных уровнях модели OSI. Помимо этого, существую исследования, направленные синтез новых служб и приложений для сети. В ходе научно-

го поиска, были выделены основные направления исследований в этой области и разделены на группы по типам служб. Структура направлений исследований представлена на рис. 4.

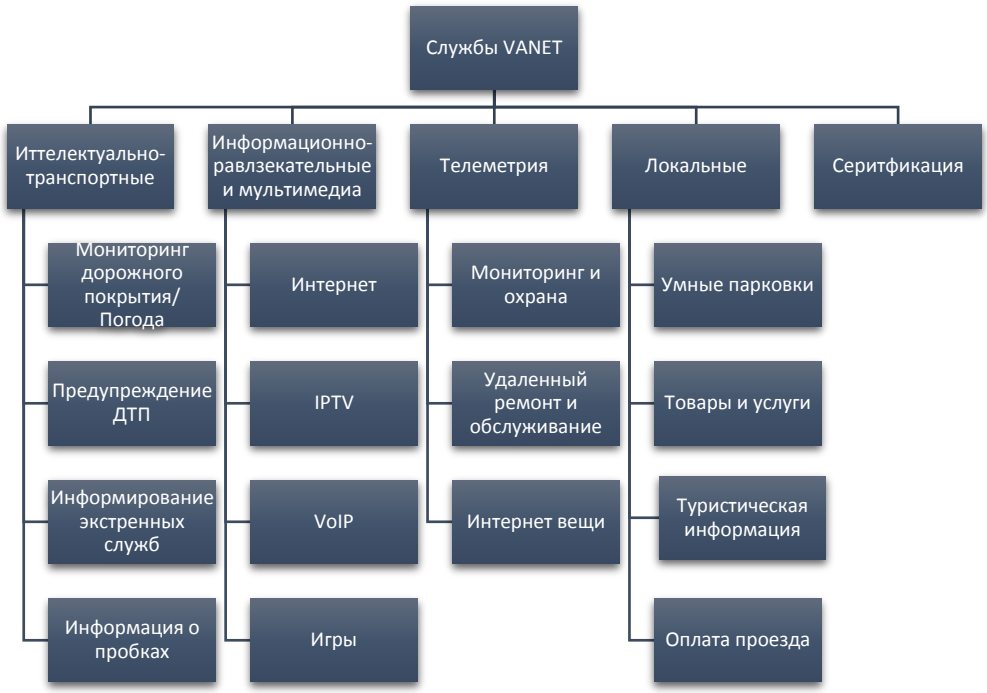


Рис. 4. Перечень возможных служб VANET

Группа служб, отвечающих за транспортную безопасность, содержит в себе: службы состояния дорожного покрытия, погоды, службы предупреждения столкновения, службы автоматического информирования экстренных служб экстренного реагирования о факте ДТП. Использование БПЛА позволит как собирать и передавать данные о дорожном покрытии, информацию о погоде. Это в свою очередь позволит заблаговременно предупреждать водителя об изменениях поверхности дорожного покрытия, а также дать рекомендации водителю в выборе скоростного режима.

Задачей службы предупреждения столкновения является обеспечение водителей информацией о ситуации на дороге, информирование водителей о возможности столкновения. Служба информирования экстренных служб обеспечивает своевременное оповещение при ДТП, а также других участников дорожного движения о ДТП. При использовании БПЛА возможно производить анализ текущей ситуации на дороге, производить заблаговременное информирование водителей о ДТП.

Информационно-развлекательная группа служб обеспечивает возможности предоставления доступа в интернет, передачи голоса по сети (VoIP, Voice over VANET), IPTV, организации многопользовательских игр и др. При использовании БПЛА для данной группы не будет очевидных преимуществ.

Группа служб телеметрии позволяет решать такие задачи как: охрана и мониторинг, удаленная помощь и оценка поломки автотранспортного средства, интеграции в состав концепции интернета вещей (англ. *Internet of Things*, IoT). При использовании БПЛА станет возможным поиск ТС, которые пропали в некотором заданном районе, сбор информации о ситуации, оценка которой в последствии поможет сформовать правильное понимание и что требуется для помощи.

Службы локальной информации обеспечивают предоставление информации о ближайшем свободном парковочном месте (возможно с системой бронирования) в определенной локации, ценах на топливо, товарах и услугах, информацию о ближайшей станцией технического обслуживания или туристическую информацию о достопримечательностях. При использовании БПЛА для данной группы не будет очевидных преимуществ.

Выводы

В ходе проделанной работы следует выделить следующие сценарии использования БПЛА в сети VANET:

1. Промежуточный узел связи IEEE 802.11p на базе БПЛА, увеличения радиуса действия сети.
2. Раннее предупреждение о столкновении с использованием БПЛА.
3. Временный узел организации движения на перекрестке с помощью БПЛА.
4. Поиск и слежение за транспортным средством при помощи БПЛА.
5. Мониторинг и анализ дорожного движения, работоспособности сети IEEE 802.11p при помощи БПЛА.
6. Временный головной узел сети VANET на базе БПЛА.

Также из приведенного анализа стоит выделить ряд преимуществ применения БПЛА для сетей VANET:

1. Увеличение радиуса действия сети.
2. Уменьшение динамичности топологии.
3. Повышение информативности водителя.
4. Организация поиска транспортного средства, при отсутствии других способов связи.

Использование БПЛА в качестве узла сети во многом расширяет возможности сети, и открывает большие возможности для исследователей с целью улучшения характеристик сети, информативности, безопасности, тем самым значительно улучшая и расширяя сферы ее применения.

Библиографический список

1. **Григорьев В. А.** Нормативное правовое регулирование и стандартизация ИТС / В. А. Григорьев, В. И. Кузнецов, Ю. А. Распаев, С. А. Тараканов // Электросвязь. – 2013. – №. 10. – С. 9–13.

2. **Кучерявый А. Е.** Сети связи общего пользования. Тенденции развития и методы расчета / А. Е. Кучерявый, А. И. Парамонов, Е. А. Кучерявый. – Москва: ФГУП ЦНИИС, 2008. – 296 с.

3. **Vehicle Safety** Communications Project Final Report, U. S. Dept. Trans., Nat. Highway Traffic Safety Admin., Rep. DOT HS 810 591, 2006.

4. **IEEE 802.11p-2012** – IEEE Standard for Information technology-- Local and metropolitan area networks-- Specific requirements-- Part 11: Wireless LAN Medium Access Control (MAC) and Physical Layer (PHY) Specifications Amendment 6: Wireless Access in Vehicular Environments, 2012.

5. **Prigg Mark** Never get stuck in traffic again: Renault reveals concept car which comes with a DRONE that watches out for gridlock / Mark Prigg; ed. By DailyMail.co.uk [Online], 2014. – URL: http://www.dailymail.co.uk/sciencetech/article-2553422/Release-drone-Renault-reveals-concept-car-traffic-spotting-quadcopter-built-roof.html

6. **Кучерявый А. Е.** Летающие сенсорные сети / А. Е. Кучерявый, А. Г. Владыко, Р. В. Киричек, А. И. Парамонов, А. В. Прокопьев, И. А. Богданов, А. А. Дорт-Гольц // Электросвязь. – 2014. – №. 9. – С. 2–5.

7. **Кучерявый А. Е.** Исследование возможности применения беспилотного летательного аппарата в качестве временного головного узла кластеров наземной сенсорной сети / А. Е. Кучерявый, А. В. Прокопьев, А. Д. Вырелкин // Информационные технологии и телекоммуникации. – 2015. – №. 1 (9). – С. 27–34.

8. **Варельджян К. С.** Оптимизация траектории движения БПЛА в летающих сенсорных сетях / К. С. Варельджян, А. И. Парамонов, Р. В. Киричек // Электросвязь. – 2015. – № 7. – С. 20–25.

9. **VDNet**: An Infrastructure-less UAV-Assisted Sparse VANET System with Vehicle Location Prediction.

10. **IEEE P1609.4-2010** - IEEE Standard for Wireless Access in Vehicular Environments (WAVE), 2010.

11. **Car 2** Car Communication Consortium Manifesto. Overview of the C2C–CC System.

12. **ETSI TS 102 636–3 V1.1.1 (2010–03)**: Intelligent Transport Systems (ITS); Vehicular Communications; GeoNetworking; Part 3: Network architecture. – European Telecommunications Standards Institute, 2010.

13. **Draft ETSI EN 302 665 V1.0.0 (2010–03)**: Intelligent Transport Systems (ITS); Communications Architecture. – European Telecommunications Standards Institute, 2010.

14. **Draft Standard** for Wireless Access in Vehicular Environments (WAVE). – Architecture. – IEEE P1609.0/D0.1. – Institute of Electrical and Electronics Engineers, 2010.

References

1. **Grigor'ev V. A.** Normativnoe pravovoe regulirovanie i standartizacija ITS / V. A. Grigor'ev, V. I. Kuznecov, Ju. A. Raspaev, S. A. Tarakanov // Jelektrosvjaz'. – 2013. – № 10. – S. 9–13.

2. **Kucherjavyj A. E.** Seti svjazi obshhego pol'zovanija. Tendencii razvitija i metody rascheta / A. E. Kucherjavyj, A. I. Paramonov, E. A. Kucherjavyj. – Moskva: FGUP CNIIS, 2008. – 296 c.

3. **Vehicle Safety** Communications Project Final Report, U. S. Dept. Trans., Nat. Highway Traffic Safety Admin., Rep. DOT HS 810 591, 2006.

4. **IEEE 802.11p-2012** – IEEE Standard for Information technology-- Local and metropolitan area networks-- Specific requirements-- Part 11: Wireless LAN Medium Access Control (MAC) and Physical Layer (PHY) Specifications Amendment 6: Wireless Access in Vehicular Environments, 2012.

5. **Prigg Mark** Never get stuck in traffic again: Renault reveals concept car which comes with a DRONE that watches out for gridlock / Mark Prigg; ed. By DailyMail.co.uk [Online], 2014. – URL: http://www.dailymail.co.uk/sciencetech/article-2553422/Release-drone-Renault-reveals-concept-car-traffic-spotting-quadcopter-built-roof.html

6. **Kucherjavyj A. E.** Letajushhie sensornye seti / A. E. Kucherjavyj, A. G. Vladyko, R. V. Kirichek, A. I. Paramonov, A. V. Prokop'ev, I. A. Bogdanov, A. A. Dort-Gol'c // Jelektrosvjaz'. – 2014. – №. 9. – S. 2–5.

7. **Koucheryavy A. E.** Research applications unmanned aerial vehicles as a temporary the head node cluster ground sensor networks / A. E. Koucheryavy, A. V. Prokopiev, A. D. Vyrelkin // IT&Telecom. – 2015. – №. 1 (9). – PP. 27–34.

8. **Varel'dzhjan K. S.** Optimizacija traektorii dvizhenija BPLA v letajushhih sensornyh setjah / K. S. Varel'dzhjan, A. I. Paramonov, R. V. Kirichek // Jelektrosvjaz'. – 2015. – № 7. – S. 20–25.

9. **VDNet**: An Infrastructure-less UAV-Assisted Sparse VANET System with Vehicle Location Prediction.

10. **IEEE P1609.4-2010** - IEEE Standard for Wireless Access in Vehicular Environments (WAVE), 2010.

11. **Car 2** Car Communication Consortium Manifesto. Overview of the C2C–CC System.

12. **ETSI TS 102 636–3 V1.1.1 (2010–03)**: Intelligent Transport Systems (ITS); Vehicular Communications; GeoNetworking; Part 3: Network architecture. – European Telecommunications Standards Institute, 2010.

13. **Draft ETSI EN 302 665 V1.0.0 (2010–03)**: Intelligent Transport Systems (ITS); Communications Architecture. – European Telecommunications Standards Institute, 2010.

14. **Draft Standard** for Wireless Access in Vehicular Environments (WAVE). – Architecture. – IEEE P1609.0/D0.1. – Institute of Electrical and Electronics Engineers, 2010.

Киричек Руслан Валентинович – кандидат технических наук, доцент кафедры «Сети связи и передача данных» Федерального государственного бюджетного образовательного учреждения высшего образования «Санкт-Петербургский государственный университет телекоммуникаций им. проф. М. А. Бонч-Бруевича», kirichek@sut.ru

Шилин Павел Анатольевич – аспирант кафедры «Сети связи и передача данных» Федерального государственного бюджетного образовательного учреждения высшего образования «Санкт-Петербургский государственный университет телекоммуникаций им. проф. М. А. Бонч-Бруевича»

УДК 621.391

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

A. S. Muthanna Bonch-Bruevich Saint-Petersburg State University of Telecommunications

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

A. A. Khakimov Bonch-Bruevich Saint-Petersburg State University of Telecommunications

СРАВНЕНИЕ ПРОТОКОЛОВ WEB-ВЕЩЕЙ

COMPARISON OF PROTOCOLS FOR WEB OF THINGS

Веб вещей (WoT) может рассматриваться как новая парадигма Интернета вещей (IoT) и облачных вычислений. Захват, обработка, хранение и обмен больших объемов данных являются ключевым требованием в данной среде. В то время как разработчики используют существующие технологии, чтобы построить IoT, научно-исследовательские группы работают над адаптацией протоколов к IoT в целях оптимизации коммуникации. В этой статье рассматриваются сравнения существующих протоколов WoT и проводится моделирование протокола CoAP в Cooja симуляторе.

Web of things (WoT) can be considered as the new paradigm of the Internet of Things (IoT) and cloud computing. Capturing, processing, storage and exchange of large amounts of data is a key requirement in this medium. While developers use existing technologies to build IoT, research groups are working to adapt protocols for IoT in order to optimize communication. This paper deals with the comparison of existing protocols WoT and also was shown the implementation of CoAP protocol in Cooja simulator.

Интернет вещей,Web-Вещей, протоколы, CoAP.

Internet of things, Web of Things, protocols, CoAP.

Введение

Последние достижения в беспроводных сенсорных сетях (БСС) [1] и использование IP-протокола в устройствах с ограниченными ресурсами радикально изменили структуру сети Интернет [2]. Триллионы умных устройств в ближайшее время будут подключены к сети Интернет, что позволит говорить о формировании концепции Интернета Вещей (ИВ) [3].

В инженерном совете Интернета IETF (Internet Engineering Task Force) был стандартизирован новый протокол IPv6 over Low power Wireless Personal Area Networks (6LoWPAN) [4]. Этот новый стандарт позволяет использовать протокол IPv6 в сетях с низким энергопотреблением и потерями

(LLNs) [5], которые, в свою очередь, основаны на стандарте IEEE 802.15.4. В дополнение к 6LoWPAN, рабочая группа IETF разработала новый протокол маршрутизации Routing Protocol for Low-power and Lossy networks (RPL) [8].

Одним из основных преимуществ IP на базе сети LLNs является применение стандартных архитектур Web-услуг без необходимости использования шлюзов, поскольку смарт-объекты будут интегрированы не только с Интернетом, но и с Web. Эта интеграция определяется как Web-вещей (WoT-Web of Things) [2]. WoT является составной частью Интернета Вещей и предоставляет возможность мониторинга и управления умными вещами с помощью страниц WWW. Концепция Web of Things (WoT) обеспечивает работу прикладного уровня для создания приложений Интернета Вещей. Целью технологии WoT является создание сети для узлов с низким энергопотреблением и потерями на основе усовершенствованных протоколов прикладного уровня.

Преимущество новой технологии состоит в том, что приложения для смарт-объектов могут быть построены на архитектуре REST (Representational State Transfer). Архитектура REST позволяет приложениям опираться на набор существующих услуг, которые могут запрашиваться клиентами в зависимости от их текущих потребностей.

Рабочая группа IETF CoRE выполнила работы по стандартизации для внедрения веб-услуг в сетях смарт-объектов. В группе CoRE на основе REST разработан протокол для веб-передачи Constrained Application Protocol (CoAP).

Целью данной статьи является сравнение протокола CoAP с другими протоколами для использования в WoT.

Протоколы Web of Things

Протокол XMPP

Расширяемый протокол обмена сообщениями и информацией о присутствии Extensible Messagingand Presence Protocol (XMPP). Данный протокол был стандартизирован в IETF более десяти лет назад и хорошо зарекомендовал себя, в результате чего до сих пор широко используется в сети Интернет. Однако, будучи достаточно давно разработанным протоколом, XMPP имеет ряд естественных недостатков для реализации новых приложений. По этой причине в прошлом году компания Google прекратила поддержку стандарта XMPP. Тем не менее, в последнее время XMPP вновь получил поддержку инженерного сообщества в качестве протокола для устройств Интернета Вещей. XMPP работает на основе протокола транспортного уровня TCP и обеспечивает асинхронный и синхронный алгоритм обмена сообщениями. Протокол XMPP предназначен для коммуникаций в реальном времени. Он поддерживает быстрый обмен сообщениями,

и обеспечивает низкую латентность (задержку) по времени. Также XMPP поддерживает взаимодействие с криптографическими протоколами TLS/SSL. Тем не менее, он не способен обеспечить требуемое качество обслуживания, что делает его применение нецелесообразным для M2M-коммуникаций. XMPP поддерживает архитектуру обмена сообщениями «издатель/подписчик», которая больше подходит для ИВ в отличие от принципа обмена сообщениями «запрос/ответ». Известно, что протокол поддерживается огромным количеством разработчиков и рядовых пользователей сети Интернет, что является преимуществом в сравнении с относительно новой технологией MQTT.

Однако, в связи с тем, что протокол XMPP основан на специализированном языке разметки XML, в его работе существует ряд недостатков, связанных с дополнительными расходами на передачу данных из-за лишних, требующих разбора, тегов XML, что увеличивает требования к вычислительным способностям, и, как следствие, увеличивает энергопотребление устройства.

Restful services

REST на самом деле не протокол, а архитектурный стиль. Он был впервые представлен Роем Филдингом (Roy Thomas Fielding) в 2000 году, и широко используется до сих пор. В его работе могут использоваться различные протоколы передачи данных, например, при использовании HTTP задействуются методы HTTP GET, POST, PUT и DELETE для предоставления ресурсов ориентированной системы обмена сообщениями, где все действия могут выполняться лишь с помощью синхронных HTTP-команд типа «запрос/ответ». Команда использует встроенный в сообщение Accept заголовок HTTP для указания формата содержащихся данных. Формат данных может быть XML или json (нотация объектов JavaScript) и зависит от http-сервера и его конфигурации. Всё вышеперечисленное может быть реализовано в смартфонах и планшетных приложениях, потому что требует только библиотеки разработчиков HTTP, которые доступны для всех операционных систем (ОС).

Функциональные особенности протокола HTTP могут быть использованы также для проверки подлинности и типа содержимого переговоров. Restful-сервисы используют различные протоколы прикладного уровня, в частности HTTP, HTTPS. Однако на текущий момент, множество коммерческих M2M платформ не поддерживают запросы HTTP/HTTPS. Вместо этого, они предоставляют уникальные ключи аутентификации, которые должны быть в заголовке каждого запроса для обеспечения определенного уровня безопасности ИВ. Однако маловероятно, что протоколы, использующие концепцию Restful, станут доминирующими протоколами связи. Учитывая нынешние тенденции в разработке мобильных приложений, связанные с дополнительными расходами пропускного ресурса канала связи,

накладываемые архитектурой «запрос/ответ» и влияющими на скорость разряда батареи. Также данная архитектура заполняет пропускной канал непрерывно поступающими опросами, не обновляющими статус устройства. Такую проблему можно избежать, если использовать протоколы прикладного уровня, функционирующие на основе архитектуры «издатель/подписка», например, MQTT, XMPP или CoAP.

AMQP

Advanced Message Queuing Protocol (AMQP) – это протокол прикладного уровня, предназначенный для передачи сообщений между компонентами системы, возникший в финансовой отрасли. Данный протокол может использовать различные протоколы транспортного уровня, но рассчитан на протоколы с гарантированной доставкой данных, например, TCP. Протокол AMQP обеспечивает асинхронную передачу данных, на базе модели издатель/подписчик. Его основным преимуществом является функция хранения и пересылки, которая обеспечивает надежность даже после сбоев сети. Надежность обеспечивают следующие свойства протокола:

- **«Как минимум раз»** означает, что протокол гарантирует корректную доставку сообщения, а в случае неудачи совершает повторную отправку.
- **«По крайней мере один раз»** означает, что сообщение будет доставлено, безусловно, один раз, возможно и больше.
- **«Точно раз»** означает, что сообщение будет доставлено только один раз.

В Последнее время исследования показали, что AMQP имеет низкую вероятность успешной доставки сообщения при низкой пропускной способности [10], но вероятность увеличивается по мере увеличения пропускной способности. Другое исследование показывают, что по сравнению с вышеупомянутым REST, AMQP может отправить большее количество сообщений в секунду. Кроме того, было установлено, что AMQP среди 2000 пользователей, распределенных по пяти континентам, может обрабатывать 300 миллионов сообщений в день.

WebSocket

Протокол WebSocket был разработан в рамках инициативы HTML по установлению каналов связи поверх протокола TCP. В WebSocket клиент инициализирует установления соединения с сервером, для установления WebSocket сессии. Само установление соединения схоже с установлением соединения в протоколе HTTP и, таким образом, web-серверы могут обрабатывать сессию WebSocket, используя тот же порт, что и HTTP соединения. На самом деле, во время сеанса http-заголовки удаляются и клиенты, и серверы могут обмениваться сообщениями в асинхронном полнодуп-

лексном соединении. Сеанс связи может быть прекращен по запросу с серверной или клиентской стороны. WebSocket используется для уменьшения нагрузки на каналы связи в Сети Связи Общего Пользования, обеспечивая в реальном времени полную дуплексную связь. Существует также протокол WebSocket, называемый суб-протокол Websocket (WAMP), который создан для поддержки в WebSocket модели издатель\подписчик. Система обмена сообщениями WebSocket работает поверх протокола TCP и сама не реализует никаких механизмов защиты. При необходимости, безопасные соединения могут быть реализованы поверх WebSocket, с помощью криптографических протоколов TLS/SSL. В ходе сессии сообщения WebSocket имеют размер 2 байта. В ходе исследований было выяснено, что при загрузке канала связи протокол HTTP повторно отправляет HTTP-заголовок, таким образом увеличивая задержки. WebSocket по оценкам, обеспечивает снижение три к одному латентности против полудуплексного режима HTTP опроса. Протокол WebSocket не предназначен для устройств с ограниченными вычислительными возможностями, в отличие от вышеперечисленных протоколов, основанных на клиент-серверной архитектуре. Данный протокол мало приспособлен для решений концепции ИВ, однако он предназначен для работы в реальном времени, является защищенным протоколом, а также минимизирует требуемые к каналу связи требования, и при использовании протокола WAMP позволяет организовать эффективные сценарии обмена информации для ИВ. Таким образом, WebSocket может конкурировать с любым другим протоколом, работающим поверх протокола TCP.

CoAP протокол

Constrained Application Protocol (CoAP) – протокол прикладного уровня, разработанный инженерами IETF для устройств с низким энергопотреблением и высокими потерями (LLN). Он был разработан на основе протокола HTTP, поэтому совместим с ним.

CoAP предназначен для использования в очень простых электронных устройствах, и позволяет им взаимодействовать в интерактивном режиме через сеть Интернет. Подробное описание имеется в стандарте RFC под номером 7252.

Протокол CoAP работает поверх протокола транспортного уровня UDP. Как и HTTP он использует методы GET, POST, PUT, DELETE при клиент-серверном взаимодействии. Кроме того, протокол можно использовать для группового взаимодействия (multicast), что дает ему преимущества над протоколами, работающими поверх TCP. Так как CoAP работает поверх UDP, потребовалась разработка механизмов, которые позволили достигнуть необходимого уровня надёжности. Два бита в заголовке сообщения CoAP используются для контроля качества доставки. На основе данного поля можно выделить четыре разновидности сообщений:

1. Confirmable – сообщения, которые требуют подтверждения доставки (ACK). Поддерживает как синхронный, так и асинхронный режим работы.

2. Non-Confirmable – сообщения, которые не требуют подтверждения доставки.

3. Acknowledgment – сообщение, которое отправляется в ответ на сообщения типа Confirmable.

4. Reset – сообщение, отправляемое в случае если принимающее сообщение повреждено.

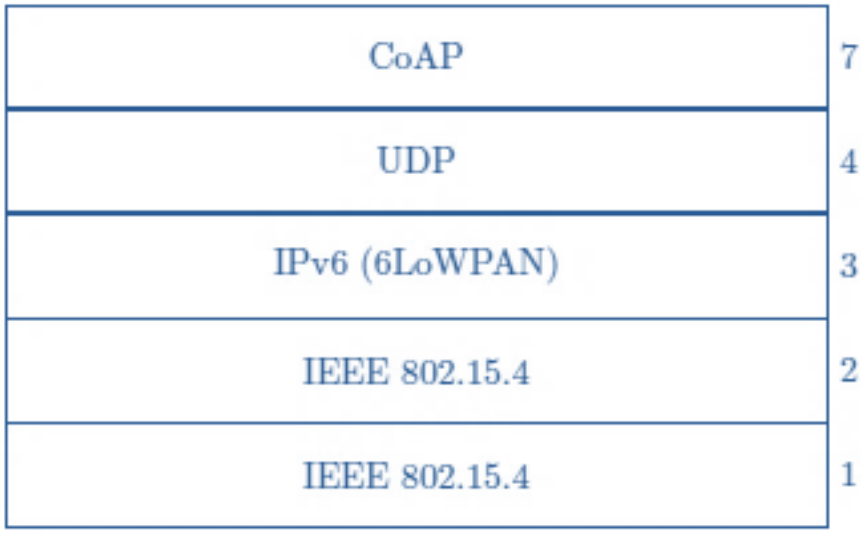


Рис. 1. Протокол CoAP

Также для протокола CoAP существует механизм Stop-and-Wait, который задерживает отправку сообщений и отправляет повторно сообщения типа Confirmable, в случае их неудачной доставки. И также в CoAP имеется поле, содержащее уникальный идентификатор сообщения размером 16 бит, с помощью которого возможно обнаружить дубликат.

Протокол CoAP, в совокупности с методом HTTP Mapping позволяет, CoAP-клиенту с помощью прокси-сервера подключаться к HTTP-серверу. По аналогии HTTP-сервер имеет возможность подключения и передачи данных к CoAP-клиенту.

Для обеспечения безопасности протокол CoAP использует криптографический протокол DTLS поверх UDP. Он обеспечивает корректную передачу данных, аутентификацию устройства на сервере и установление криптографически защищенного канала связи.

MQTT

Message Queue Telemetry Transport (MQTT) – протокол прикладного уровня, разработанный компанией IBM для упрощения работы M2M. Это

асинхронный протокол, построенный поверх протокола транспортного уровня TCP. В качестве сервера MQTT используется так называемый брокер. Каждый клиент, подключенный к MQTT-брокеру, при обновлении брокера, получает новые данные от канала на брокере, на который он подписан. MQTT разработан для устройств с низким энергопотреблением и высокими потерями (LLN).

Типы сообщений MQTT:

1. Fireandforget – сообщение отправляется один раз и не требуется подтверждения.

2. Deliveredatleastonce – повторно отправленные сообщения требуют подтверждения.

3. Deliveredexactlyonce – механизм четырехступенчатого рукопожатия клиент-брокера.

MQTT, как и протокол HTTP, для обеспечения безопасной передачи данных использует методы аутентификации TLS/SSL.

Реализация протокола CoAP в симуляторе Cooja

Для реализации протокола авторы использовали инструменты разработки, поставляемые с ОС Contiki [7, 9]. Данная операционная система поддерживает современные протоколы связи для сетей с низким энергопотреблением и потерями: 6LoWPAN, RPL, CoAP. Моделирование производилось с помощью инструмента COOJA. Для построения сети на базе CoAP использовалась реализация протокола ОС Contiki.

На рис. 2 показано сенсорное поле, которое представляет собой квадрат 100 на 100 метров и содержит 22 узла, размещенных случайным образом.

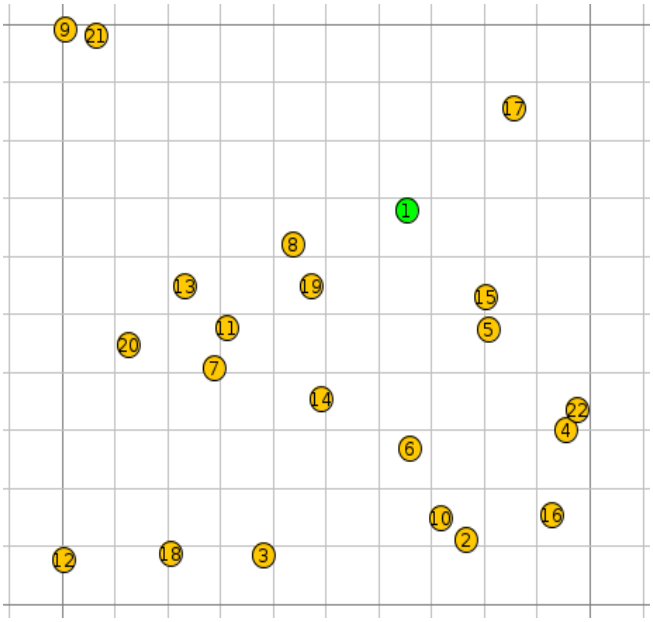


Рис. 2. Сенсорное поле

Для реализации работы CoAP сервера (er-rest) на cooja нужно маршрутизировать запросы\ответы пакетов между ОС Contiki Ubuntu и Cooja. В качестве такого маршрутизатора использовались как внешние платформы, так и localhost. Для этого использовался интерфейс с адресом 127.0.0.1 узла, на котором скомпилирован er-rest (server CoAP) и потом установить маршрутизацию между сенсорным полем и ОС. Для решения данной задачи авторы использовали протокол RPL (рис. 3).

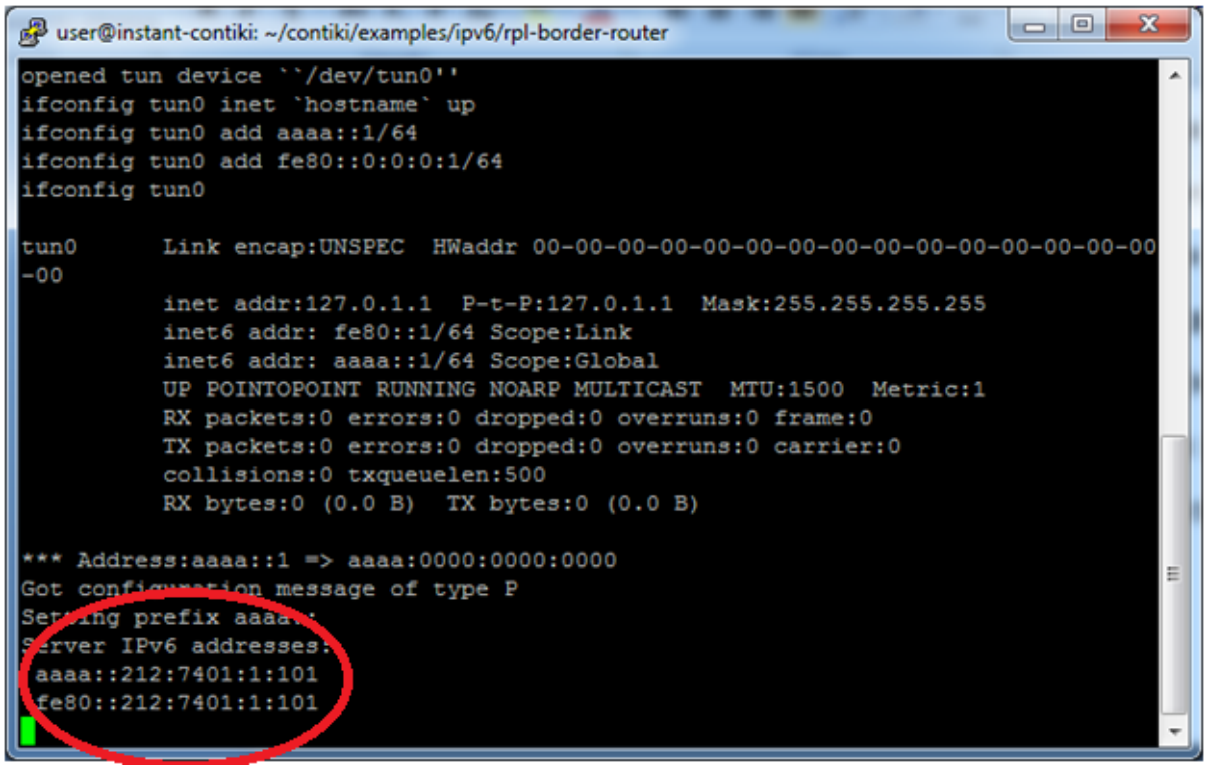


Рис. 3. Сетевой адрес er-rest узла

Протокол CoAP в WoT

Для того чтобы обеспечить удобное взаимодействие пользователя с устройствами Интернета Вещей в браузерах используют дополнительный инструмент Copper (решение для браузера Mozila Firefox) (CU). CoAP клиент (CU) позволяет взаимодействовать с сервером CoAP (рис. 4). Для подключения требуется ввести в адресной строке URL адрес удалённого узла. В открывшейся страничке можно увидеть методы GET,PUT, POST, и DELETE. Их регистрирует обработчик протокола для схем COAP URI (Uniform Resource Identifier) – унифицированный идентификатор ресурса. Пользователи могут просматривать состояние устройств, использовать закладки, обнаруживать и добавлять новые устройства по ссылкам, как в обычных документах HTML.

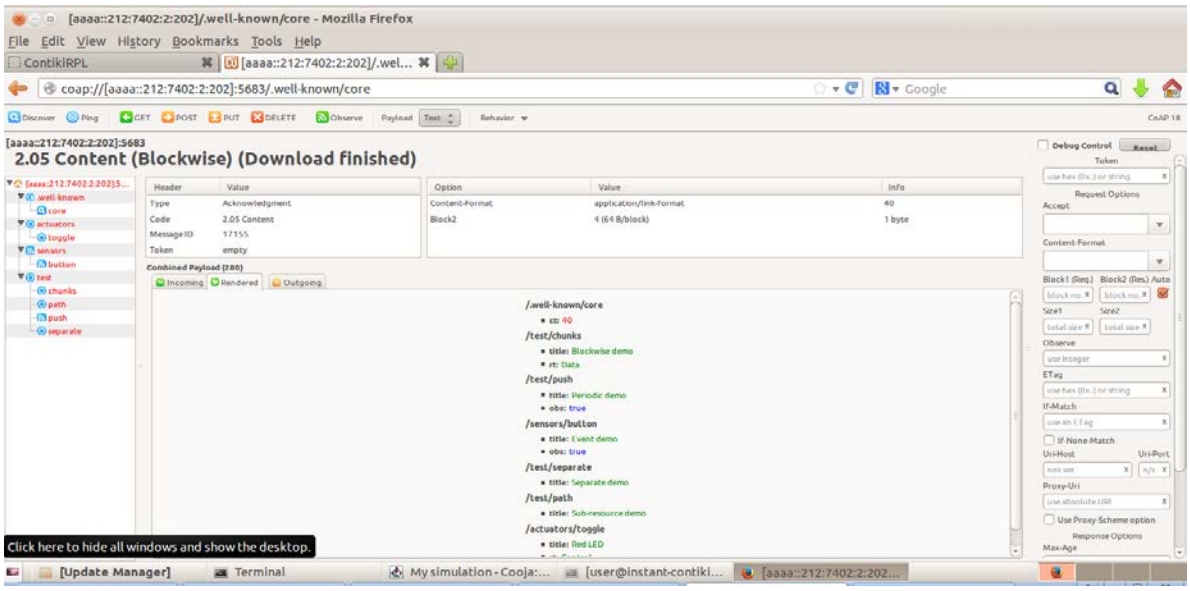


Рис. 4. Протокол CoAP в WoT

Основным преимуществом протокола CoAP – является то, что он работает поверх UDP, что уменьшает объём служебной информации в передаваемом пакете и не требует дополнительной синхронизации, что очень хорошо для сетей с низким энергопотреблением. Также это обеспечивает возможность мониторинга удалённого объекта в реальном времени в случаях, когда невозможно обеспечить узел постоянным источником энергии.

ТАБЛИЦА. Сравнение протоколов WoT

Протокол	**Транспортный уровень**	**QOS**	**Архитектура**	**Безопасность**
CoAP	UDP	ДА	Запрос\ответ	DTLS
MQTT	TCP	ДА	издатель\подписчик	TLS/SSL
XMPP	TCP	нет	издатель\подписчик Запрос\ответ	TLS/SSL
AMQP	TCP	да	издатель\подписчик	TLS/SSL
WebSocket	TCP	Нет	Клиент\сервер издатель\подписчик	TLS/SSL

Заключение

В работе проанализированы наиболее популярные протоколы, которые получили развитие в рамках WoT.

Произведено сравнение протоколов WoT и рассмотрены их возможности по развитию Интернета Вещей.

Проанализирован протокол CoAP, являющийся новым веб-протоколом, который был стандартизирован IETF, его функции, специфицированые для приложений Интернета Вещей и сценариев обмена инфор-

мацией машина-машина (M2M), что позволяет утверждать то, что CoAP очень перспективен для WoT.

Библиографический список

1. **Кучерявый А. Е.** Самоорганизующиеся сети и новые услуги / А. Е. Кучерявый // Электросвязь. – 2009. – № 1. – С. 19–23.

2. **Кучерявый А. Е.** Самоорганизующиеся сети / А. Е. Кучерявый, А. В. Прокопьев, Е. А. Кучерявый. – СПб. : Любавич, 2011. – 311 с.

3. **Кучерявый А. Е.** Интернет вещей / А. Е. Кучерявый // Электросвязь. – 2013. – № 1. – С. 21–24.

4. **Прокопьев А. В.** Перспективы использования протокола 6LoWPAN в сетях IEEE 802.15.4 / А. В. Прокопьев // Электросвязь. – 2009. – № 1. – С. 33–36.

5. **Routing Over** Low power and Lossy networks IETF WG [Электронный ресурс]. – Режим доступа: http://tools.ietf.org/wg/roll

6. **Кучерявый А. Е.** Сравнительный анализ протоколов маршрутизации RPL и AODV / А. Е. Кучерявый, А. С. Мутханна, А. В. Прокопьев // В сборнике: Актуальные проблемы инфотелекоммуникаций в науке и образовании II Международная научно-техническая и научно-методическая конференция. Санкт–Петербург, 2013. – С. 167–171.

7. **Contiki** Operating System [Электронный ресурс]. – Режим доступа: http://www.contiki-os.org/.

8. **Мутханна А. С.** Сравнение протоколов маршрутизации для всепроникающих сенсорных сетей / А. С. Мутханна // Электросвязь. – 2014. – № 9. – С. 5–10.

9. **Мутханна А.** С. CONTIKI – Операционная система для Интернета вещей / А. С. Мутханна // В сборнике: Актуальные проблемы инфокоммуникаций в науке и образовании. Сб. науч. ст. – СПб., 2014. – С. 304–308.

10. http://www.amqp.org/about/examples, cited 28 Jul 2014.

References

1. **Kucherjavyj A. E.** Samoorganizujushhiesja seti i novye uslugi / A. E. Kucherjavyj // Jelektrosvjaz'. – 2009. – № 1. – S. 19–23.

2. **Kucherjavyj A. E.** Samoorganizujushhiesja seti / A. E. Kucherjavyj, A. V. Prokop'ev, E. A. Kucherjavyj. – SPb. : Ljubavich, 2011. – 311 s.

3. **Kucherjavyj A. E.** Internet veshhej / A. E. Kucherjavyj // Jelektrosvjaz'. – 2013. – № 1. – S. 21–24.

4. **Prokop'ev A. V.** Perspektivy ispol'zovanija protokola 6LoWPAN v setjah IEEE 802.15.4 / A. V. Prokop'ev // Jelektrosvjaz'. – 2009. – № 1. – S. 33–36.

5. **Routing** Over Low power and Lossy networks IETF WG [Электронный ресурс]. – Режим доступа: http://tools.ietf.org/wg/roll

6. **Koucheryavy A.** The RPL and AODV Routing Protocol Features Comparison / A. Muthanna, A. Prokopiev, A. Koucheryavy // II International Scientific and Technical and Methodological Conference «Actual Problems of Infotelecommunications in Science and Education». – SPb. : SUT, 2013. – PP. 167–171.

7. **Contiki** Operating System [Электронный ресурс]. – Режим доступа: http://www.contiki-os.org/.

8. **Muthanna A. S.** Sravnenie protokolov marshrutizacii dlja vse-pronikajushhih sensornyh setej / A. S. Muthanna // Jelektrosvjaz'. – 2014. – № 9. – S. 5–10.

9. **Muthanna A.** Contiki – Operating System for Internet of Things / A. Muthanna // III International Scientific and Technical and methodological Conference «Actual Problems of Infotltcommunications in science and Education». – SPB. : SUT, 2014. – PP. 304–308.

10. http://www.amqp.org/about/examples, cited 28 Jul 2014.

Мутханна Аммар С. – аспирант кафедры «Сети связи и передача данных» Федерального государственного бюджетного образовательного учреждения высшего образования «Санкт-Петербургский государственный университет телекоммуникаций им. проф. М. А. Бонч-Бруевича», ammarexpress@gmai.com

Хакимов Абдукодир Абдукаримович – студент группы ИКТУ-210 Федерального государственного бюджетного образовательного учреждения высшего образования «Санкт-Петербургский государственный университет телекоммуникаций им. проф. М. А. Бонч-Бруевича»

СИСТЕМНЫЙ АНАЛИЗ, УПРАВЛЕНИЕ И ОБРАБОТКА ИНФОРМАЦИИ

УДК 621.391

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

S. S. Vladimirov Bonch-Bruevich Saint-Petersburg State University of Telecommunication

ЭФФЕКТИВНОСТЬ МАЖОРИТАРНОГО ДЕКОДИРОВАНИЯ КОДА МАКСИМАЛЬНОЙ ДЛИНЫ ПО *K*-ЭЛЕМЕНТНЫМ ЛИНЕЙНО-НЕЗАВИСИМЫМ КОМБИНАЦИЯМ В ДВОИЧНОМ СИММЕТРИЧНОМ КАНАЛЕ

THE EFFICIENCY OF MAXIMUM LENGTH CODE MAJORITY-LOGIC DECODING ALGORITHM WITH K-ARY LINEAR-INDEPENDENT SUBSEQUENCES IN BINARY SYMMETRIC CHANNEL

Статья знакомит с последними результатами научных исследований автора в рамках научной работы по оценке эффективности помехоустойчивых кодов с использованием различных алгоритмов декодирования. Для оценки эффективности приводятся вероятностные характеристики исследуемого алгоритма по вероятности правильного приема в сравнении с новыми и известными классическими алгоритмами. Приводится математика алгоритма декодирования кода максимальной длины по k-элементным линейно-независимым комбинациям. Сделаны предположения об использовании исследуемого алгоритма в системах с адаптацией к каналу передачи данных.

The paper presents the latest results of author's scientific studies referred to large-scale research of the efficiency of error-correcting coding algorithms. The efficiency of examined decoding algorithm has been estimated with probability of correct receiving in comparison with modern and classical decoding algorithms. There has been considered the mathematic basis of maximum length code majority-logic decoding algorithm with k-ary linear-independent subsequences. The paper presentes proposal of the examined algorithm usage in data transmission systems with adaptation to data transmission channel.

код максимальной длины, последовательность максимальной длины, М-последовательность, помехоустойчивое кодирование, мажоритарное декодирование, двоичный симметричный канал, вероятностные характеристики, метод декодирования на основе двойственного базиса, корреляционный метод декодирования, табличный метод декодирования.

Maximum length code, maximum length sequence, M-sequence, error-correcting coding, majority-logic decoding, binary symmetric channel, probabilistic characteristics, dual basis based decoding algorithm, correlation decoding algorithm, table decoding algorithm.

Введение

Развитие систем и сетей передачи цифровой информации неразрывно связано с совершенствованием и развитием методов обработки сигналов в цифровых каналах, среди которых важную роль играют методы помехоустойчивого кодирования, повышающие вероятность правильного приема информации, передаваемой по каналу связи. Актуальность разработки обусловлена исследованием нового алгоритма декодирования, уменьшающего время обработки полученной на приеме искаженной кодовой комбинации и тем самым сокращающего время передачи данных. Поскольку разные коды и алгоритмы их декодирования по-разному работают в различных каналах передачи данных, одной из важных задач является проведение соответствующих исследований как на компьютерных моделях, так и в реальных системах передачи.

В данной работе сообщаются результаты оценки эффективности нового алгоритма мажоритарного декодирования циклического кода максимальной длины по k-элементным линейно-независимым комбинациям [1, 2] в двоично-симметричном канале, и предлагаются предварительные рекомендации по его использованию. Эта работа отражает новый результат очередного этапа научных исследований в рамках системной научной работы по исследованию кодов максимальной длины. В ранних публикациях предлагались результаты исследований по оценке исправляющей способности рассматриваемого алгоритма методом полного перебора [2, 3].

Второй раздел статьи описывает математику кодов максимальной длины и принципы работы алгоритма мажоритарного декодирования по k-элементным линейно-независимым комбинациям. Третий раздел посвящен вопросам построения программной модели, использованной для анализа. В четвертом разделе приводятся результаты моделирования исследуемого алгоритма декодирования.

Код максимальной длины и его мажоритарное декодирование по k-элементным линейно-независимым комбинациям

Под кодом максимальной длины понимают разновидность эквидистантного циклического кода, кодовые комбинации которого представляют собой последовательности максимальной длины, так называемые М-последовательности [4, 5].

М-последовательность – 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 либо аппаратная схема, либо программный алгоритм [1].

Аппаратная схема реализуется на основе регистра сдвига с линейной обратной связью, который строится, исходя из вида порождающего полинома поля Галуа $p(x)$. Следовательно, полином $p(x)$ также можно считать порождающим полиномом как М-последовательности, так и соответствующего ей кода максимальной длины [1].

В программном алгоритме М-последовательность рассматривается как рекуррентная последовательность $\{\boldsymbol{s}\}$, выраженная через функцию-след $T(x)$ элемента поля Галуа по формуле (1) [1]:

$$\{\boldsymbol{s}\} = [s_0; s_1; \dots; s_{2^m-2}] = \left[T(\varepsilon^z); T(\varepsilon^{z+1}); \dots; T\left(\varepsilon^{z+2^m-2}\right)\right] = \\ = \left[T(c); T(c\varepsilon); \dots; T\left(c\varepsilon^{2^m-2}\right)\right] = \left\{T\left(c\varepsilon^i\right)\right\}_{i=0}^{2^m-2}, \quad (1)$$

где $c = \varepsilon^z$ – начальная фаза М-последовательности, которая является элементом поля Галуа GF(2^m).

Функция-след $T(x)$ для элемента ε^i поля GF(2^m) рассчитывается по формуле (2) [1].

$$T\left(\varepsilon^i\right) = \varepsilon^i + \left(\varepsilon^i\right)^2 + \left(\varepsilon^i\right)^{2^2} + \dots + \left(\varepsilon^i\right)^{2^{m-1}} = \sum_{j=0}^{m-1}\left(\varepsilon^i\right)^{2^j}. \quad (2)$$

Совокупность М-последовательностей $\{s\}$, 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 $d_{\min} = 2^{k-1}$ [3].

Для примера рассмотрим М-последовательность с периодом $2^4 - 1 = 15$, построенную над полем GF(2^4). Она представляет собой двоичный эквидистантный код максимальной длины (15, 4) с $d_{\min} = 8$. Этот код гарантированно исправляет $t \leq 3$ ошибок [3].

Поскольку М-последовательность $\{\boldsymbol{s}\}$ полностью определяется начальной фазой $c = \varepsilon^z$, то при заданном заранее характеристическом многочлене, задача декодирования М-последовательности сводится к определению начальной фазы c [1–3].

Эта задача достаточно просто решается декодированием по k-элементным участкам без ошибок на основе двойственного базиса [1]. Для решения поставленной задачи выберем k распределенных линейно-

независимых элементов последовательности $\{\boldsymbol{s}\}$, а именно $s_{i_1}, s_{i_2}, \dots, s_{i_k}$, из которых составим систему уравнений (3) [1, 2].

$$\begin{cases} s_{i_1} = T\left(\varepsilon^{z+i_1}\right) = T\left(c\varepsilon^{i_1}\right); \\ s_{i_2} = T\left(\varepsilon^{z+i_2}\right) = T\left(c\varepsilon^{i_2}\right); \\ \vdots \\ s_{i_k} = T\left(\varepsilon^{z+i_k}\right) = T\left(c\varepsilon^{i_k}\right). \end{cases} \tag{3}$$

Решим эту систему уравнений относительно элемента $c = \varepsilon^z$, определяющего начальную фазу последовательности $\{\boldsymbol{s}\}$. Известными величинами в системе уравнений (3) являются значения индексов i_1, i_2, ..., i_k относительно начальной фазы и значения самих линейно-независимых элементов $s_{i_1}, s_{i_2}, \dots, s_{i_k} \in \mathrm{GF}(2)$ последовательности $\{\boldsymbol{s}\}$ [1, 2].

Искомый элемент $c = \varepsilon^z$ поля $\mathrm{GF}(2^m)$ выразим через левый степенной базис поля в векторной форме (4), учитывая, что $m = k$:

$$\varepsilon^z = a_0 + a_1\varepsilon + \cdots + a_{k-1}\varepsilon^{k-1} = [a_0 a_1 \dots a_{k-1}] = [\boldsymbol{a}], \tag{4}$$

где $a_i \in \mathrm{GF}(2)$.

Исходя из формулы (4), элемент ε^{z+i_1} можно представить в виде формулы (5):

$$\varepsilon^{z+i_1} = \varepsilon^z \varepsilon^{i_1} = [\boldsymbol{a}]\boldsymbol{F}^{i_1}, \tag{5}$$

где $\boldsymbol{F}^{i_1}$ – сопровождающая матрица элемента поля ε^{i_1}, вид которой определяется характеристическим многочленом $p(x)$, соответствующим рекуррентному соотношению последовательности $\{s\}$ [1].

Подставим формулу (5) в формулу (2) вычисления функции-след элемента ε^{z+i_1}, заменим возведение в степень 2^j на умножение на соответствующую ему матрицу $\boldsymbol{X}_{2^j}$ и вынесем за скобки общий множитель [1, 2].

$$T\left(\varepsilon^{z+i_1}\right) = [\boldsymbol{a}]\boldsymbol{F}^{i_1}(\boldsymbol{E} + \boldsymbol{X}_2 + \boldsymbol{X}_4 + \cdots + \boldsymbol{X}_{2^{m-1}}) = [\boldsymbol{a}]\boldsymbol{F}^{i_1}\boldsymbol{\theta}, \tag{6}$$

где матрица $\boldsymbol{\theta} = \boldsymbol{E} + \boldsymbol{X}_2 + \boldsymbol{X}_4 + \cdots + \boldsymbol{X}_{2^{m-1}}$.

Подставив формулу (6) в систему уравнений (3), получим

$$\begin{cases} s_{i_1} = [\boldsymbol{a}]\boldsymbol{F}^{i_1}\boldsymbol{\theta} = f_1([\boldsymbol{a}]); \\ s_{i_2} = [\boldsymbol{a}]\boldsymbol{F}^{i_2}\boldsymbol{\theta} = f_2([\boldsymbol{a}]); \\ \vdots \\ s_{i_k} = [\boldsymbol{a}]\boldsymbol{F}^{i_k}\boldsymbol{\theta} = f_k([\boldsymbol{a}]). \end{cases} \tag{7}$$

Учитывая, что s_{i_1} принадлежит простому полю GF(2), в результате перемножения $[\boldsymbol{a}]\boldsymbol{F}^{i_1}\boldsymbol{\theta}$ будет получена вектор-строка, в которой младший разряд s_{i_1} является элементом поля, выраженным через коэффициенты $[a_0, a_1, \dots, a_{k-1}]$. Остальные разряды полученного вектора нулевые. Поэтому из матрицы $\boldsymbol{\theta}$ оставляем только младший вектор-столбец $\boldsymbol{\theta}_0$. Следовательно, строки системы уравнений (7) можно записать в виде формулы (8) [1, 2].

$$s_j = [\boldsymbol{a}]\boldsymbol{F}^j\boldsymbol{\theta}_0 = f_j([\boldsymbol{a}]), \tag{8}$$

где j принимает значения $i_1, i_2, \dots, i_k$.

Полученную линейно-независимую систему уравнений (8) окончательно решаем относительно коэффициентов $[a_0, a_1, \dots, a_{k-1}]$, что дает векторное представление элемента $c = \varepsilon^z$, определяющего начальную фазу последовательности $\{\boldsymbol{s}\}$.

Для этого запишем систему уравнений (8) в матричном виде.

$$\boldsymbol{S} = \boldsymbol{\Theta}\boldsymbol{A}, \tag{9}$$

где

$$\boldsymbol{S} = \begin{bmatrix} s_{i_1} \\ s_{i_2} \\ \vdots \\ s_{i_k} \end{bmatrix};\ \boldsymbol{\Theta} = \boldsymbol{F}^j\boldsymbol{\theta}_0 = \begin{bmatrix} \left(\boldsymbol{F}^{i_1}\boldsymbol{\theta}_0\right)^T \\ \left(\boldsymbol{F}^{i_2}\boldsymbol{\theta}_0\right)^T \\ \vdots \\ \left(\boldsymbol{F}^{i_k}\boldsymbol{\theta}_0\right)^T \end{bmatrix};\ \boldsymbol{A} = \begin{bmatrix} a_0 \\ a_1 \\ \vdots \\ a_{k-1} \end{bmatrix}.$$

Для решения системы уравнений (9) используем формулу (10) [1, 2].

$$\boldsymbol{A} = \boldsymbol{\Theta}^{-1}\boldsymbol{S}, \tag{10}$$

где $\boldsymbol{\Theta}^{-1}$ – обратная матрица для матрицы $\boldsymbol{\Theta}$.

Применяя мажоритарную обработку М-последовательности по всем k-элементным линейно-независимым комбинациям определяем начальную фазу c [1, 2].

Этот алгоритм применим как для систематического, так и для несистематического кода максимальной длины. Отличие состоит в том, что в случае несистематического кода информационные элементы получаются сразу при решении системы уравнений (9) по формуле (10), так как они соответствуют начальной фазе М-последовательности, а в случае систематического кода их необходимо вычислить по полученной начальной фазе [3].

Для определения k-элементных линейно-независимых комбинаций проверяем каждую k-элементную комбинацию $s_{i_1}, s_{i_2}, \dots, s_{i_k}$ на линейную независимость. Для этого необходимо построить соответствующую этой k-элементной комбинации матрицу $\boldsymbol{\Theta}$ и определить, является ли она линей-

но-независимой, найдя соответствующий ей определитель $\boldsymbol{\Delta = |\Theta|}$. Для линейно-независимой матрицы, определитель $\boldsymbol{\Delta}$ будет не равен нулю [1]. Кодовая комбинация рассматриваемого в качестве примера кода максимальной длины $(15, 4)$ содержит 840 k-элементных линейно-независимых комбинаций [2].

При проведении процедуры декодирования линейно-независимые комбинации и соответствующие им обратные матрицы необходимо вычислить заранее и хранить в базе в виде так называемых «масок», откуда их будет считывать декодер. Для примера рассмотрим одну из «масок» для взятого в качестве примера кода (15, 4): 100110001000000. Длина маски равна длине кодовой комбинации (М-последовательности), а единицами отмечены позиции линейно-независимых элементов. Наложив «маску» на принятую кодовую комбинацию, декодер сразу получает линейно-независимые элементы [2, 3].

Такой принцип работы позволяет распараллелить алгоритм декодирования на число ветвей, соответствующих количеству «масок». При этом процедура декодирования начинается сразу по получении первых k элементов кодовой комбинации и заканчивается непосредственно с получением последнего элемента. При малом числе ошибок процедура декодирования завершается до получения всей кодовой комбинации, как только будет накоплено количество результатов, достаточное для принятия однозначного верного решения по мажоритарному принципу.

На рис. 1 показана блок-схема исследуемого алгоритма декодирования. Из блок-схемы видно, что в алгоритме есть три точки завершения. Во-первых, как было сказано ранее, результат может быть получен до получения последнего элемента кодовой комбинации, когда декодер определяет достоверный результат по мажоритарному принципу (вес результата становится больше, чем половина количества масок). Неправильное декодирование может произойти лишь в том случае, когда возникает набор ошибок большого веса, который преобразует передаваемую кодовую комбинацию в другую разрешенную кодовую комбинацию, что крайне маловероятно, учитывая большое минимальное кодовое расстояние кодов максимальной длины. Во-вторых, результат может быть получен по завершении цикла декодирования. В этом случае при определении по мажоритарному принципу возможны два основных варианта. В том случае, если среди результатов есть два с одинаковым весом, декодер не может принять решение о верном результате и возвращает сигнал о неисправляемой ошибке (отказ от декодирования). По получении такого сигнала, приемник может отправить сигнал перезапроса по каналу обратной связи, если это предусмотрено алгоритмом передачи. Если же есть результат, вес которого максимален, то декодер считает его верным и передает получателю [2].

Исходя из структуры алгоритма декодирования и принципа мажоритарности, можно предположить, что использование данного алгоритма де-

кодирования позволяет применить механизмы адаптации к каналу. Все *k*-элементные линейно-независимые комбинации, по которым производится декодирование, равномерно распределены по всей длине кодового слова кода максимальной длины. Следовательно, если рассмотреть канал с равномерным распределением ошибок, то можно предположить, что использовать *k*-элементные комбинации, включающие близко расположенные элементы, не имеет смысла, поскольку они с большей вероятностью будут накладываться на одни и те же ошибочные элементы. В этом случае целесообразно использовать *k*-элементные линейно-независимые комбинации, распределенные по длине кодового слова. В случае канала с группированием ошибок необходимо наоборот использовать сгруппированные *k*-элементные комбинации. Это позволит сократить общее число используемых «масок» и, следовательно, приведет к уменьшению времени декодирования при последовательной обработке «масок» и к уменьшению сложности декодера при их параллельной обработке [3].

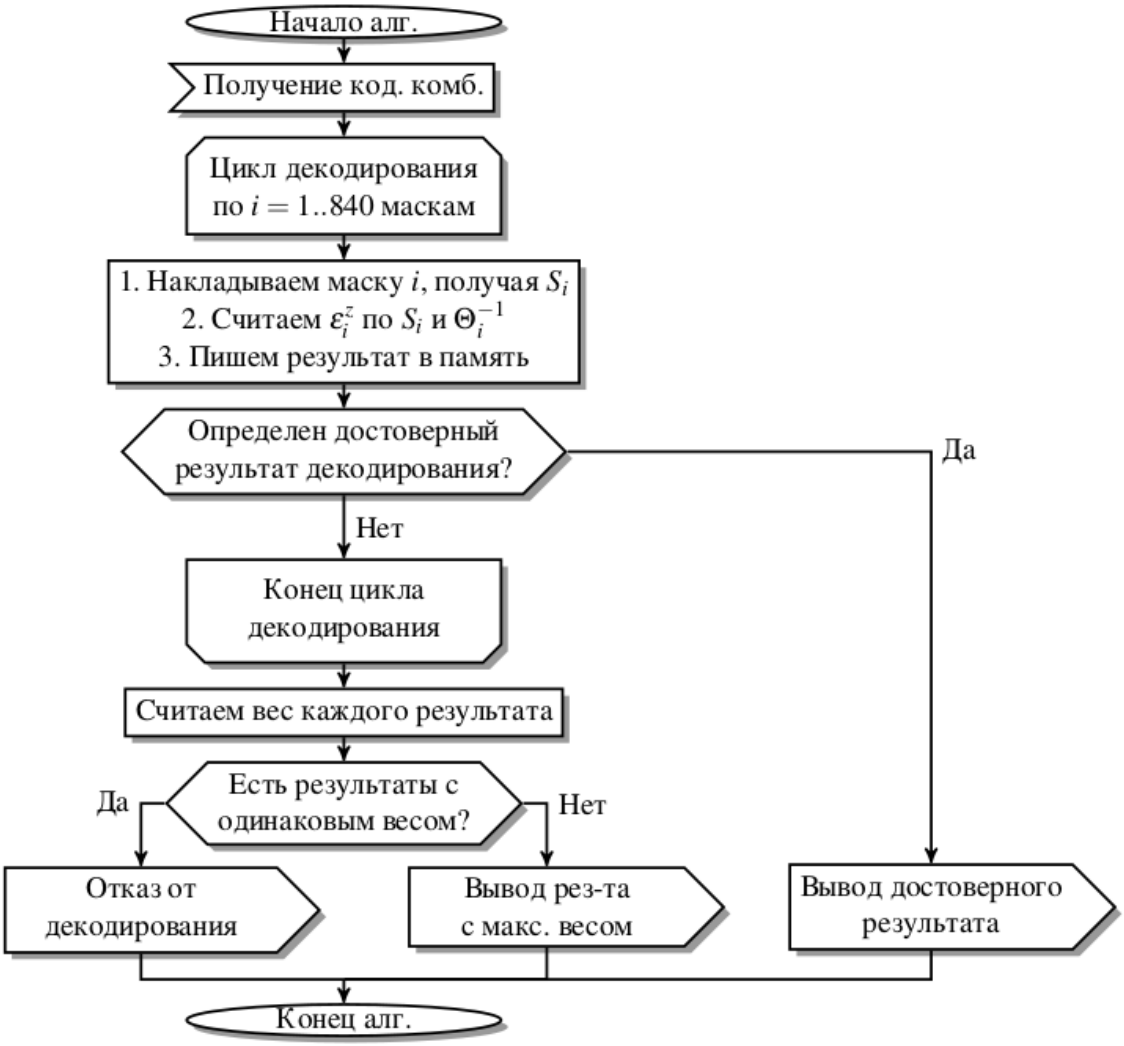


Рис. 1. Алгоритм мажоритарного декодирования кодовой комбинации кода максимальной длины по *k*-элементным линейно независимым комбинациям

Программная модель оценки эффективности алгоритма мажоритарного декодирования кода максимальной длины по *k*-элементным линейно-независимым комбинациям

Для исследования алгоритма была написана программная модель на языке Pascal с использованием компилятора Free Pascal и среды программирования Lazarus. Блок-схема программной модели представлена на рис. 2.

Рис. 2. Блок-схема программной модели оценки эффективности алгоритма мажоритарного декодирования кода максимальной длины по *k*-элементным линейно-независимым комбинациям

Модель состоит из источника информационных сообщений, реализованного по принципу генератора случайных комбинаций; кодера кода максимальной длины, основанного на использовании формул (1) и (2); модели цифрового двоичного симметричного канала с независимым распределением ошибок; декодера кода максимальной длины, реализующего алгоритм декодирования, представленный на рис. 1; блока обработки результатов декодирования, сравнивающего информационную комбинацию, полученную от источника сообщений, и комбинацию на выходе декодера.

При проведении исследований используется статистическое моделирование по методу Монте-Карло. Через модель канала последовательно передаются N кодовых слов кода максимальной длины, которые декодируются на приёмной стороне. Результат декодирования сравнивается с информационной комбинацией, полученной от источника сообщений. По результатам сравнения, как следует из описания алгоритма декодирования, приведенного выше, блок обработки результатов может принять одно из трех возможных решений: принятая кодовая комбинация декодирована верно (правильное декодирование), кодовая комбинация декодирована неверно (неправильное декодирование) и обнаружена неисправляемая ошибка (отказ от декодирования). По собранной при моделировании статистике оцениваются вероятностные характеристики алгоритма декодирования, которые включают в себя вероятность правильного декодирования кодового слова, вероятность неправильного декодирования и вероятность отказа от декодирования. Эти вероятностные характеристики позволяют оценить эффективность декодирования и сравнить исследуемый алгоритм с другими алгоритмами декодирования кодов максимальной длины. Оценочные значения вероятностных характеристик алгоритма, так называемые частости, рассчитываются по формулам (11) [6].

$$P_{\text{ПД}} = \frac{N_{\text{ПД}}}{N}, \quad P_{\text{НД}} = \frac{N_{\text{НД}}}{N}, \quad P_{\text{ОД}} = \frac{N_{\text{ОД}}}{N}, \tag{11}$$

где $P_{\text{ПД}}$, $P_{\text{НД}}$, $P_{\text{ОД}}$ – оценочные значения (частости) вероятностей правильного декодирования, неправильного декодирования и отказа в декодировании; $N_{\text{ПД}}$, $N_{\text{НД}}$, $N_{\text{ОД}}$ – количество правильно декодированных комбинаций, неправильно декодированных комбинаций и комбинаций, вызвавших отказ в декодировании.

В предыдущих работах было показано, что для получения оценочных значений вероятности, имеющих наименьшее среднеквадратичное отклонение от математического ожидания, достаточно передать через модель канала $N = 10^5$ кодовых комбинаций [6, 7]. Для малых вероятностей битовой ошибки в двоичном симметричном канале используем $N = 10^6$ кодовых комбинаций, что позволит обеспечить более высокую точность при малом количестве комбинаций с ошибкой.

Помимо вероятностей правильного декодирования, неправильного декодирования и отказа в декодировании для оценки эффективности алгоритма декодирования используется эквивалентная вероятность ошибки $P_{\text{ЭКВ}}$, т. е. вероятность ошибки в постоянном симметричном двоичном канале без памяти, в котором система с примитивным кодированием (кодированием без избыточности) оказывается эквивалентной рассматриваемой системе. Эквивалентная вероятность ошибки удобна тем, что позволяет сравнивать между собой не только различные алгоритмы декодирования, но и различные коды [8–10].

Для алгоритмов, обеспечивающих обнаружение неисправляемой ошибки, эквивалентную вероятность ошибки можно оценить по формуле (12) [10].

$$P_{\text{ЭКВ}} = 1 - \left(1 - \frac{P_{\text{НД}}}{1 - P_{\text{ОД}}}\right)^{\frac{1}{i}}, \tag{12}$$

где i – количество двоичных единиц информации, содержащихся в кодовой комбинации.

Результаты оценки эффективности алгоритма мажоритарного декодирования кода максимальной длины по *k*-элементным линейно-независимым комбинациям в двоичном симметричном канале

На рис. 3 приведены графики зависимости оценочных значений (частостей) вероятности правильного декодирования $P_{\text{ПД}}$, вероятности неправильного декодирования $P_{\text{НД}}$, вероятности отказа в декодировании $P_{\text{ОД}}$ и эквивалентной вероятности ошибки $P_{\text{ЭКВ}}$ в зависимости от вероятности битовой ошибки p_0 в двоичном симметричном канале для кода (15, 4).

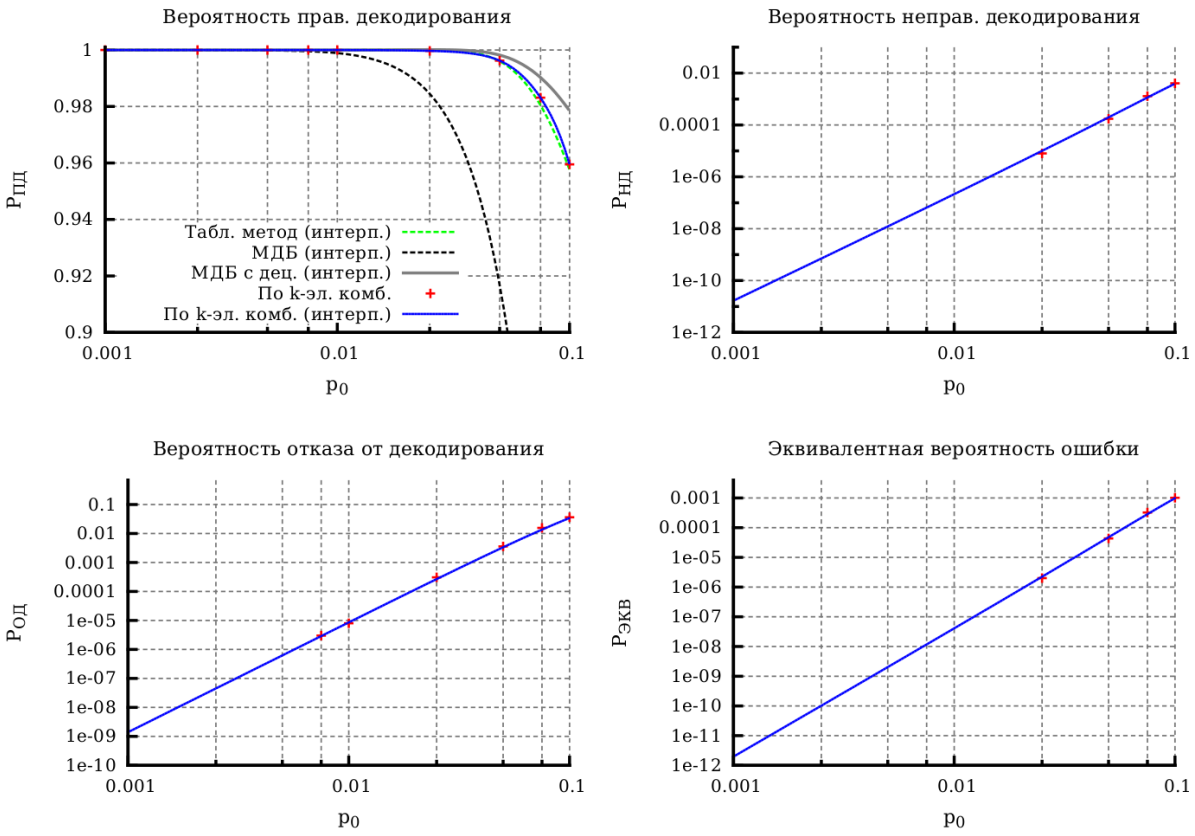


Рис. 3. Зависимость оценочных значений характеристик
от вероятности битовой ошибки в двоичном симметричном канале для кода (15, 4)

Графики интерполированы для получения общей картины во всем рассматриваемом диапазоне вероятностей битовой ошибки в двоичном симметричном канале, потому что для вероятностей битовой ошибки в канале, меньшей 0,025, неправильно декодированных ошибочных кодовых комбинаций выявлено не было.

Был выполнен сравнительный анализ с другими алгоритмами декодирования кодов максимальной длины по вероятности правильного декодирования.

Исходя из проведенного анализа, можно утверждать, что рассмотренный алгоритм декодирования по параметру исправляющей способности незначительно превосходит табличный метод декодирования эквидистантных кодов максимальной длины [3, 11] и полностью соответствует корреляционному методу [3, 11], график которого полностью совпадает с графиком рассмотренного алгоритма.

Сравнение с современным методом декодирования на основе двойственного базиса (МДБ) поля Галуа [1, 3, 11] показало, что исследованный алгоритм декодирования по *k*-элементным линейно-независимым комбинациям имеет значительно большую исправляющую способность, нежели простой метод МДБ, но при этом незначительно уступает по тому же параметру методу МДБ с использованием децимаций [1], что обуславливает-

ся собственно процедурой децимирования, позволяющей сгруппировать случайные ошибки, возникающие в двоичном симметричном канале [1]. При этом необходимо отметить, что введение дополнительной операции децимирования на приеме замедляет процедуру декодирования и тем самым вносит дополнительную задержку в передачу информации потребителю, тогда как алгоритм декодирования по k-элементным линейно-независимым комбинациям, как было показано ранее, позволяет завершить декодирование практически одновременно с приемом последнего бита кодовой комбинации.

Библиографический список

1. **Когновицкий О. С.** Двойственный базис и его применение в телекоммуникациях / О. С. Когновицкий. – СПб. : Линк, 2009. – 423 с.

2. **Владимиров С. С.** Моделирование процессов мажоритарного декодирования комбинации эквидистантного кода по К линейно-независимым элементам / С. С. Владимиров // Научно-технические ведомости Санкт-Петербургского государственного политехнического университета. Информатика. Телекоммуникации. Управление. – 2010. – Т. 3. № 101. – С. 149–156.

3. **Владимиров С. С.** Исследование алгоритма мажоритарного декодирования комбинации эквидистантного кода по k линейно-независимым элементам / С. С. Владимиров // IV Международная научно-техническая и научно-методическая конференция «Актуальные проблемы инфотелекоммуникаций в науке и образовании»: сборник научных статей в 2 томах. – СПб. : Санкт-Петербургский государственный университет телекоммуникаций им. проф. М.А. Бонч-Бруевича, 2015. – С. 281–285.

4. **Mahafza Bassem R.** Radar Systems Analysis and Design Using MATLAB / Bassem R. Mahafza. – Third Edition. – CRC Press, 2013. – 772 p.

5. Кларк Д. К. Кодирование и исправление ошибок в системах цифровой связи. Статистическая теория связи / Д. К. Кларк, Д. Б. Кейн. – М. : Радио и Связь, 1987. – 392 с.

6. **Владимиров С. С.** Исследование алгоритма мажоритарного декодирования кода Рида-Соломона на основе двойственного базиса в канале с памятью / С. С. Владимиров // Информационные технологии и телекоммуникации. – 2015. – № 1 (9). – С. 19–26.

7. **Владимиров С. С.** Анализ эффективности декодирования циклических кодов Рида-Соломона с использованием двойственного базиса : дис. … канд. техн. наук / Сергей Сергеевич Владимиров ; Санкт-Петербургский государственный университет телекоммуникаций им. проф. М. А. Бонч-Бруевича. – Санкт-Петербург, 2013. – 159 с.

8. **Финк Л. М.** Теория передачи дискретных сообщений / Л. М. Финк. – М. : «Сов. радио», 1970. – 728 с.

9. **Деев В. В.** Методы модуляции и кодирования в современных системах связи / В. В. Деев. – СПб. : Наука, 2007. – 267 с.

10. **Теория** передачи сигналов : учебник для вузов / А. Г. Зюко, Д. Д. Кловский, М. В. Назаров, Л. М. Финк. – М. : Связь, 1980. – 288 с.

11. **Кукунин Д. С.** Анализ эффективности декодирования циклических кодов с использованием двойственного базиса : дис. … канд. техн. наук / Д. С. Кукунин ; Санкт-Петербургский государственный университет телекоммуникаций им. проф. М.А. Бонч-Бруевича. – Санкт-Петербург, 2009. – 197 с.

References

1. **Kognovitsky O. S.** Dvoystvenniy bazis i ego primenenie v telecommunikatziyah [Dual Basis and its Appliance in Telecommunication] / O. S. Kognovitsky. – St.-Petersburg. Link, 2009. – 423 s.

2. **Vladimirov S. S.** Modelirovanie protzessov mazhoritarnogo dekodirovaniya po k lineyno-nezavisimym kombinatziyam / S. S. Vladimirov // Nauchno-tehnicheskie vedomosti Sankt-Peterburgskogo gosudarstvennogo politehnicheskogo universiteta. Informatika. Telekommunikatzii. Upravlenie. – 2008. – Vol. 5. no. 65. – PP. 86–92.

3. **Vladimirov S. S.** Analysis of Major Decoding Algorithm of Equidistant Code Combination with K Linear-Independent Elements / S. S. Vladimirov // VI Mezhdunarodnaya nauchno-tehnicheskaya i nauchno-metodicheskaya konferenciya «Actual'nye problemy infotelekommunikatziy v nauke i obrazovanii»: sb. nauchnyh statey v dvuh tomah. St.-Petersburg. St.Petersburg State University of Telecommunications. – 2015. – PP. 281–285.

4. **Mahafza Bassem R.** Radar Systems Analysis and Design Using MATLAB / Bassem R. Mahafza. – Third Edition. – CRC Press, 2013. – 772 p.

5. **Clark, George C. Jr.** Error-Correction Coding for Digital Communications / George C. Jr. Clark, and J. Bibb Cain. – New York: Plenum Press, 1981.

6. **Vladimirov S. S.** The research of dual basis based majority-logic decoding algorithm of Reed-Colomon codes in memory channel / S. S. Vladimirov // IT&Telecom. – 2015. – N 1 (9). – PP. 19–26.

7. **Vladimirov S. S.** Analiz effektivnosti dekodirovaniya tziklicheskih kodov Rida-Solomona s ispol'zovaniem dvoystvennogo bazisa. Cand.Sc. Thesis. St.Petersburg State University of Telecommunications. – St.-Petersburg. 2013.

8. **Fink L. M.** Teoriya peredachi diskretnyh soobscheniy [Digital Data Transmisison Theory] / L. M. Fink. – Moscow: Sovetskoe radio. 1970.

9. **Deev V. V.** Metody modulyatzii i kodirovaniya v sovremennyh sistemah svyazi [Modulation and Coding in Modern Communication Systems] / V. V. Deev. – St.-Petersburg. Nauka, 2007.

10. **Teoriya** peredachi signalov [Signal Transmission Theory] / A. G. Zyuko, D. D. Klovskiy, M. V. Nazarov, L. M. Fink – Moscow. Svyaz. 1980.

11. **Kukunin D. S.** Analiz effektivnosti dekodirovaniya tziklicheskih kodov s ispol'zovaniem dvoystvennogo bazisa. Cand.Sc. Thesis / D. S. Kukunin; St.Petersburg State University of Telecommunications. – St.-Petersburg. 2009.

Владимиров Сергей Сергеевич – кандидат технических наук, доцент кафедры «Сети связи и передача данных» Федерального государственного бюджетного образовательного учреждения высшего образования «Санкт-Петербургский государственный университет телекоммуникаций им. проф. М. А. Бонч-Бруевича»,
vladimirov.opds@gmail.com