



Том 8. № 4
2022

ISSN: 1813-324X (print)

ISSN: 2712-8830 (online)

ТРУДЫ УЧЕБНЫХ ЗАВЕДЕНИЙ СВЯЗИ

Темы номера:

- ✓ Оптимизация конструкции многосердцевинного волокна
- ✓ Использование низкоплотностных кодов в канале Гилберта
- ✓ Применение виртуальных магнитных диполей в антенной решетке

Vol. 8. Iss. 4
2022

PROCEEDINGS
OF TELECOMMUNICATION UNIVERSITIES

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

Научный журнал

**ТРУДЫ
УЧЕБНЫХ ЗАВЕДЕНИЙ СВЯЗИ**

Том 8. № 4

Proceedings of Telecommunication Universities

Vol. 8. Iss. 4

Санкт-Петербург

2022

Описание журнала

Научный журнал. Включен в Перечень рецензируемых научных изданий, в которых должны быть опубликованы основные научные результаты диссертаций на соискание ученой степени кандидата наук, на соискание ученой степени доктора наук (распоряжение Минобрнауки России № 21-р от 12.02.2019), по специальностям (распоряжение № 33-р от 01.02.2022):

1.2.2. Математическое моделирование, численные методы и комплексы программ

2.2.6. Оптические и оптико-электронные приборы и комплексы

2.2.13. Радиотехника, в том числе системы и устройства телевидения

2.2.14. Антенны, СВЧ-устройства и их технологии

2.2.15. Системы, сети и устройства телекоммуникаций

2.2.16. Радиолокация и радионавигация

2.3.1. Системный анализ, управление и обработка информации

2.3.6. Методы и системы защиты информации, информационная безопасность

Выпускается с 1960 года. Выходит 4 раза в год (ежеквартально). Издается на русском и английском языках.

Редакционный совет

Дукельский К.В. к.т.н., доцент, АО «Государственный оптический институт имени С.И. Вавилова» (ГОИ),
Главный редактор г. Санкт-Петербург, Россия

Буйневич М.В. д.т.н., проф., Санкт-Петербургский государственный университет телекоммуникаций
Зам. Главного редактора им. проф. М.А. Бонч-Бруевича (СПбГУТ), г. Санкт-Петербург, Россия

Розанов Н.Н. д.ф.-м.н., проф., чл.-корр. РАН, АО «Государственный оптический институт
имени С.И. Вавилова» (ГОИ), г. Санкт-Петербург, Россия

Кучерявый Е. PhD, Технологический университет Тампере, г. Тампере, Финляндия

Гошек И. PhD, Технологический университет Брно, г. Брно, Чешская республика

Тиамийу О.А. PhD, Университет Илорина, г. Илорин, Нигерия

Козин И.Д. д.ф.-м.н., проф., Алматинский университет энергетики и связи, г. Алма-Аты, Казахстан

Самуйлов К.Е. д.т.н., проф., Российский университет дружбы народов (РУДН), г. Москва, Россия

Степанов С.Н. д.т.н., проф., Московский технический университет связи и информатики (МТУСИ),
г. Москва, Россия

Росляков А.В. д.т.н., проф., Поволжский государственный университет телекоммуникаций
и информатики (ПГУТИ), г. Самара, Россия

Кучерявый А.Е. д.т.н., проф., Санкт-Петербургский государственный университет телекоммуникаций
им. проф. М.А. Бонч-Бруевича (СПбГУТ), г. Санкт-Петербург, Россия

Канаев А.К. д.т.н., проф., Петербургский университет путей сообщения имени Александра I (ПГУПС),
г. Санкт-Петербург, Россия

Новиков С.Н. д.т.н., проф., Сибирский государственный университет телекоммуникаций и информатики
(СибГУТИ), г. Новосибирск, Россия

Дворников С.В. д.т.н., проф., Военная академия связи им. Маршала Советского Союза С.М. Буденного (ВАС),
г. Санкт-Петербург, Россия

Коржик В.И. д.т.н., проф., Санкт-Петербургский государственный университет телекоммуникаций
им. проф. М.А. Бонч-Бруевича (СПбГУТ), г. Санкт-Петербург, Россия

Ковалгин Ю.А. д.т.н., проф., Санкт-Петербургский государственный университет телекоммуникаций
им. проф. М.А. Бонч-Бруевича (СПбГУТ), г. Санкт-Петербург, Россия

Владыко А.Г. к.т.н., Санкт-Петербургский государственный университет телекоммуникаций
им. проф. М.А. Бонч-Бруевича (СПбГУТ), г. Санкт-Петербург, Россия

Регистрационная информация

Журнал зарегистрирован Федеральной службой по надзору в сфере связи, информационных технологий и массовых коммуникаций: ПИ № 77-77501 от 17.01.2020 г. (пред. рег. № 77-17986 от 07.04.2004 г.)

Подписной индекс в объединенном каталоге «ПРЕССА РОССИИ»: 59983

Размещение в РИНЦ (elibrary.ru) по договору: № 59-02/2013R от 20.02.2013

Контактная информация

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

Адрес учредителя: 191186, Санкт-Петербург, набережная реки Мойки, д. 61, литера А

Адрес редакции: 193232, Санкт-Петербург, пр. Большевиков, 22/1, к. 334/2
Тел.: +7 (812) 326-31-63, м. т. 2022, +79643759970
E-mail: tuzs@spbgt.ru
Web: <http://tuzs.sut.ru>
ВК: <http://vk.com/spbtuzs>

Description

Scientific journal. The journal is included in the List of reviewed scientific publications, in which the main scientific results of dissertations for the degree of candidate of science and for the degree of doctor of science should be published (order of the Ministry of Education and Science of Russia No 21-r of 12 February 2019) in the field of (order of the Ministry of Education and Science of Russia No 33-r of 01 February 2022):

1.2.2. Mathematical modeling, numerical methods and complexes of programs

2.2.6. Optical and optoelectronic devices and complexes

2.2.13. Radio engineering, including television systems and devices

2.2.14. Antennas, microwave devices and its technologies

2.2.15. Systems, networks and telecommunication devices

2.2.16. Radiolocation and radio navigation

2.3.1. System analysis, management and information processing

2.3.6. Methods and systems of information security, cybersecurity

Since 1960. Published 4 times per year. Published in Russian and English.

Editorial Board

K.V. Dukel'skii <i>Editor-in-chief</i>	PhD, associate prof., executive Director of Open Joint Stock Company «S.I. Vavilov State Optical Institute» (SOI), Saint-Petersburg, Russia
M.V. Buinevich <i>Deputy editor-in-chief</i>	DSc, prof., The Bonch-Bruевич Saint-Petersburg State University of Telecommunications (SPbSUT), Saint-Petersburg, Russia
N.N. Rozanov	DSc, prof., member-corr. RAS, Open Joint Stock Company «S.I. Vavilov State Optical Institute» (SOI), Saint-Petersburg, Russia
Y. Koucheryav	PhD, Tampere University of Technology, Tampere, Finland
I. Hošek	PhD, Brno University of Technology, Brno, Czech Republic
O.A. Tiamiyu	PhD, University of Ilorin, Ilorin, Nigeria
I.D. Kozin	DSc, prof., Almaty University of Power Engineering and Telecommunications, Almaty, Kazakhstan
K.E. Samuilov	DSc, prof., Peoples' Friendship University (RUDN), Moscow, Russia
S.N. Stepanov	DSc, prof., Moscow Technical University of Communication and Informatics (MTUCI), Moscow, Russia
A.V. Roslyakov	DSc, prof., Povolzhskiy State University of Telecommunications and Informatics (PSUTI), Samara, Russia
A.E. Koucheryav	DSc, prof., The Bonch-Bruевич Saint-Petersburg State University of Telecommunication (SPbSUT), Saint-Petersburg, Russia
A.K. Kanaev	DSc, prof., Emperor Alexander I-st Petersburg State Transport University (PSTU), Saint-Petersburg, Russia
S.N. Novikov	DSc, prof., Siberian State University of Telecommunications and Information Sciences (SibSUTIS), Novosibirsk, Russia
S.V. Dvornikov	DSc, prof., Military Academy of Telecommunications named after Marshal Union S.M. Budyonny, Saint-Petersburg, Russia
V.I. Korzhik	DSc, prof., The Bonch-Bruевич Saint-Petersburg State University of Telecommunication (SPbSUT), Saint-Petersburg, Russia
Yu.A. Kovalgin	DSc, prof., The Bonch-Bruевич Saint-Petersburg State University of Telecommunication (SPbSUT), Saint-Petersburg, Russia
A.G. Vlado	PhD, The Bonch-Bruевич Saint-Petersburg State University of Telecommunication (SPbSUT), Saint-Petersburg, Russia

Registration Information

Registered by Federal Service for Supervision of Communications, Information Technology and Mass Media on 17.01.2020: PI No. 77-77501 (prev. reg. on 04.07.2004: No. 77-17986)

Subscription index for joint catalog «PRESSA ROSSII»: 59983

Accommodation in RINC (elibrary.ru) by agreement on 20.02.2013: No. 59-02/2013R

Contact Information

Publisher:	Federal State Budget-Financed Educational Institution of Higher Education «The Bonch-Bruевич Saint-Petersburg State University of Telecommunications» (SPbSUT)	Post address:	193232, Saint Petersburg, Prospekt Bolshevikov, 22/1
		Phone:	+7 (812) 326-31-63, local 2022, +79643759970
		E-mail:	tuzs@spbgt.ru
		Web:	http://tuzs.sut.ru
Publisher address:	191186, Saint Petersburg, Moika river embankment, 61-A		

НАЧАЛА ДЕКАНАУК И ТЕХНОЛОГИЙ СПБГУТ

Указом Президента РФ В.В. Путина 2022-2031 годы объявлены в России десятилетием науки и технологий. Такое решение продиктовано позицией усилить роль науки в решении важнейших задач развития общества и страны, а также учитывая результаты 2021 года, объявленного в России Годом науки.

Целями десятилетия, согласно Указу, названы активное привлечение молодежи в науку, всемерное вовлечение исследователей и разработчиков в решение важных для страны задач, а также повышение доступности информации о достижениях российской науки для граждан России. И Указ стал активно претворяться в жизнь. Минобрнауки России инициирует различные инструменты вовлечения исследователей и разработчиков в решение важнейших задач развития общества и государства. Такой подход уже доказал свою эффективность, обеспечив нашей стране значимое место в рейтинге ведущих стран по научно-технологическому развитию. Если по этому показателю наша страна занимает сегодня 9 место, то к концу десятилетия, согласно программе «Научно-технологического развития Российской Федерации», должны занять 7 место.

Санкт-Петербургский государственный университет телекоммуникаций им. проф. М.А. Бонч-Бруевича [1], как ведущий разработчик передовых цифровых технологий, является активным участником и исполнителем научных работ в национальных и федеральных проектах. Поэтому в планах проректора по научной работе с 2022 г. включены насыщенные и долгосрочные мероприятия СПбГУТ в свете Указа Президента РФ по популяризации науки, развитию научно-образовательной инфраструктуры, формированию продуктивной среды для молодых исследователей и научных школ, социальной поддержке отдельных категорий студентов и молодых ученых, повышению наукометрических показателей за счет вклада публикаций университетской науки.



Научно-исследовательская работа СПбГУТ организована в рамках реализации мероприятий (работ) по национальным проектам «Цифровая экономика Российской Федерации», «Наука и университеты», федеральным проектам «Кадры для цифровой экономики», «Информационная безопасность», «Цифровые технологии», «Развитие человеческого капитала в интересах регионов, отраслей и сектора исследований и разработок» и ряду других.

Исследовательскими коллективами университета в 2022 г. успешно выполнены установленные календарными планами этапы научно-исследовательских работ по национальной программе «Цифровая экономика Российской Федерации» [2] по заказам Минцифры России:

- разработка методов, моделей и средств повышения производительности и отказоустойчивости программно-определяемых систем хранения данных с использованием средств автоматизированного контроля и анализа результатов на базе нейронной сети, шифр «Мульти-ЦОД» [3], результаты которой позволят внедрить технологии искусственного интеллекта в процессы управления и компенсировать дефицит высококвалифицированных специалистов служб эксплуатации операторов инфокоммуникационных инфраструктур Российской Федерации; научный руководитель – А.А. Зарубин;

- разработка экспериментального образца аппаратно-программной платформы предоставления приоритетного проезда регулируемых перекрестков для общественного, грузового и специального транспорта, шифр «Приоритетный проезд» [4], результаты которой подтверждают возможность реализации конкурентоспособных отечественных технических решений в области интегрированных средств навигации, связи и транспортных коммуникаций беспилотного транспорта в интегрированных транспортных системах Российской Федерации; научный руководитель – А.Г. Владыко;



[1] Ссылка на сайт СПбГУТ



[2] Ссылка на сайт «Цифровая экономика РФ»



[3] Ссылка на НИР Мульти-ЦОД



[4] Ссылка на НИР Приоритетный проезд

– исследование и отработка современных технологий проектирования адаптивных («умных») антенн и поиска решений для систем связи будущего, шифр «Растр» [5], результаты которой обеспечат технологический паритет радиотехнических средств на основе новых оригинальных отечественных алгоритмов обработки сигналов в сетях связи 2030; научный руководитель – Д.И. Кирик.

Нашли конструктивное продолжение в национальном проекте по развитию атомной науки и технологий результаты, достигнутые СПбГУТ в 2022 г. в рамках исследований «Прямой внутренний рециклинг дейтерий/третий с помощью сверхпроницаемых мембран», которые выполняются в интересах Росатома. Руководитель проекта – А.И. Лившиц.

Одна из продвинутых в настоящее время форм стимулирования научной деятельности – **мегагранты**. Мегагранты – программа международного сотрудничества российских вузов и научных организаций с учеными мирового уровня и ведущими зарубежными научно-образовательными центрами в сферах науки, образования и инноваций. Программа мегагрантов направлена, прежде всего, на подготовку научных кадров мирового уровня. Ежегодно в реализации ее проектов принимают участие около 2 500 молодых исследователей [6]. **Объем финансирования программы мегагрантов в РФ будет увеличен до 100 млн. рублей в год**, срок предоставления гранта будет увеличен до пяти с лет с возможностью продления еще на три года. В 2023 г. программа мегагрантов будет существенным образом обновлена. В новой версии программы будут введены новые форматы поддержки молодых ученых, а также усилен акцент на поддержку проектов с высокой образовательной составляющей и инициатив, направленных на возвращение кадров из-за рубежа.



[6] Ссылка на 9-й конкурс программы Мегагрантов

СПбГУТ активно участвует в подобных мегагрантах. В девятом конкурсе грантов Правительства Российской Федерации приняли участие 235 вузов и 58 научных организаций. Кроме российских ученых, больше всего заявок подали исследователи из Германии (24), США, Франции и Италии (по 17), а также Великобритании, Китая и Испании (16, 15 и 11 заявок соответственно). В число 30 победителей из 293 заявок, представленных на конкурс, вошел наш университет в область наук «Компьютерные, информационные науки и технологии». В июле между СПбГУТ и Минобрнауки России заключено соглашение («Мегагрант») на период 2022–2024 гг. в рамках федерального проекта «Развитие человеческого капитала в интересах регионов, отраслей и сектора исследований и разработок» национального проекта «Наука и университеты» в форме субсидий из федерального бюджета, выделяемых для государственной поддержки научных исследований, проводимых под руководством ведущих ученых в российских образовательных организациях высшего образования. По проекту СПбГУТ «Исследование сетевых технологий с ультрамалой задержкой и сверхвысокой плотностью на основе широкого применения искусственного интеллекта для сетей 6G» под руководством ведущего ученого Абд Эль-Латифа Ахмеда Абдельрахима (Египет) и д.т.н., профессора А.Е. Кучерявого – научного руководителя творческого коллектива исследователей (М.А. Маколкиной, А.И. Парамоновым, Р.А. Дунайцевым, Л.С. Горбачевой и др.) в 2022 г. получено несколько значимых результатов: разработаны методологические основы перспективных сетевых технологий, создана первая в научном международном сообществе модельная сеть с ультрамалыми задержками, а также проведена международная конференция International Conference on Advanced Computing & Next-Generation Communication (ICACNGC 2022) при поддержке и участии Университета принца Султана (Саудовская Аравия), Национальной школы прикладных наук Хурибга (Марокко), Российского университета дружбы народов и ряда других [7].



[5] Ссылка на НИР РАСТР



[7] Ссылка на ICACNGC 2022

В 2022 г. Российский научный фонд впервые организовал совместно с органами исполнительной власти субъектов Федерации в рамках софинансирования региональные конкурсы на проведение фундаментальных научных исследований и поисковых научных исследований отдельными и малыми научными группами, итоги которых будут подведены в 2023 г. В число заявок, представленных на региональный конкурс, включен проект кафедры безопасности информационных систем (зав. кафедрой Ю.М. Бородинский) факультета информационных систем и технологий.

По объектам интеллектуальной собственности в 2022 г. СПбГУТ вел интенсивную деятельность в области разработки технологий и технических решений, охраняемых патентным правом, авторскими и смежными правами. Среди результатов труда работников университета не только программы для ЭВМ, но и базы данных. Обеспечен прирост показателей СПбГУТ в Роспатенте, общее количество объектов превысило **отметку 2021 г. – 70 шт.**, а в ходе выполнения заказных НИР было дополнительно направлено на регистрацию более 10 РИД, патентовладельцем которых являются органы исполнительной власти – государственные заказчики в лице Российской Федерации. Важной тенденцией является прирост

объектов промышленной собственности СПбГУТ, в числе которых изобретения и полезные модели по проблематике систем передачи информации, синхронизации и информационной безопасности.

В СПбГУТ к 13 существующим открылись 2 новые лаборатории и киберполигон:

– лаборатория VR (**виртуальной реальности**) на кафедре информатики и компьютерного дизайна факультета информационных систем и технологий. В ходе летней учебной практики студенты университета (М. Зюриков, П. Никифоров, Ж. Эркинов, Д. Шеремет, И. Комаров) создали для Центрального музея связи им. А.С. Попова 3D-модели диска Нипкова, Рельефного аппарата Морзе фирмы Siemens&Halske (1886), первого радиоприемника «Фестиваль» и других экспонатов музея [8]. Опыт взаимодействия признан успешным, что послужило основой совместных совещаний представителей университета (А.В. Шестаков, А.А. Нестеров) и ФГБУК «Государственный Эрмитаж» (Д.А. Буданов) по заключению соглашения о взаимодействии в области практической подготовки студентов;



[8] Ссылка на сайт СПбГУТ 3D-моделей

– межфакультетская лаборатория **киберфизических систем** на кафедре программной инженерии и вычислительной техники факультета инфокоммуникационных систем и сетей (руководитель лаборатории А.В. Пачин), которая состоит из фрагмента производственной линии (роботизированные манипуляторы – с угловой кинематикой и плоскопараллельной кинематикой, управляющее оборудование, комплекты смарт-устройств для построения производственной линии) и программное обеспечение PTC ThingWorx;

– Северо-Западный федеральный образовательный центр Национального киберполигона на кафедре защищенных систем связи факультета инфокоммуникационных систем и сетей, в открытии которого приняли участие Д. Реуцкий, заместитель директора Департамента обеспечения кибербезопасности Минцифры России, А. Малышева, начальник отдела государственной службы и кадров УФССТЭК России по СЗФО.

СПбГУТ принял активное участие в крупнейших профильных федеральных и региональных выставках и форумах:



[9] Ссылка на сайт конференции АПИНО-2022

– в феврале проходила XI-я Международная научно-техническая и научно-методическая конференция **«Актуальные проблемы инфотелекоммуникаций в науке и образовании»** [9]; площадка объединила 700 участников: ученых из стран ближнего и дальнего зарубежья, представителей телекоммуникационных и IT-компаний, аспирантов и студентов; программа мероприятия включала пленарное заседание, выставку и работу семи научных направлений; было представлено и обсуждено свыше 500 докладов;

– в марте в конгрессно-выставочном центре «ЭКСПОФОРУМ» Санкт-Петербурга прошла Международная выставка передовых технологий обеспечения безопасности личности, общества и государства **«ЭКСПОТЕХНОСТРАЖ»**; университет телекоммуникаций был представлен на коллективном стенде предприятий Санкт-Петербурга по приглашению одного из организаторов выставки – Правительства Санкт-Петербурга;

– в апреле в Москве в ЦВК «Экспоцентр» разработки СПбГУТ были представлены на форуме **«Связь-2022»** в рамках «Российской недели высоких технологий-2022»;

– в мае состоялась 76-я по счету региональная научно-техническая конференция студентов, аспирантов и молодых ученых **«СТУДЕНЧЕСКАЯ ВЕСНА-2022»** [10]; участники представляли свои научные результаты в таких направлениях, как радиотехнологии связи, инфокоммуникационные сети и системы, информационные системы и технологии, цифровая экономика, управление и бизнес-информатика и т.д.; в период проведения конференции **СПбГУТ был аккредитован как площадка программы «УМНИК» для полуфинального отбора конкурсантов;**



[10] Ссылка на сайт «Студенческая весна-2022»

– в мае-июне в Москве прошли финальные мероприятия Всероссийского инженерного конкурса – профессионального соревнования по выявлению лучших представителей среди студентов и аспирантов выпускных курсов; отобраны более 3 тыс. участников, обучающихся в 172 вузах из 71 региона страны; магистрант СПбГУТ А. Тишкин (ИНО, БИМ-11з) стал призером в номинации «Лучшая выпускная квалификационная работа магистра»;

– в июле КНВШ СПб подведены итоги конкурса грантов для студентов вузов, аспирантов вузов, отраслевых и академических институтов, расположенных на территории Санкт-Петербурга; конкурс проводился по определенным направлениям: гуманитарные науки, естественные и точные науки, технические науки, медицинские науки, культура и искусство; от СПбГУТ в число победителей вошли: Д. Дмитриева (магистрант кафедры ФилС), А. Валов (аспирант кафедры ФилС), А. Помогалова (аспирант кафедры ИКС), А. Спиркина (аспирант кафедры ИКС);

– в конце октября в Зеленограде на территории Технополиса «Москва» в четвертый раз прошли Всероссийские технологические соревнования по перспективным направлениям развития радиосвязи «Радиофест-2022»; организаторы соревнований – Минпромторг России, Минобрнауки России, Фонд перспективных исследований, Технополис «Москва», НИУ «МИЭТ» и АО «Завод ПРОТОН»; по направлению «Радиоперехват» в финальном раунде между СПбГУТ и ТУСУР наша команда (Е. Червинко, М. Гордеев) заняла второе место; в раунде за третье место в нижней турнирной сетке между СПбГУТ и МАИ победу одержала наша команда (В. Мошков, Д. Юраков); по направлению «Радиосвязь» команда СПбГУТ (С. Мышнянов, О. Гуминский) заняла третье место;

– в октябре СПбГУТ совместно с Федеральным учебно-методическим объединением в сфере высшего образования по УГСН 10.00.00 «Информационная безопасность» при поддержке Национального киберполигона выступил организатором проведения Всероссийских киберучений по информационной безопасности «OpenBonch 2022» [11]; в рамках федерального проекта «Информационная безопасность» национальной программы «Цифровая экономика Российской Федерации»;

– в октябре в университете в шестой раз состоялось заседание Молодежной научной школы «Интеллектуальные безопасные информационные системы и технологии» в рамках XVIII Санкт-Петербургской международной конференции «Региональная информатика (РИ-2022)» под эгидой ЮНЕСКО при поддержке Правительства Санкт-Петербурга; мероприятие прошло под руководством профессора И.А. Зикратова (декана факультета ИСиТ);

– в ноябре представители СПбГУТ (О. Караева и А. Ильина) приняли активное участие в VII Всероссийской научно-практической конференции «Актуальные вопросы реализации образовательных программ на подготовительных факультетах для иностранных граждан» на базе Государственного института русского языка им. А.С. Пушкина, которая была организована Минобрнауки России, Росотрудничеством и Международной ассоциацией преподавателей русского языка и литературы;

– в ноябре в рамках Международного форума «ИТ-Диалог 2022» стенд и экспозиция СПбГУТ были представлены М.И. Шадаеву, министру цифрового развития, связи и массовых коммуникаций Российской Федерации, С. Казарину, вице-губернатору Санкт-Петербурга, и Ю. Смирновой, председателю комитета по информатизации и связи Санкт-Петербурга. Мероприятие проходило в Центральном музее связи имени А.С. Попова и объединило более 800 специалистов из 40 регионов России [12]. На выставке СПбГУТ представлены сегмент ИТ-инфраструктуры телекоммуникационной отрасли Национального киберполигона (проект кафедры защищенных систем связи), совместно с ИТ-компанией «Омега» – программно-аппаратный комплекс «Нейробокс», а совместно с музеем связи – цифровой 3D-двойник музейных экспонатов;

– в декабре в СПбГУТ состоялся **Международный Балтийский коммуникационный форум – BAFO-2022**; это масштабное научно-практическое мероприятие, ставшее визитной карточкой факультета социальных цифровых технологий (СЦТ) университета; программа Форума включала в себя: мастер-классы от специалистов в области социальных, маркетинговых и международных коммуникаций, а также научные конференции студентов и преподавателей и т. д.;

– в декабре СПбГУТ принимал региональную научно-методическую конференцию магистрантов и их руководителей «Подготовка профессиональных кадров в магистратуре для цифровой экономики» – ПКМ-2022 [13], на котором было заявлено 427 докладов от ВолГУ, ИТМО, КФУ, МФТИ, НИУ ВШЭ, ПГУТИ, СамГТУ, СибГУТИ, СПбЛТУ, СПбГМТУ, СПбГУ, СПбПУ и СПбГУТ; цель форума – апробация результатов научно-исследовательской деятельности магистрантов, их наставников, а также руководителей образовательных программ магистратуры; направления ПКМ-2022 – радиотехнологии связи, инфокоммуникационные сети и системы, информационные системы и технологии, теоретические основы радиоэлектроники и систем связи, цифровая экономика и управление в инфокоммуникациях;

– в декабре в Санкт-Петербурге состоялся финал программы интенсивного развития для студентов в области логистики, закупок и оптимизации – Акселератор «Снабжение» (организаторы проекта – компания «Газпромнефть-Снабжение», группа «АКТИОН. Студенты»), в котором СПбГУТ представляла студентка К. Большакова (БИМ21-з) и в составе группы студентов представили проект наглядной 3D-модели инновационного проекта с использованием искусственного интеллекта.

Студенческая научная деятельность в 2022 г., при постоянной поддержке А.В. Шестакова, проректора по научной работе, А.А. Нестерова, начальника управления организации научной работы и подготовки научных кадров, при тесном взаимодействии с комитетом по научной работе студенческого совета университета (Е. Карелиным, В. Нецветаевым), представляет собой многоаспектную палитру участия в конкурсах, грантах и кейс-чемпионатах; в 2022 г. более чем на 30 % выросло число студентов-участников конкурсов, конференций и грантовых программ; свыше 50 студентов и аспирантов стали



[11] Ссылка на итоги OPEN-BONCH



[12] Ссылка на сайт ИТ-Диалог



[13] Ссылка на сайт конференции ПКМ

победителями российских и международных конкурсов проектов; среди наиболее выдающихся и интересных результатов следует отметить:

- по результатам конкурсного отбора грантовой программы «Гранты Президента Российской Федерации» в 2021/2022 учебном году были признаны победителями конкурса и получателями грантов на протяжении всего срока обучения Е. Галимова (студентка Института непрерывного образования), А. Запайщиков, Д. Юраков (магистранты факультета РТС);

- по итогам Всероссийского конкурса «Инфофорум – Новое поколение», в номинации «Студент года» лауреатом стал А. Катасонов (магистрант факультета ИКСС, ныне аспирант);

- призерами региональных олимпиад стали студенты СПбГУТ 3 место по направлению «Биотехнические системы (биомедицинская инженерия)» В. Мишарин (РТС), 3 место по направлению «Русский язык» – А. Лоскутова (СЦТ);



[14] Ссылка на сайт
#Арктический
дневник

- в октябре–ноябре благодаря победе команды института магистратуры СПбГУТ (зам. директора ИМ по учебной работе А.Б. Степанов, Д. Кузьмина и А. Лосев (НОЦ «Медиацентр»), студенты А. Горцева, А. Запайщиков, Е. Каранова, В. Коновалова, К. Тафинцев, Н. Шашков) в профессиональном конкурсе «Открываем Россию заново», организованном Высшей школой экономики и АНО «Россия – страна возможностей» организована студенческая экспедиция по программе «Больше, чем путешествие; в ходе экспедиции А.Д. Степанову, заместителю главы администрации пгт. Диксон, был вручен флаг СПбГУТ, переданный проректором по научной работе А.В. Шестаковым руководителю экспедиции у памятника Э.Т. Кренкеля в Колледже телекоммуникаций за несколько дней до отъезда команды, проведен ряд научных исследований и мероприятий по научной и образовательным тематикам в Норильске и Диксоне [14];

- в ноябре в финале всероссийского студенческого акселератора StartupHouse Universities 2022 на базе Университета Иннополис в Татарстане СПбГУТ представляли Д. Бельшева, С. Максимова, В. Побегалова и А. Романова (ИМ) со стартап-проектом «Изготовление пластиковой нити для 3D-печати из утилизированного материала», который получил номинацию «Уровень презентации»;

- в ноябре в Москве в Центре Событий РБК на Всероссийском форуме университетского технологического предпринимательства СПбГУТ представляли студенты Р. Ибрагимов (ИКСС) и Я. Стахира (ИСИТ) благодаря победе в конкурсе «Студенческий стартап» и грантом на реализацию платформы, которая генерирует внешний вид и подбирает одежду российских дизайнеров;

- в декабре студенты Н. Паскидов и В. Дрепа (факультет ИКСС) стали призерами (2 и 3 место с денежной премией) открытого всероссийского конкурса на лучшую научную работу в области информационной безопасности (организатор МТУСИ);

- в декабре на Форуме молодых профессионалов «АтомПрофи», организованном Корпоративной Академией «Росатома», университет представляла студентка А. Белая (факультет РТС), благодаря ее победе в финале Всероссийского кейс-чемпионата по решению прикладных задач «Opportunity cup 2022», с проектом экзоскелета для строителей АЭС.

Учитывая многотысячный студенческий коллектив, одной из форм воспитательной работы по линии науки стали регулярные встречи в режиме онлайн с проректором по научной работе в студенческий полдень (в длинный перерыв между парами) с обсуждением наиболее острых и насущных текущих тем и проблем, а также с участием различных специалистов и экспертов не только нашего вуза.

В СПбГУТ в текущем году обеспечен **переход подготовки научных кадров высшей квалификации (аспирантов) в соответствии с новыми федеральными государственными требованиями**, вступившими в силу с 01.03.2022 [15]. Успешно выполнен план приема на 2022/2023 учебный год, общее число аспирантов на 09.12.2022 составило 162 чел., в том числе поступивших в 2022 г. – 41 чел. (в аспирантуре СПбГУТ 150 чел. по состоянию на 31.12.2021).

В октябре в университете введено в действие «Положение о докторантуре в СПбГУТ», в соответствии с которым в декабре 2022 г. состоялся конкурсный отбор **2 кандидатов в докторантуру (внебюджет за счет средств мегагранта): А.И. Выборновой и А.С.А. Мутханна, доценты кафедры ССиПД СПбГУТ.**



[15] Ссылка на сайт
Отдела аспирантуры
и докторантуры

В диссертационных советах СПбГУТ 55.2.004.01 и 99.2.038.03 аналогично показателям 2021 г. успешно состоялись **3 защиты докторских диссертаций** (Е.А. Максимова, МЧС России; Д.А. Щемелинин, Политех; С.С. Владимиров, СПбГУТ) и **13 защит кандидатских диссертаций** (СПбГУТ: М.А. Блинников, С.Н. Бушеленков, М.В. Захаров, Д.В. Кашкаров, А.Р.А. Мохамед, А.В. Спиркина, А.А. Хакимов, И.Е. Пестов; НИУ ВШЭ: А.Ю. Ануфриенко; Политех: А.С. Римша; ГУАП: И.С. Козин; ВОЕНМЕХ: К.А. Коваль, О.А. Орешина). Выпускники аспирантуры и работники СПбГУТ защищают научные квалификационные работы и в других диссертационных советах. Так, Д.О. Стародубцев успешно защитил 20.04.2022 диссертацию на соискание ученой степени кандидата экономических наук в Д 212.354.04 ФГБОУ ВО «Санкт-

Петербургский государственный экономический университет», а К.В. Дукельский 20.12.2022 диссертацию на соискание ученой степени доктора технических наук в Диссертационном совете Национального исследовательского университета ИТМО 05.22.00 по специальности 1.3.6 «Оптика» (технические науки).

Научно-технический совет СПбГУТ в 2022 г. существенно усилил помощь в организации деятельности диссертационных советов университета и в экспертизе результатов НИОКТР, выполняемых структурными подразделениями университета, благодаря активной деятельности отдела организации научной работы и интеллектуальной собственности (Е.А. Аникевич). В состав НТС университета введены ученые секретари (А.Г. Владыко, М.А. Маколкина), а также ряд новых членов диссертационных советов университета. Несмотря на значительную загрузку ученых, проведено более 20 заседаний НТС СПбГУТ, что превышает аналогичные показатели предыдущих лет (2018 – 11 заседаний) [16].



[16] Ссылка на сайт
НТС СПбГУТ

Качество научной работы университета находится в непрерывной взаимосвязи с уровнем развития системы менеджмента качества университета в целом и регламентированной организации. В ноябре 2022 года СПбГУТ занял 1 место и удостоен почетного знака в конкурсе на соискание награды Правительства Санкт-Петербурга – почетного знака «За качество товаров (продукции), работ и услуг», организатором которого выступил Комитет по промышленной политике, инновациям и торговле Санкт-Петербурга. В декабре 2022 года СПбГУТ стал победителем ежегодной городской премии «Признание и влияние» в номинации «Вуз года», в которой участвовали 58 учебных заведений Санкт-Петербурга. В университете впервые разработано и введено в действие СМК-ВНД-160/22 «**Положение о научных школах университета**», которое в условиях недостаточно однозначного современного нормативно-правового поля позволяет регламентировать статус научных, научно-образовательных и научно-педагогических школ и процедуры его присвоения научным коллективам в СПбГУТ [17]. Актуализирована **университетская библиотека стандартов (более 30 ед.)**, которые введены в действие в Российской Федерации с 2021 г., для всестороннего обеспечения в университете исполнителей НИОКТР в рамках государственных заказов. Активно проводятся работы по расширению перечня лицензий на выполнение различных работ (услуг). Разработан и введен в действие СМК-ВНД «**Порядок формирования плана научной работы университета**» в части показателей, критериев и процедур университетского задания для структурных подразделений СПбГУТ. Выпущено и размещено в открытом доступе на сайте СПбГУТ учебное пособие «**Подготовка квалификационной работы на соискание ученой степени**» (авторы – А.В. Шестаков, В.С. Елагин, И.М. Татарникова, А.В. Федорова), в котором изложены основные направления в подготовке научно-педагогических кадров высшей квалификации: процесс обучения в аспирантуре и подготовке диссертации, мероприятия Диссертационного совета, публикационная деятельность, процедуры регистрации результатов интеллектуальной деятельности аспирантов и соискателей [18]. Многоаспектно были представлены результаты по науке при осуществлении обследования экспертной комиссией по заявке СПбГУТ на конкурс Премии Правительства Российской Федерации в области качества в 2022 г., что было достигнуто благодаря активности работников подразделений проректора по научной работе (Н.И. Карташовой, А.С. Мамончиковой, Е.М. Аникевич, Е.М. Матовой, П.А. Гладышевой).



[17] Ссылка на сайт
Научных школ
СПбГУТ



[18] Ссылка
на учебное пособие

В число победителей на соискание премий Правительства Санкт-Петербурга в области научно-педагогической деятельности в 2022 г. от СПбГУТ вошли 4 преподавателя (А.С. Алешин, А.В. Неровный, И.А. Цвериганашвили, Г.А. Фокин). Победители конкурсов грантов и стипендиатов Правительства Санкт-Петербурга в 2022 г. от СПбГУТ стали 13 человек (в номинациях: молодой кандидат наук – К.А. Ахрамеев, И.А. Ушаков; аспирант – А.В. Помоголова; студенты – Е.В. Колтунова, В.В. Романов, Н.В. Тимошин, Д.А. Щетинина, И.И. Ярыгина и другие).

В Указе Президента РФ от 25.04.2022 № 231 «Об объявлении в Российской Федерации Десятилетия науки и технологий» говорится об усилении роли исследовательской работы, которая действительно является залогом решения важнейших задач развития общества и страны. Одним из показателей исследовательской работы является **публикационная активность**.

Публикационная активность университета в 2022 г. по прогнозам превысит показатели 2021 г. За авторством сотрудников, аспирантов и студентов СПбГУТ издано **1058 публикаций** (по состоянию на 12.12.2022), входящих в РИНЦ (по итоговым данным Госмониторинга, в 2021 г. было 1285 публикаций). В 2022 г. впервые внедрена благодаря кропотливой организационной работе А.А. Нестерова, Н.И. Карташовой, Н.Н. Громовой практика материального стимулирования работников СПбГУТ за публикации в высокорейтинговых изданиях [19]. В результате количе-



[19] Ссылка на
документы СПбГУТ

ство научных статей в квартилях Q1 и Q2 базы **Scopus увеличилось на 43 %** (в 2022 и в 2021 гг. 40 и 28 статей, соответственно). Возросла доля публикаций в журналах, входящих в перечень **ВАК – 17,6 %** в 2022 г. против 14,5 % в 2021 г.

На плановой основе последовательно повышается **статус и качество научно-технических журналов университета**. В настоящее время **регистрацию в качестве СМИ в Роскомнадзоре** успешно прошло вновь созданное электронное сетевое издание «Социогуманитарные коммуникации» по гуманитарным специальностям ВАК, в состав редсовета и редколлегии которого вошли Г.М. Машков, С.И. Ивасишин, А.В. Шестаков, И.А. Алексеенко, А.А. Зарубин, Д.В. Шутман, А.Б. Гехт и др.

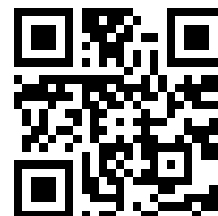
Организована системная работа по повышению научной значимости журнала «Труды учебных заведений связи» [20].

Как известно, действующая концепция оценки труда ученых преимущественно опирается на наукометрический подход (анализ публикационной активности) – чем больше у исследователя публикаций в зарубежных изданиях, тем выше оценка. При этом, согласно условиям финансирования госпрограмм, а также предоставления грантов от Российского научного фонда, обязательна публикация в высокорейтинговых научных изданиях. До недавнего времени к ним относились только журналы, индексируемые в международных базах научных изданий – Web of Science и Scopus. В свете последних политических событий **Минобрнауки отменило обязательный наукометрический показатель по количеству статей на этих платформах**, и приняло решение создать свою, **Национальную систему оценки результативности научных исследований и разработок**. В сжатые сроки Рабочей группой ВАК по совершенствованию и оптимизации перечня научных изданий была разработана, апробирована и введена в действие в октябре текущего года методика их оценки и распределения по категориям значимости. Методика включает в себя две составляющие: **количественную** (наукометрические показатели) и **качественную** (экспертную). В количественные показатели входят такие параметры оценки, как Science Index, индексы Херфиндала – Хиршмана и Джинни, индекс Хирша – средний для авторов и 10-летний для издания, среднее число просмотров на одну статью за год. В качестве экспертно-оцениваемых показателей приняли качество и уникальность научных статей, уровень авторитетности авторов, качество организации рецензирования, организация-учредитель.

По результатам проведенного анализа наукометрических показателей все научные издания, включенные в Перечень рецензируемых научных изданий (так называемый «Перечень ВАК»), **были «выстроены» (отранжированы) по убыванию интегрального показателя научной значимости, распределены по категориям и переданы на рассмотрение в профильные экспертные советы ВАК**. С учетом оценки, проведенной экспертными советами ВАК по каждой представленной в журналах научной специальности, был сформирован **Итоговый список распределенных по категориям K1, K2 и K3 рецензируемых научных изданий**, и опубликован в письме от 06.12.2022 № 02-1198, адресованном главным редакторам, председателям редакционных коллегий и редакционных советов рецензируемых научных изданий [21].

В соответствии с утвержденным распределением, журналу «Труды учебных заведений связи» был присвоена высшая категория – K1.

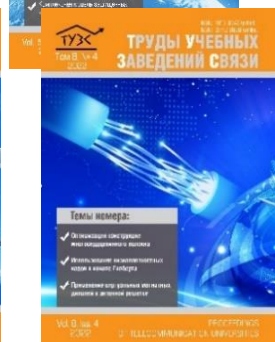
26.10.2022 на заседании ВАК были актуализированы требования, в части критериев к соискателям ученой степени доктора технических наук. Согласно им, количество публикаций, в которых излагаются основные научные результаты в рецензируемых научных изданиях, должно быть не менее 10, из которых не менее 5 – в изданиях, отнесенных к категориям K-1 или K-2, либо RSCI, а также в индексируемых WoS и Scopus; то



[20] Ссылка на сайт журнала «Труды учебных заведений связи»



[21] Письмо ВАК о присвоении журналам K-1, K-2, K-3



есть, фактически приравняв их научную значимость. Более того, наблюдая тенденцию последних лет, можно прогнозировать ужесточение требований по примеру критериев оценки результативности кандидатов в члены Диссоветов для обладателей степени PhD или кандидатов наук: не менее 20 K-1 и RSCI, или Q-1 и Q-2. Все это говорит о большом «научном весе» журнала – обладателя K-1.

Вне всякого сомнения, данную категорию журнал получил по совокупности заслуг, и это очень наглядно демонстрируют наукометрические показатели издания. **Согласно рейтингу SCIENCE INDEX по тематике «Связь» (по данным БД РИНЦ), издание поднялось с 6 (2020 г.) на 5 место (2021 г.).** Как видно из отчета БД E-library, за последние 5 лет в журнале «Труды учебных заведений связи» было опубликовано 258 статей, в написании которых принимали участие свыше 500 авторов. Цитирование статей за последние 5 лет возросло **с 24 (2017 г.) до 132 (2021 г.)**, просмотры публикаций – **с 384 (2016 г.) до 4215 (2021 г.)**, а число загрузок статей – **с 61 (2017 г.) до 441 (2021 г.)**. Подтверждается правильность курса руководства по научной работе на **рост числа публикаций молодых ученых** во вновь введенной рубрике журнала «Результаты исследования молодых ученых». В 2022 г. опубликовано 14 работ (30,4 % от общего числа публикаций за год). Для сравнения, в 2021 г. таких работ было 9 (19,1 % от числа публикаций за год).

Благодаря усилиям коллектива Редакции (М.В. Буйневича, Д.Н. Яшугина, И.М. Татарниковой) при поддержке научных работников и Руководства СПбГУТ, журнал заслуженно занимает лидирующие позиции среди научных изданий, и надеемся, будет удерживать эту высокую планку и впредь.

Искренне считаю, что наш ВУЗ и далее будет оставаться отличной площадкой для новых научных достижений и открытий.

Впереди всех нас ждет только успех и плодотворная, дающая хорошие результаты работа, потому что сегодня – это только Начала деканаук и технологий, как и главный труд Евклида, Марка Порция Катона Старшего, Исаака Ньютона и Рене Декарта!

С наступающим Новым годом! Здоровья и благополучия вам, дорогие друзья и коллеги, и вашим семьям!

*Проректор по научной работе СПбГУТ,
доктор технических наук,
старший научный сотрудник
Александр Викторович Шестаков*



СОДЕРЖАНИЕ

CONTENTS

КОМПЬЮТЕРНЫЕ НАУКИ И ИНФОРМАТИКА

Сергеев А.М. Связь симметрии и антисимметрии квазиортогональных циклических матриц с простыми числами	14	Sergeev A. Interrelation of symmetry and antisymmetry of quasi-orthogonal cyclic matrices with prime numbers
---	-----------	--

ЭЛЕКТРОНИКА, ФОТОНИКА, ПРИБОРОСТРОЕНИЕ И СВЯЗЬ

Брусин Е.А. Реализация алгоритма начальной синхронизации демодулятора сигналов с прямым расширением спектра на основе быстрого преобразования Фурье. Часть 1. Постановка задачи и подход к решению	21	Brusin E. Direct sequence spread spectrum signal's demodulator acquisition implementation based on fast Fourier transform. Part 1. Problem statement and solution approach
Былина М.С., Гультяева Л.А. Многосердцевинное оптическое волокно со ступенчатыми одномодовыми сердцевинами. Часть 1. Изоляция сплошными оболочками	28	Bylina M., Gultyayeva L. Multi-core optical fiber with stepped single-mode cores. Part 1. Insulation with solid clads
Ищенко Е.А., Пастернак Ю.Г., Пендюрин В.А., Фёдоров С.М. Применение виртуальных магнитных диполей в антенной решетке для повышения точности пеленгации	39	Ishchenko E., Pasternak Yu., Pendyurin V., Fedorov S. Application of a virtual magnetic dipoles in antenna array to increase the direction finding accuracy
Каретников В.В., Косяк Я.В., Данилов О.О., Беспалов А.П. Современный подход к сбору и обработке данных от автоматической идентификационной системы в целях организации управления движением судов	48	Karetnikov V., Kosiak Ya., Danilov O., Bespalov A. Modern approach to data collection and processing from automatic identification system for ship traffic organization
Овчинников А.А., Вересова А.М., Фоминых А.А. Об использовании низкоплотностных кодов в канале Гилберта	55	Ovchinnikov A., Veresova A., Fominykh A. Usage of LDPC codes in a Gilbert channel

ИНФОРМАЦИОННЫЕ ТЕХНОЛОГИИ И ТЕЛЕКОММУНИКАЦИИ

Елагин В.С. Модели применения блокчейн в государственных информационных системах	65	Elagin V. Models of blockchain application in government information systems
---	-----------	---

РЕЗУЛЬТАТЫ ИССЛЕДОВАНИЯ МОЛОДЫХ УЧЕНЫХ

Акишин В.А. Методика поддержки принятия решений на основе оценки клиентского опыта и показателей эффективности оператора связи	75	Akishin V. Decision support methodology based on evaluation of customer experience and telecommunications operator efficiency indicators
Алзагир А.А. Летающие мобильные граничные вычисления на базе БПЛА для узлов Интернета вещей в «умном» сельском хозяйстве	82	Alzaghir A. Flying fog mobile edge computing based on UAV-Assisted for IoT nodes in smart agriculture
Аль-Свейти М. Методы машинного обучения для прогнозирования трафика в многоуровневой облачной архитектуре для сервисов беспилотных автомобилей	89	Alsweity M. Deep learning approaches for traffic prediction forecasting in multi-level cloud architecture for autonomous vehicle services
Бабанов И.А. Исследование корреляционных свойств сигналообразующих последовательностей в целях оптимизации характеристик канала случайного доступа 5G NR	100	Babanov I. Correlation properties investigation of signaling sequences to optimize the 5G NR random access channel characteristics
Ишкуватов С.М. Способ и алгоритм определения типа трафика в зашифрованном канале связи	109	Ishkuvatov S. Method and Algorithm for Determining the Type of Traffic in an Encrypted Communication Channel
Ярмак А.В. Разработка схемы контроля доступа к данным на основе иерархии ролей с использованием постквантовых математических преобразований	119	Yarmak A. Post-quantum cryptographic access control based on hierarchical RBAC model

КОМПЬЮТЕРНЫЕ НАУКИ И ИНФОРМАТИКА

1.2.2 – Математическое моделирование, численные методы и комплексы программ

Научная статья

УДК 519.614

DOI:10.31854/1813-324X-2022-8-4-14-19



Связь симметрии и антисимметрии квазиортогональных циклических матриц с простыми числами

Александр Михайлович Сергеев, aleks.asklab@gmail.com

Санкт-Петербургский государственный университет аэрокосмического приборостроения,
Санкт-Петербург, 190000, Российская Федерация

Аннотация: Рассматриваются квазиортогональные матрицы Адамара и матрицы Мерсенна с двумя и тремя значениями элементов, используемые в обработке цифровых данных, а также в качестве основы помехоустойчивых кодов и алгоритмов ортогональных преобразований изображений. Внимание уделяется структурам циклических матриц с симметриями и антисимметриями. Показывается связь симметрии и антисимметрии структур циклических матриц Адамара и Мерсенна на порядках, равных простым числам, произведению близких простых чисел, составным числам, степеням простого числа. Отдельно выделены порядки, равные степени простого числа 2, как порядки матриц Адамара, так и основа составных порядков матриц Мерсенна блочных структур с двумя значениями элементов. Показывается, что симметричные матрицы Адамара циклических и двуциклических структур, согласно расширенной границе Райзера, не существуют на порядках выше 32. Матрицы Мерсенна составных порядков, относящихся к последовательности чисел Мерсенна $2k - 1$, вложенных в последовательность порядков основного семейства матриц Мерсенна $4t - 1$, существуют в симметричном и антисимметричном виде. Для порядков, равных степеням простого числа, матрицы Мерсенна существуют в виде блочно-диагональных конструкций с тремя значениями элементов. Значение степени простого числа определяет количество блоков вдоль диагонали матрицы, на которой расположены элементы с третьим значением. При этом блоки являются циклическими симметричными и антисимметричными.

Ключевые слова: простые числа, квазиортогональные матрицы, матрицы Адамара, матрицы Мерсенна, симметричные и антисимметричные матрицы, кодирование сигналов, кодирование изображений

Источник финансирования: Исследование выполнено при финансовой поддержке РФФИ в рамках научного проекта № 19-29-06029.

Ссылка для цитирования: Сергеев А.М. Связь симметрии и антисимметрии квазиортогональных циклических матриц с простыми числами // Труды учебных заведений связи. 2022. Т. 8. № 4. С. 14–19. DOI:10.31854/1813-324X-2022-8-4-14-19

Interrelation of Symmetry and Antisymmetry of Quasi-Orthogonal Cyclic Matrices with Prime Numbers

Aleksandr Sergeev, aleks.asklab@gmail.com

Saint-Petersburg State University of Aerospace Instrumentation,
St. Petersburg, 190000, Russian Federation

Abstract: Quasi-orthogonal Hadamard matrices and Mersenne matrices with two and three values of the elements, used in digital data processing, are considered, as well as the basis of error-correcting codes and algorithms for transforming orthogonal images. Attention is paid to the structures of cyclic matrices with

symmetries and antisymmetries. The connection between symmetry and antisymmetry of structures of cyclic Hadamard and Mersenne matrices on a orders equal to prime numbers, products of close primes, composite numbers, powers of a prime number is shown. Separately, orders equal to the degrees of the prime number 2 are distinguished, both the orders of Hadamard matrices and the basis of the composite orders of Mersenne matrices of block structures with two element values. It is shown that symmetric Hadamard matrices of cyclic and bicyclic structures, according to the extended Riser boundary, do not exist on orders above 32. Mersenne matrices of composite orders belonging to the sequence of Mersenne numbers $2^k - 1$ nested in the sequence of orders of the main family of Mersenne matrices $4t - 1$ exist in a symmetric and antisymmetric form. For orders equal to the powers of a prime number, Mersenne matrices exist in the form of block-diagonal constructions with three element values. The value of prime power determines the number of blocks along the diagonal of the matrix on which the elements with the third value are located. The cyclic blocks are symmetrical and antisymmetric.

Keywords: prime numbers, quasi-orthogonal matrices, Hadamard matrices, Mersenne matrices, symmetric and antisymmetric matrices, signal encoding, image encoding

Funding: This research was funded by RFBR according to the research project No. 19-29-06029.

For citation: Sergeev A. Interrelation of Symmetry and Antisymmetry of Quasi-Orthogonal Cyclic Matrices with Prime Numbers. *Proc. of Telecom. Universities*. 2022;8(4):14–19. (in Russ.) DOI:10.31854/1813-324X-2022-8-4-14-19

Введение

Ортогональные (квазиортогональные) матрицы широко применяются в задачах обработки и преобразования информации. Особый интерес представляет поиск структурированных матриц с двумя или тремя значениями элементов [1], таких, например, как матрицы Адамара H_n , для которых справедливо $H_n^T H_n = nI$ на порядках $n = 4t$, где t – натуральное число, и матрицы Мерсенна M_n , для которых справедливо $M_n^T M_n = \omega(n)I$ на порядках $n = 4t - 1$, где $\omega(n)$ – вес матрицы [2, 3]; $I = \text{diag}\{1, 1, 1, \dots, 1\}$.

В помехоустойчивом кодировании изображений при передаче по открытым коммуникациям [4], в обработке изображений и их фильтрации [5–7] преимущественно используются ортогональные матрицы симметричные и структурированные по Уолшу, в кодировании сигналов – циклические матрицы [4, 8]. Однако для таких матриц ограничены возможные порядки существования и виды симметрии их структур на этих порядках.

Поиску связей математических объектов разного происхождения посвящено много работ. Именно понимание таких связей, например, для матриц, чисел и известных числовых последовательностей позволило получить уникальные результаты:

- матрицы золотого сечения на порядках, кратных размерам изображений в форматах JPEG и MJPEG [9];
- способ цепочного вычисления квазиортогональных матриц с разными предикторами [10];
- получение новых конструкций матриц Адамара на основе ядра (матриц Мерсенна) с окаймлением на всех порядках $n = 4t$ [11].

В настоящей работе рассматривается связь простых чисел, произведения близких простых чисел, составных чисел и степеней простых чисел как порядков матриц Адамара и Мерсенна с симметриями их циклических структур. Эта связь позволяет упростить выбор и процесс поиска таких матриц для конкретных преобразований изображений и сигналов.

Симметрии матриц Адамара и Мерсенна

Известно, что матрица:

- симметрична, если ее одинаковые элементы расположены симметрично относительно главной диагонали;
- антисимметрична, если расположенные симметрично относительно главной диагонали элементы имеют разные знаки [12];
- персимметрична, если одинаковые элементы расположены симметрично относительно побочной диагонали.

Порядки матриц Адамара, равные степеням простого числа 2, входят в общую последовательность порядков матриц Адамара $4t$.

Количество симметричных циклических матриц Адамара с элементами $\{1, -1\}$ ограничивает гипотеза Райзера [13]. Согласно ей, матриц Адамара порядков, больших 2^2 , нет. Эта гипотеза расширена на двуциклические матрицы порядков до 2^5 из четырех блоков порядка 2^4 [14]. Хотя гипотезы не доказаны, однако вычислительный эксперимент по поиску матриц указанных конструкций на порядках выше 32, длящийся более 5 лет, не позволил их опровергнуть. Таким образом, циклических и би-

циклических симметричных матриц Адамара ограниченное число, и осуществлять их поиск на порядках, больших 2^5 , не имеет смысла.

Ограничения на существование симметричных (антисимметричных) циклических матриц Мерсенна с элементами $\{1, -b\}$ носят иной характер, поскольку эти матрицы нечетных порядков, обобщающие матрицы Адамара, имеют другой генезис, и в основном циклические [15]. Нечетные порядки матриц Мерсенна связаны с нечетными простыми числами. На рисунке 1 приведены портреты [16] циклических симметричной и антисимметричной матриц Мерсенна порядка 11, где белое поле обозначает позицию элемента со значением 1, а синее – позицию элемента $-b$ в матрице. Здесь антисимметричная матрица является персимметричной.

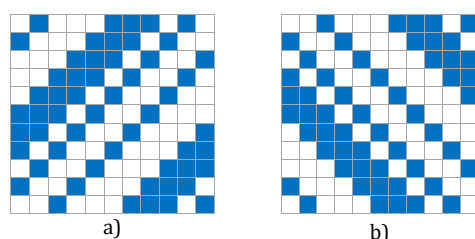


Рис. 1. Портреты циклических симметричной (а) и антисимметричной (б) матриц M_{11}

Fig. 1. Portraits of Cyclic Symmetric (a) and Antisymmetric (b) Matrices M_{11}

Порядки матриц Мерсенна $n = 4t - 1$ включают простые или составные числа Мерсенна, степень простого числа или произведение пар близких простых чисел [17].

Связь простых чисел как порядков матриц Мерсенна с их структурами

Впервые связь порядков, равных простым числам, была отмечена Холлом в работе [18]. Он обнаружил, что если порядок матрицы Мерсенна равен произведению пар близких простых чисел, то она будет циклической. В качестве примера на рисунке 2 приведен портрет циклической матрицы Мерсенна порядка 15 ($n = 3 \times 5$).

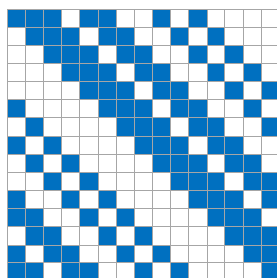


Рис. 2. Портрет циклической персимметричной матрицы M_{15} с дефектом антисимметрии

Fig. 2. Portrait of a Cyclic Persymmetric Matrix M_{15} with an Antisymmetry Defect

Однако Холл никак не отметил того факта, что циклическость структуры этой матрицы получена за

счет дефекта антисимметрии [12], который сегодня для циклических матриц измеряется и учитывается при построении. Учет возможных дефектов антисимметрии позволил найти другие циклические матрицы порядков 15 и 35 [19], портреты которых приведены на рисунке 3, где видны эти дефекты.

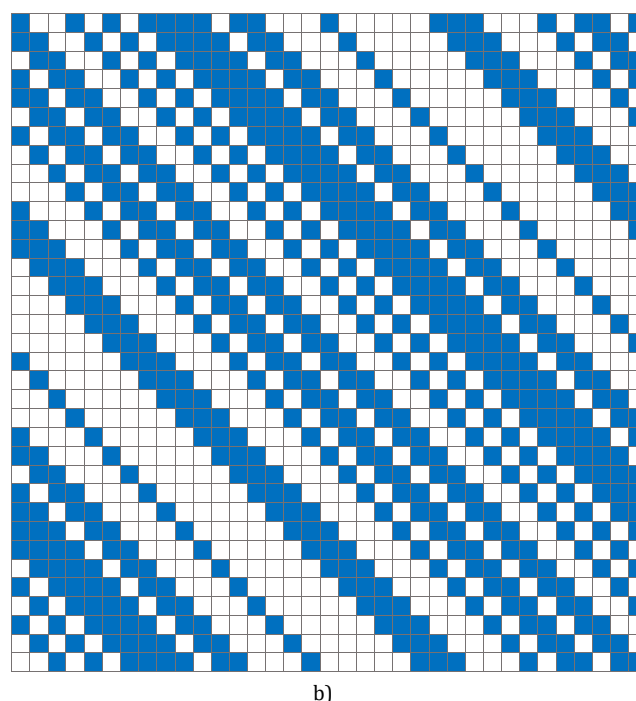
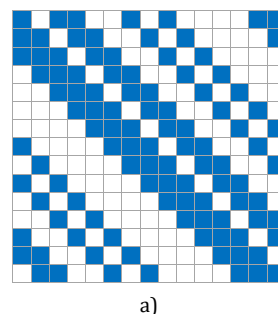


Рис. 3. Портреты циклических матриц M_{15} (а) и M_{35} (б) с дефектами антисимметрии

Fig. 3. Portraits of Cyclic Matrices M_{15} (a) and M_{35} (b) with Antisymmetry Defects

Позже Холл нашел еще циклические матрицы порядков 35 ($n = 5 \times 7$) и 63 ($n = 7 \times 9$). Однако число 9 не является простым, и можно предположить, что матрица Мерсенна порядка 63, найденная Холлом, относится к матрицам рассматриваемого типа по другому основанию (ведь циклической матрицы Мерсенна порядка 99 ($n = 9 \times 11$) нет именно по причине того, что число 9 не является простым). Действительно, порядок 63 является составным и относится к последовательности чисел Мерсенна $n = 2^k - 1$, вложенных в последовательность порядков основного семейства матриц Мерсенна $n = 4t - 1$. Матрицы же основного семейства всегда имеют циклическую структуру.

Простое число 2 является четным. Следовательно, степени этого числа и связанные с ними минимальным расстоянием в единицу числа Мерсенна отличаются от степеней прочих простых чисел. Плата за существование матриц Мерсенна составных порядков $n = 2^k - 1$ прежняя – это циклические матрицы с дефектом антисимметрии.

Для порядков, равных степеням простых чисел, соответствуют блочно-циклические матрицы, у которых степень определяет число блоков вдоль диагонали. Например, найденная матрица M_{27} ($n = 3^3$) состоит из 3×3 блоков порядка 9, а каждый из них, в свою очередь, состоит из блоков порядка 3, каждый из которых является циклическим симметричным или антисимметричным. Такие блочно-циклические матрицы также наделены свойством симметрии и антисимметрии относительно главной диагонали, на которой располагаются элементы с третьим значением d . Пример блочно-циклической антисимметричной матрицы Мерсенна порядка 27 (она же матрица Якобсталя с элементом -1 вместо $-b$) [18], приведен на рисунке 4. Здесь элементы со значением d на диагонали представлены серым цветом.

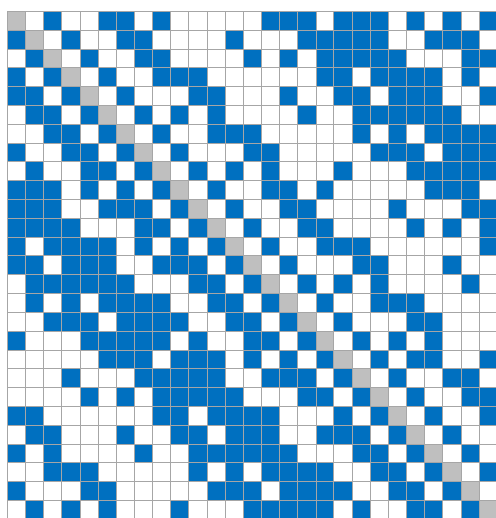


Рис. 4. Портрет блочно-циклической антисимметричной матрицы M_{27}

Fig. 4. Portrait of a Block-Cyclic Antisymmetric Matrix M_{27}

Как и матрица M_{11} , приведенная на рисунке 4, матрица M_{27} является в целом антисимметричной и персимметричной.

Особенности практических применений циклических матриц

Преимущества практических применений симметричных ортогональных матриц Адамара и Мерсенна – Уолша в системах сжатия, маскирования,

помехоустойчивого кодирования изображений показаны в работах [20–22] и многих других.

Однако в отличие от симметричных ортогональных матриц, особенности симметричных и персимметричных циклических квазиортогональных матриц, имеющие практическое значение, следующие.

Во-первых, это простота хранения. Матрица восстанавливается по первой строке циклическим сдвигом – работой с индексами элементов при программной реализации алгоритмов преобразований.

Во-вторых, циклическая симметричная и персимметричная матрицы при транспонировании не меняют симметрии, что упрощает выполнение матричных умножений при прямом и обратном преобразованиях.

В-третьих, циклические матрицы Мерсенна, являясь основой (ядром) матриц Адамара [11], обеспечивают получение целого спектра «почти циклических» матриц Адамара – матриц с каймой [23], значительно расширяя их количество для применения в ортогональных преобразованиях.

Циклические персимметричные матрицы Мерсенна, являясь основой помехоустойчивых кодов, хорошо себя зарекомендовали в системах с корреляционным приемом сигналов [8, 24], в том числе в виде вложенных конструкций. Они имеют наилучшие отношения главного пика автокорреляционной функции к максимальным по амплитуде боковым лепесткам. Как показано в работе [8], по данной характеристике полученные коды оказались лучше, чем широко известные коды Баркера, используемые в наборе стандартов связи IEEE802.11 [25].

Заключение

Строки циклических квазиортогональных матриц могут быть использованы в качестве основы кодов для систем связи с корреляционным приемом или помехоустойчивого кодирования радиосигналов и изображений.

В работе показано, что циклические квазиортогональные матрицы с симметриями существуют на порядках, равных составным числам Мерсенна, в том числе равных произведениям пар близких простых чисел. Блочные циклические матрицы Мерсенна с симметриями структуры существуют на порядках, равных степени простого числа.

Рассмотренные в работе связи порядков матриц и простых чисел позволяют упростить поиск циклических квазиортогональных матриц с особенностями симметрий на порядках, необходимых при разработке помехозащищенных кодов.

БЛАГОДАРНОСТИ

Автор выражает искреннюю благодарность профессору Н.А. Балонину за консультации и ценные советы в процессе работы над материалом.

Список источников

1. Seberry J., Yamada M. *Hadamard Matrices: Constructions using Number Theory and Linear Algebra*. Hoboken: John Wiley & Sons, 2020. 352 p.
2. Балонин Н.А., Сергеев М.Б. Нормы обобщенных матриц Адамара // Вестник Санкт-Петербургского университета. Прикладная математика. Информатика. Процессы управления. 2014. № 2. С. 5–11.
3. Mohan M.T. p -almost Hadamard matrices and λ -planes // *Journal of Algebraic Combinatorics*. 2022. Vol. 55. Iss. 1. PP. 89–108. DOI:10.1007/s10801-020-00991-y
4. Mironovsky L.A., Slaev V.A. *Strip-Method for Image and Signal Transformation*. Berlin, Boston: De Gruyter, 2011. 166 p. DOI:10.1515/9783110252569
5. Seberry J., Wysocki B.J., Wysocki T.A. On some applications of Hadamard matrices // *Metrika*. 2005. Vol. 62. Iss. 2-3. PP. 221–239. DOI:10.1007/s00184-005-0415-y
6. Wang R. *Introduction to Orthogonal Transforms: With Applications in Data Processing and Analysis*. Cambridge: Cambridge University Press, 2010. 504 p.
7. Balonin N., Vostrikov A., Sergeev M. Mersenne-Walsh Matrices for Image Processing // *Proceedings of the 8th International KES Conference on Intelligent Interactive Multimedia: Systems and Services (KES-IIMSS-15, Sorrento, Italy, 17–19 June 2015)*. *Smart Innovation, Systems and Technologies*. Vol. 40. Cham: Springer, 2015. PP. 141–147. DOI: 10.1007/978-3-319-19830-9_13
8. Сергеев М.Б., Ненашев В.А., Сергеев А.М. Вложенные кодовые конструкции Баркера – Мерсенна – Рагхаварао // Информационно-управляющие системы. 2019. № 3(100). С. 71–81. DOI:10.31799/1684-8853-2019-3-71-81
9. Балонин Н.А., Сергеев М.Б. Матрица золотого сечения G_{10} // Информационно-управляющие системы. 2013. № 6(67). С. 2–5.
10. Balonin N.A., Vostrikov A.A., Sergeev M.B. On two predictors of calculable chains of quasi-orthogonal matrices // *Automatic Control and Computer Sciences*. 2015. Vol. 49. Iss. 3. PP. 153–158. DOI:10.3103/S0146411615030025
11. Сергеев А.М. О взаимосвязи одного вида квазиортогональных матриц, построенных на порядках последовательностей $4k$ и $4k-1$ // Известия СПбГЭТУ ЛЭТИ. 2017. № 7. С. 12–17.
12. Sergeev A., Sergeev M., Balonin N., Vostrikov A. Symmetry Indices as a Key to Finding Matrices of Cyclic Structure for Noise-Immune Coding // *Proceedings of the 12th KES International Conference on Intelligent Decision Technologies (KES-IDT 2020, 17–19 June 2020)*. *Smart Innovation, Systems and Technologies*. Vol. 193. Singapore: Springer, 2020. PP. 223–230. DOI:10.1007/978-981-15-5925-9_19
13. Ryser H.J. *Combinatorial Mathematics*. New York: John Wiley, 1963. 162 p.
14. Балонин Н.А., Сергеев М.Б. Расширение гипотезы Райзера на двуциклические структуры и разрешимость матриц Адамара орнаментом в виде бицикла с двойной каймой // Информационно-управляющие системы. 2017. № 1(86). С. 2–10. DOI:10.15217/issnl684-8853.2017.1.2
15. Балонин Н.А., Сергеев М.Б. К вопросу существования матриц Мерсенна и Адамара // Информационно-управляющие системы. 2013. № 5(66). С. 2–8.
16. Sergeev A., Sergeev M., Vostrikov A., Kurtyanik D. Portraits of Orthogonal Matrices as a Base for Discrete Textile Ornament Patterns // *Smart Innovation, Systems and Technologies*. 2019. Vol. 143. P. 135 – 143. DOI:10.1007/978-981-13-8303-8_12
17. Зенкин В.И. Распределение простых чисел: элементарные методы. Калининград, 2008. URL: http://regiomontan.ru/book/VZ_primes.pdf (дата обращения 14.08.2022)
18. Hall M., Jr. A Survey of Difference Sets // *Proceedings of the American Mathematical Society*. 1956. Vol. 7. Iss. 6. PP. 975–986. DOI:10.2307/2033024
19. One circulant Mersenne Matrices // *Mathscinet*. URL: <http://mathscinet.ru/catalogue/CM1> (дата обращения 14.08.2022)
20. Vostrikov A., Sergeev A., Balonin Y. Using Families of Extremal Quasi-Orthogonal Matrices in Communication Systems // *Proceedings of the 13th KES Conference on Intelligent Decision Technologies (KES-IDT 2021, 14–16 June 2020)*. *Smart Innovation, Systems and Technologies*. Vol. 238. Singapore: Springer, 2021. PP. 95–108. DOI:10.1007/978-981-16-2765-1_8
21. Востриков А.А., Чернышев С.А. Об оценке устойчивости к искажениям изображений, маскированных М-матрицами // Научно-технический вестник информационных технологий, механики и оптики. 2013. № 5(87). С. 99–103.
22. Мироновский Л.А., Слаев В.А. Стрип-метод помехоустойчивого преобразования изображений // Измерительная техника. 2006. № 8. С. 6–12.
23. Balonin Y., Vostrikov A., Sergeev M. Software for finding M-matrices // *Frontiers in Artificial Intelligence and Applications*. 2014. Vol. 262. P. 475–480. DOI:10.3233/978-1-61499-405-3-475
24. Григорьев Е.К. Анализ корреляционных характеристик новых кодовых последовательностей, основанных на персимметричных квазиортогональных циркулянтах // Труды учебных заведений связи. 2022. Т. 8. № 2. С. 83–90. DOI:10.31854/1813-324X-2022-8-2-83-90
25. Roshan P., Leary J. 802.11 Wireless LAN Fundamentals. Cisco Press, 2004. 312 p.

References

1. Seberry J., Yamada M. *Hadamard Matrices: Constructions using Number Theory and Linear Algebra*. Hoboken: John Wiley & Sons; 2020. 352 p.
2. Balonin N.A., Sergeev M.B. The generalized Hadamard matrix norms. *Vestnik of Saint Petersburg University. Applied Mathematics. Computer Science. Control Processes*. 2014;2:5–11. (in Russ.)
3. Mohan M.T. p -almost Hadamard matrices and λ -planes. *Journal of Algebraic Combinatorics*. 2022;55(1):89–108. DOI:10.1007/s10801-020-00991-y

4. Mironovsky L.A., Slaev V.A. *Strip-Method for Image and Signal Transformation*. Berlin, Boston: De Gruyter; 2011. 166 p. DOI:10.1515/9783110252569
5. Seberry J., Wysocki B.J., Wysocki T.A. On some applications of Hadamard matrices. *Metrika*. 2005;62(2-3):221–239. DOI:10.1007/s00184-005-0415-y
6. Wang R. *Introduction to Orthogonal Transforms: With Applications in Data Processing and Analysis*. Cambridge: Cambridge University Press; 2010. 504 p.
7. Balonin N., Vostrikov A., Sergeev M. Mersenne-Walsh Matrices for Image Processing. *Proceedings of the 8th International KES Conference on Intelligent Interactive Multimedia: Systems and Services, KES-IIMSS-15, 17–19 June 2015, Sorrento, Italy. Smart Innovation, Systems and Technologies. vol.40*. Cham: Springer; 2015. p.141–147. DOI: 10.1007/978-3-319-19830-9_13
8. Sergeev M.B., Nenashev V.A., Sergeev A.M. Nested code sequences of Barker – Mersenne – Raghavarao. *Informatsionno-upravliaiushchie sistemy*. 2019;3(100):71–81. (in Russ.) DOI:10.31799/1684-8853-2019-3-71-81
9. Balonin N.A., Sergeev M.B. Golden ratio Matrix G_{10} . *Informatsionno-upravliaiushchie sistemy*. 2013;6(67):2–5. (in Russ.)
10. Balonin N.A., Vostrikov A.A., Sergeev M.B. On two predictors of calculable chains of quasi-orthogonal matrices. *Automatic Control and Computer Sciences*. 2015;49(3):153–158. DOI:10.3103/S0146411615030025
11. Sergeev A.M. The interconnection of one kind of quasi-orthogonal matrices built on the orders of sequences 4k and 4k – 1. *Proceedings of Saint Petersburg Electrotechnical University*. 2017;7:12–17. (in Russ.)
12. Sergeev A., Sergeev M., Balonin N., Vostrikov A. Symmetry Indices as a Key to Finding Matrices of Cyclic Structure for Noise-Immune Coding. *Proceedings of the 12th KES International Conference on Intelligent Decision Technologies, KES-IDT 2020, 17–19 June 2020. Smart Innovation, Systems and Technologies. vol.193*. Singapore: Springer; 2020. p. 223–230. DOI:10.1007/978-981-15-5925-9_19
13. Ryser H.J. *Combinatorial Mathematics*. New York: John Wiley; 1963. 162 p.
14. Balonin N.A., Sergeev M.B. Ryser's Conjecture Expansion for Birculant Strictures and Hadamard Matrix Resolvability by Double-Border Bicycle Ornament. *Informatsionno-upravliaiushchie sistemy*. 2017;1(86):2–10. (in Russ.) DOI:10.15217/issn1684-8853.2017.1.2
15. Balonin N.A., Sergeev M.B. To the question of the existence of Mersenne and Hadamard matrices. *Informatsionno-upravliaiushchie sistemy*. 2013;5(66):2–8. (in Russ.)
16. Sergeev A., Sergeev M., Vostrikov A., Kurtyanik D. Portraits of Orthogonal Matrices as a Base for Discrete Textile Ornament Patterns. *Smart Innovation, Systems and Technologies*. 2019. Vol. 143. P. 135 – 143. DOI:10.1007/978-981-13-8303-8_12
17. Zenkin V.I. *Prime number distribution: Elementary methods*. Kaliningrad; 2008. (in Russ.) URL: http://regiomont-tan.ru/book/VZ_primes.pdf [Accessed 14th August 2022]
18. Hall M., Jr. A Survey of Difference Sets. *Proceedings of the American Mathematical Society*. 1956;7(6):975–986. DOI:10.2307/2033024
19. Mathscinet. *One circulant Mersenne Matrices*. URL: <http://mathscinet.ru/catalogue/CM1> [Accessed 14th August 2022]
20. Vostrikov A., Sergeev A., Balonin Y. Using Families of Extremal Quasi-Orthogonal Matrices in Communication Systems. *Proceedings of the 13th KES Conference on Intelligent Decision Technologies, KES-IDT 2021, 14–16 June 2020. Smart Innovation, Systems and Technologies. vol.238*. Singapore: Springer; 2021. p.95–108. DOI:10.1007/978-981-16-2765-1_8
21. Vostrikov A., Chernyshev S. On distortion assessment of images masking with M-matrices. *Scientific and Technical Journal of Information Technologies, Mechanics and Optics*. 2013;5(87):99–103. (in Russ.)
22. Mironovsky L.A., Slaev V.A. The strip method of noise-immune image transformation. *Measurement Techniques*. 2006;49:745–754. (in Russ.) DOI:10.1007/s11018-006-0183-8
23. Balonin Y., Vostrikov A., Sergeev M. Software for finding M-matrices. *Frontiers in Artificial Intelligence and Applications*. 2014;262:475–480. DOI:10.3233/978-1-61499-405-3-475
24. Grigoriev E. Study of Correlation Properties of New Code Sequences Based on Persymmetric Quasi-Orthogonal Circulants. *Proc. of Telecom. Universities*. 2022;8(2):83–90. (in Russ.) DOI:10.31854/1813-324X-2022-8-2-83-90
25. Roshan P., Leary J. *802.11 Wireless LAN Fundamentals*. Cisco Press; 2004. 312 p.

Статья поступила в редакцию 23.09.2022; одобрена после рецензирования 14.10.2022; принята к публикации 19.10.2022.

The article was submitted 23.09.2022; approved after reviewing 14.10.2022; accepted for publication 19.10.2022.

Информация об авторе:

СЕРГЕЕВ
Александр Михайлович

кандидат технических наук, доцент кафедры вычислительных систем и сетей Санкт-Петербургского государственного университета аэрокосмического приборостроения

 <https://orcid.org/0000-0002-4788-9869>

ЭЛЕКТРОНИКА, ФОТОНИКА, ПРИБОРОСТРОЕНИЕ И СВЯЗЬ

**2.2.6 – Оптические
и оптико-электронные приборы
и комплексы**

**2.2.13 – Радиотехника, в том числе системы
и устройства телевидения**

**2.2.14 – Антенны, СВЧ-устройства
и их технологии**

**2.2.15 – Системы, сети и устройства
телекоммуникаций**

2.2.16 – Радиолокация и радионавигация

Научная статья

УДК 621.372.632

DOI:10.31854/1813-324X-2022-8-4-21-27



Реализация алгоритма начальной синхронизации демодулятора сигналов с прямым расширением спектра на основе быстрого преобразования Фурье. Часть 1. Постановка задачи и подход к решению

Ефим Александрович Брусин, yefim07@inbox.ru

АО «Российский институт радионавигации и времени»,
Санкт-Петербург, 192012, Российская Федерация
Санкт-Петербургский государственный университет телекоммуникаций им. М.А. Бонч-Бруевича,
Санкт-Петербург, 193232, Российская Федерация

Аннотация: Работа посвящена проблеме начальной синхронизации демодуляторов сигналов с прямым расширением спектра (Direct Spread Spectrum Signals). Как правило, для каналов связи, в которых используются указанные сигналы, характерны значительные сдвиги по задержке и значительные изменения несущей частоты. Поэтому данная проблема является наиболее существенной при построении аппаратуры приема. В работе предлагаются подход к реализации алгоритма начальной синхронизации на основе использования методов быстрого преобразования Фурье и обсуждаются результаты моделирования предложенного алгоритма.

Ключевые слова: прямое расширение спектра, начальная синхронизация, быстрое преобразование Фурье

Ссылка для цитирования: Брусин Е.А. Реализация алгоритма начальной синхронизации демодулятора сигналов с прямым расширением спектра на основе быстрого преобразования Фурье. Часть 1. Постановка задачи и подход к решению // Труды учебных заведений связи. 2022. Т. 8. № 4. С. 21–27. DOI:10.31854/1813-324X-2022-8-4-21-27

Direct Sequence Spread Spectrum Signal's Demodulator Acquisition Implementation Based on Fast Fourier Transform. Part 1. Problem Statement and Solution Approach

Ефим Брусин, yefim07@inbox.ru

Russian Institute of Radionavigation and Time,
St. Petersburg, 192012, Russian Federation
The Bonch-Bruevich Saint-Petersburg State University of Telecommunications,
St. Petersburg, 193232, Russian Federation

Abstract: The article is dedicated to direct sequence spread spectrum signals acquisition. Communication channels that use direct sequence spread spectrum signals are characterized by significant delay and carrier frequency shift as a rule. That's why the acquisition is most significant problem in receive equipment design. Suggested approach to acquisition problem base on the Fast Fourier Transform and discussed modeling suggested algorithm's results.

Keywords: direct sequence spread spectrum signals, acquisition, Fast Fourier Transform

For citation: Brusin E. Direct Sequence Spread Spectrum Signal's Demodulator Acquisition Implementation Based on Fast Fourier Transform. Part 1. Problem Statement and Solution Approach. *Proc. of Telecom. Universities*. 2022;8(4):21–27. (in Russ.) DOI:10.31854/1813-324X-2022-8-4-21-27

Постановка задачи

Под начальной синхронизацией (*от англ.* acquisition) при приёме сигналов с прямым расширением спектра понимается оценивание несущей частоты и задержки принимаемого сигнала.

Традиционно процедура начальной синхронизации сводится к поиску максимума по несущей частоте и задержке в наборе корреляторов [1]. Алгоритм поиска сводится к последовательной проверке всех возможных комбинаций временного и частотного сдвигов. При значительном диапазоне поиска по несущей частоте возникает проблема роста количества корреляторов, необходимых для реализации начальной синхронизации. Процедура поиска может быть реализована последовательно с использованием одного коррелятора, но в таком случае критически растёт время начальной синхронизации демодулятора.

В последнее время представляется актуальным подход, основанный на использовании быстрого преобразования Фурье (БПФ) [2–4]. Основное преимущество этого подхода состоит в возможности совместного оценивания параметров сигнала в частотной и во временной области. Следует также заметить, что интерес к использованию методов, построенных на основе БПФ, обусловлен появившейся возможностью реализации вычислений преобразования Фурье в реальном масштабе времени [5–8].

Некоторые подходы к реализации процедур начальной синхронизации с использованием преобразования Фурье представлены в [9]. Однако ввиду ограниченного формата работы проблемы реализации алгоритма и анализ его эффективности изложены там весьма кратко.

В связи с этим, представляется целесообразным более подробно описать собственно алгоритм начальной синхронизации с точки зрения реализации последнего на базе БПФ, а также провести анализ эффективности предложенного алгоритма.

Реализация начальной синхронизации

Будем рассматривать сигнал двухпозиционной фазовой модуляции (ФМ-2). Традиционно модель сигнала включает в себя умножение на сигнатуру (расширяющую спектр последовательность) $s_k(t)$:

$$s_k(t; b_k) = s_k(t) \cdot B_k(t) \cdot \cos(2\pi f_0 t),$$

где $B_k(t) = b_{k,i} = \pm 1$ – информационные символы, передаваемые на интервалах $(i-1)T_b < t \leq T_b$; T_b – длительность информационного символа (бита); f_0 – номинальное значение частоты несущего колебания.

Упрощенная схема формирования сигнала с прямым расширением спектра представлена на рисунке 1.

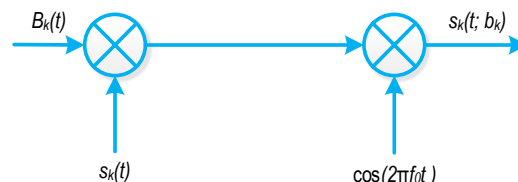


Рис. 1. Формирование сигнала с прямым расширением спектра

Fig. 1. Direct Spread Spectrum Signal Generation

Передаваемые данные умножаются на расширяющую спектр последовательность (далее просто расширяющая последовательность); это называется процедурой расширения спектра (*от англ.* spreading). Сформированный таким образом сигнал переносится на несущую частоту.

Принимаемый сигнал можно представить в виде:

$$\tilde{s}_k(t; b_k) = s_k(t - \tau_k) \cdot B_k(t - \tau_k) \times \cos(2\pi(f_0 + f)t + \varphi_k) + n_\tau(t),$$

где τ_k – задержка в канале; f – смещение частоты несущего колебания относительно заданного номинального значения; φ_k – фаза несущей частоты; $n_\tau(t)$ – отсчеты шума.

Упрощенная схема приема сигнала с прямым расширением спектра представлена на рисунке 2.

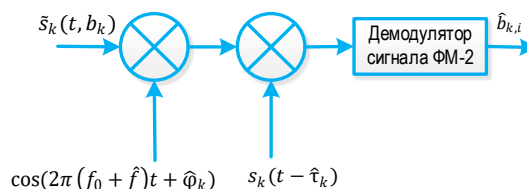


Рис. 2. Прием сигнала с прямым расширением спектра

Fig. 2. Direct Spread Spectrum Signal Receiving

Принимаемый сигнал смещается по несущей частоте, умножается на синхронизируемую неким образом расширяющую последовательность (*от англ.* dispreading), после чего поступает на вход демодулятора сигнала ФМ-2. $\hat{\tau}_k, \hat{\varphi}_k$ и $\hat{f}$ на рисунке 2 – полученные оценки соответствующих параметров принимаемого сигнала, $\hat{b}_{k,i}$ – принимаемые символы.

Задача начальной синхронизации сводится к оцениванию смещения частоты несущего колебания принимаемого сигнала относительно заданного номинального значения и определение смещения расширяющей последовательности относительно сформированной на приеме.

Предлагаемый подход основан на эквивалентности операции дискретной свертки сигналов во «временной» области (области сигнала) умножению одноименных спектральных составляющих сигналов с последующим вычислением обратного преобразования Фурье полученного произведения для обратного перехода в сигнальную область. Действительно, если вычисление корреляции трактовать как свертку принимаемого сигнала с заданной корреляционной последовательностью, то коррелятор может быть реализован в частотной области.

Пусть N – длина расширяющей последовательности. Вычислив преобразование Фурье длины N принимаемого сигнала на некоторой несущей частоте $f_0 + \hat{f}$, умножим его на заранее полученное комплексно-сопряженное преобразование Фурье от сигнатуры. Затем достаточно вычислить обратное преобразование Фурье от этого произведения. В результате получим искомый корреляционный пик на выделенной частоте несущего колебания $f_0 + \hat{f}$.

Таким образом, для реализации начальной синхронизации в полосе частотной неопределенности принимаемого сигнала по несущей частоте необходимо вычислить M прямых преобразований Фурье на частотах $f_0 \pm m\Delta f$, где Δf – шаг сетки частот.

Здесь M определяется следующим образом:

$$M = \lfloor \cdot \rfloor \frac{\Delta F}{\Delta f},$$

где ΔF – диапазон частотной неопределенности принимаемого сигнала по несущей частоте; $\lfloor \cdot \rfloor$ – усечение до целого, а m , соответственно, меняется от $-M/2$ до $M/2$.

Затем каждое из полученных преобразований Фурье умножается на комплексно-сопряженное от корреляционной последовательности. После этого вычисляются M обратных преобразований Фурье от этих произведений. Модули указанных обратных преобразований формируют набор из M корреляционных пиков, который в совокупности даст функцию неопределенности (*от англ. ambiguity function*) принимаемого сигнала. Найдя максимум этой функции как по частоте, так и по длине преобразования Фурье, получим оценки несущей частоты и смещения принимаемого сигнала по отношению к заданной расширяющей последовательности.

Таким образом, предлагаемый алгоритм состоит в следующем. Формируется опорная последовательность. В буфер БПФ записываются отсчеты одного периода расширяющей последовательности:

$$r_n = s_k(t_n) + js_k(t_n),$$

где $n = 0, 1, \dots, N - 1$; N – длина преобразования Фурье.

Будем полагать, что частота следования отсчетов сигнала $s_k(t_n)$ равна удвоенной частоте следования символов расширяющей последовательности (удвоенной чиповой частоте). Если длина преобразования Фурье больше удвоенной длины расширяющей последовательности, то оставшиеся отсчеты буфера заполняются нулями. Вычисляются отсчеты преобразования Фурье опорного сигнала:

$$\hat{R}_l = R_l^*,$$

где R_l^* – комплексно-сопряженные отсчеты преобразования Фурье r_n , $l = 0, 1 \dots N - 1$.

Затем вычисляется преобразование Фурье принимаемого сигнала. Отсчеты преобразования умножаются на соответствующие отсчеты $\hat{R}_l$. Вычисляются обратные преобразования Фурье и образуется набор корреляционных пиков, которые фактически формируют функцию неопределенности принимаемого сигнала.

В основном суть предлагаемого подхода изложена в работе [9]. В представленной работе представляется целесообразным более подробно остановиться на практической реализации алгоритма и результатах моделирования процедуры начальной синхронизации.

Моделирование проводилось для следующего сигнала: длительность информационного символа $T_b = 50$ мкс (что соответствует информационной скорости 20 кбит/с), вид модуляции – ФМ-2, диапазон поиска по несущей частоте ± 40 кГц ($\Delta F = 80$ кГц). Шаг Δf устанавливается равным четверти от информационной скорости:

$$\Delta f = \frac{1}{4T_b}.$$

То есть в рассматриваемом случае:

$$M = \lfloor \cdot \rfloor 4T_b \Delta F = 16.$$

Соответственно m будет изменяться в диапазоне:

$$m = -8, \dots, -1, 0, 1, \dots, 8.$$

Для формирования расширяющей последовательности используются последовательности Голда исходной длины 2047, укороченные до 2046. С учетом выбранных параметров расширение спектра (*от англ. spreading factor*) составляет 2046. Таким образом, частота следования символов (чипов) равна $f_{chip} = 40,92$ МГц. Отношение сигнал/шум на чип изменялось от -30 до 0 дБ. Моделирование проводилось на удвоенной частоте чипов. То есть частота дискретизации анализируемого сигнала составляла 81,84 МГц.

В ходе моделирования вычислялись вероятность обнаружения и нормированная дисперсия оценок несущей частоты:

$$P_d = \frac{1}{N_p} \sum_{i=0}^{N_p-1} P_i,$$

$$(\sigma_f T_b)^2 = \frac{1}{N_p} \sum_{i=0}^{N_p-1} [(\hat{f}_{c0} - f) \cdot T_b]^2,$$

где $\hat{f}_{c0}$ – оценка смещения несущей частоты;

N_p – количество попыток реализации алгоритма начальной синхронизации,

$P_i = 1$, если $L_f = \tilde{L}_f$, и $P_i = 0$, если $L_f \neq \tilde{L}_f$,

$\tilde{L}_f$ – правильное, априорно известное значение смещения временной позиции на приеме.

На первом этапе интервал наблюдения составил один информационный символ – $K = 1$ (здесь и далее K – выражен в символах принимаемого сигнала). При каждом отношении проводилось 100 попыток реализации алгоритма. Соответственно длина сформированной опорной последовательности и БПФ составила 4092. Моделирование проводилось для различных значений $\tilde{L}_f$. Зависимость усредненной вероятности обнаружения сигнала от отношения сигнал/шум на чип представлена на рисунке 3.

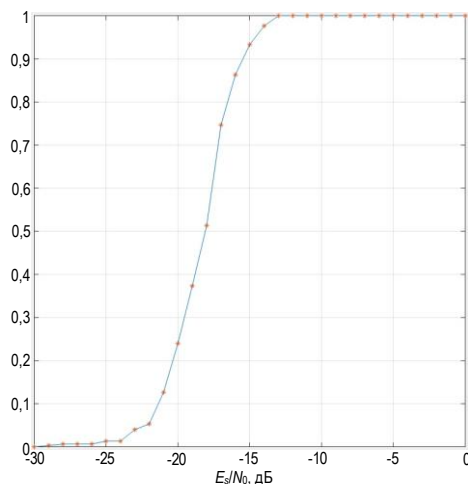


Рис. 3. Вероятность обнаружения. $N = 4092$

Fig. 3. Detection probability. $N = 4092$

Зависимость соответствующей дисперсии оценок несущей частоты от отношения E_s/N_0 представлена на рисунке 4. Показанные зависимости получены при усреднении результатов моделирования для $\tilde{L}_f = 12, 2196$ и 4087 .

Следует отметить, что предлагаемый алгоритм обеспечивает вероятность обнаружения, близкую к единице при E_s/N_0 больше -12 дБ. Получаемая при этом дисперсия оценок ограничена шагом сетки частот. Действительно, при $\Delta f T_b = 0,25$ получаем нормированную дисперсию $(\sigma_f T_b)^2 \sim (\Delta f T_b)^2$. Понятно, что для начальной синхронизации при меньших отношениях сигнал/шум интервал наблюдения необходимо увеличить. Проанализируем предлагаемый алгоритм для $K = 2, 4$ и 8 .

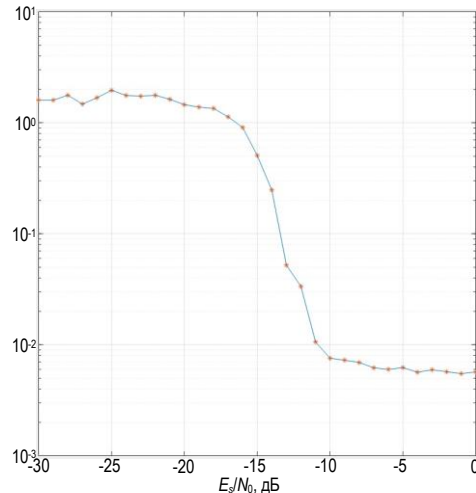


Рис. 4. Дисперсия оценки несущей частоты. $N = 4092$

Fig. 4. Carrier frequency variance. $N = 4092$

Соответственно длины сформированных опорных последовательностей $\hat{R}_l$ и длины преобразований Фурье составили 8184, 16368 и 32736. При $K = 2$ вычислялись M преобразований Фурье. Для $K = 4$ и 8 вычисляется одно прямое преобразование Фурье вида:

$$\tilde{s}_{ml} = \sum_{n=0}^{N-1} \tilde{s}_k(t_n; b_k) \cdot e^{-j2\pi f_0 t_n} \cdot e^{-j\frac{2\pi n l}{N}}. \quad (1)$$

Переносы по несущей частоте осуществляются за счет смещения по оси частот компонент преобразования (1). Для всех K после умножения на отсчеты опорного сигнала вычисляются модули обратного преобразования Фурье $|s_{ml}|$ и проводится усреднение вида:

$$\langle |s_{ml}| \rangle = \frac{1}{K} \sum_{k=0}^{K-1} |s_{m,l+k \cdot N}|, \quad (2)$$

где K – число усреднений, в нашем случае 2, 4 и 8, $l = 0, 1, \dots, N-1$.

На основании (2) вычисляется усредненная функция неопределенности:

$$\bar{\rho}(m, l) = \langle |s_{ml}| \rangle,$$

и правило (3) переписывается в виде:

$$\{M_f, L_f\} = \arg \left\{ \max_{m,l} \bar{\rho}(m, l) \right\}. \quad (3)$$

В качестве иллюстрации рассматриваемого подхода на рисунке 5а слева представлены отсчеты модуля обратного преобразования Фурье $|s_{ml}|$, полученные по результатам моделирования для $K = 2$ при $E_s/N_0 = -15$ дБ. Соответствующие отсчеты усредненного модуля обратного БПФ (2) $\langle |s_{ml}| \rangle$ представлены слева на рисунке 5б. На рисунке 5с изображена усредненная функция неопределенности $\bar{\rho}(m, l)$. Аналогичные результаты моделирования для $K = 8$ при $E_s/N_0 = -10$ дБ приведены справа на рисунках 5а–5с.

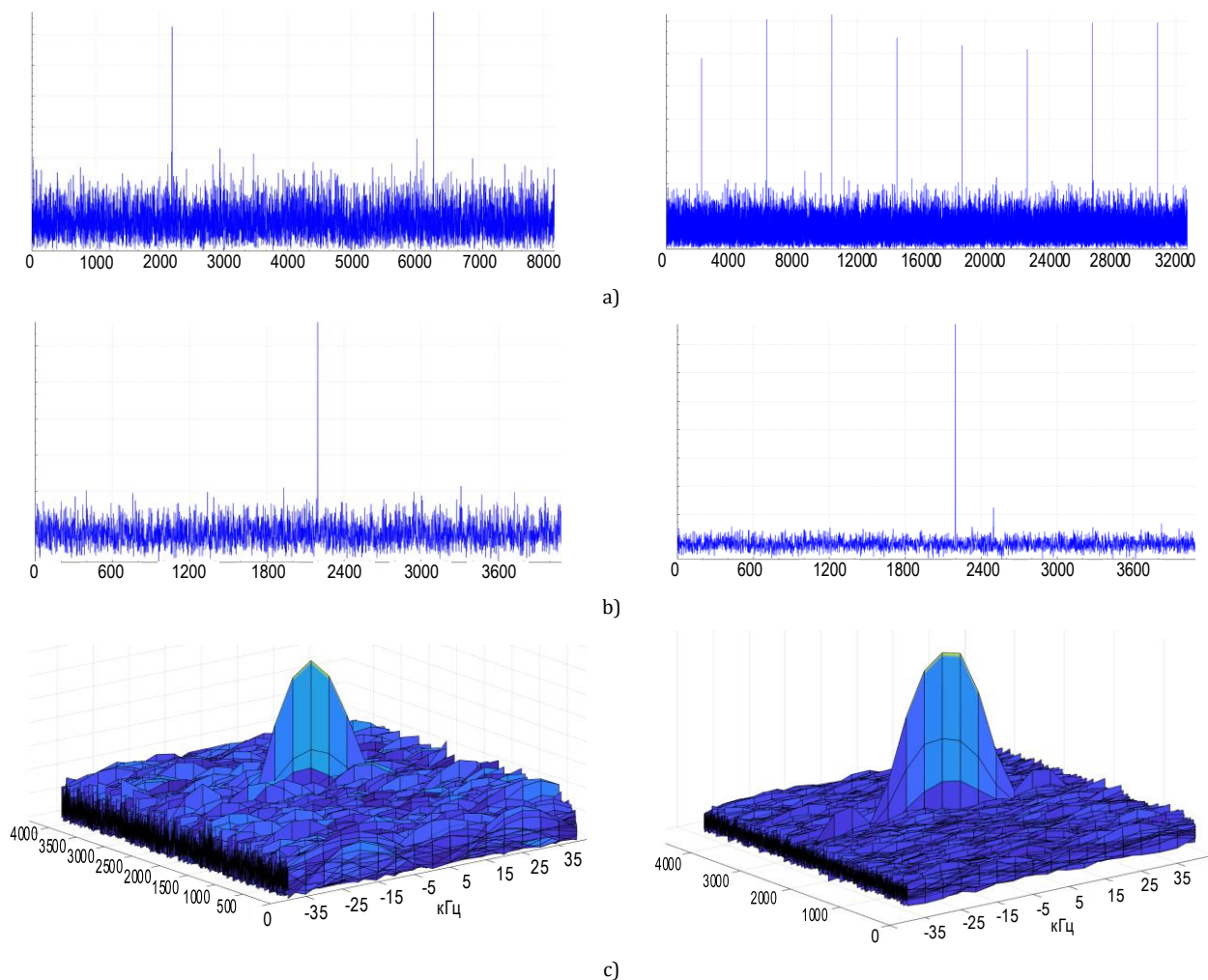


Рис. 5. Результаты моделирования: а) $|s_{ml}|$, б) $\langle |s_{ml}| \rangle$, в) $\bar{p}(m, l)$

Fig. 5. Results of Modeling: а) $|s_{ml}|$, б) $\langle |s_{ml}| \rangle$, в) $\bar{p}(m, l)$

Для оценки эффективности предложенного алгоритма начальной синхронизации проведено компьютерное моделирование процедуры. Отношение сигнал/шум на чип E_s/N_0 менялось от -30 до 0 дБ с шагом 1 дБ. На передающей стороне устанавливалось случайное смещение временной позиции сигнала по отношению к опорной расширяющей последовательности и случайное значение смещения по несущей частоте. На приемной стороне вычислялось смещение несущей частоты принимаемого сигнала относительно заданного номинального значения и определялось смещение принимаемого сигнала относительно сигнатуры, сформированной на приеме. Как и для $K = 1$, по результатам моделирования вычислялись $(\sigma_f T_b)^2$ и P_d . Результаты моделирования для $K = 8$ (длина БПФ 32736) представлены на рисунках 6 и 7.

На них приведены зависимости вероятности обнаружения и дисперсии оценок несущей частоты от отношения сигнал/шум на чип. Указанные зависимости получены путем усреднения выявленных по результатам моделирования результа-

тов для трех значений $\tilde{L}_f$. Увеличение интервала наблюдения, как и следовало ожидать, «сдвигает» зависимости влево. При этом получаемая нормированная дисперсия оценки также ограничена шагом сетки частот Δf .

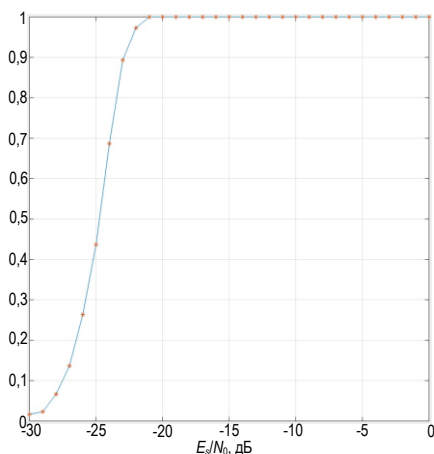
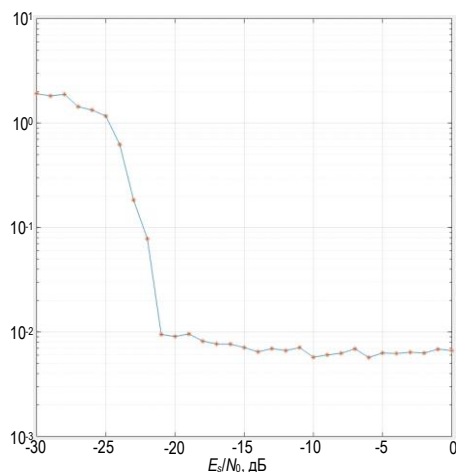


Рис. 6. Вероятность обнаружения. $N = 32736$

Fig. 6. Detection Probability. $N = 32736$

Рис. 7. Дисперсия оценки несущей частоты. $N = 32736$ Fig. 7. Carrier Frequency Variance. $N = 32736$

Предварительные выводы

Предложенный подход позволяет реализовать начальную синхронизацию демодулятора сигналов с прямым расширением спектра в параллельном режиме. В свою очередь, традиционный метод начальной синхронизации требует реализацию последовательного поиска по всем позициям расширяющей последовательности в каждом из частотных каналов.

Фактически, процедура начальной синхронизации, рассматриваемая в настоящей работе, решает задачу совместного оценивания несущей частоты и определение смещения принимаемого сигнала по отношению к началу заданной расширяющей последовательности.

Реализация алгоритма сводится к накоплению выборки K интервалов принимаемого сигнала и последовательному вычислению набора прямых и обратных преобразований Фурье. На основании указанных вычислений строится функция неопределенности, поиск максимума которой дает оценку несущей частоты и задержки. С точки зрения вычислительных затрат именно вычисление БПФ вносит основной вклад во временные затраты на процедуры оценивания.

В частности, для реализации алгоритма при $K = 8$ вычисляется одно прямое и семнадцать обратных преобразований Фурье. То есть, реализация процедуры начальной синхронизации при $K = 8$ требует всего 18 вычислений БПФ длиной

32736; иными словами, требует 18 вычислений преобразования Фурье относительно небольшой длины. Например, сигнальный процессор фирмы Texas Instruments типа TMS320C6678 при использовании одного вычислительного ядра реализует БПФ длиной 32768 за время порядка 1 миллисекунды [8].

Понятно, что при использовании современных аппаратных средств вычисление преобразований Фурье на сигнальных процессорах или элементах программируемой логики, предложенный алгоритм начальной синхронизации реализуется практически в реальном масштабе времени.

Результаты моделирования, приведенные в работе, показывают высокую эффективность предложенных процедур начальной синхронизации.

Алгоритм при достаточно небольших длинах БПФ обеспечивает вероятность обнаружения, близкую к единице, при уменьшении отношения сигнал/шум на чип до -20 дБ. Соответственно, начальная частотная неопределенность по частоте несущего колебания $\Delta F = 4/T_b$ сводится к отклонению порядка $0,25/T_b$. Иначе говоря, начальная частотная неопределенность ΔF , равная 4 информационным скоростям, «сжимается» в результате реализации предложенной процедуры до одной четверти информационной скорости. То есть, «сжимается» в 16 раз.

В этой связи следует особо подчеркнуть, что предложенный подход особо эффективен при значительной неопределенности принимаемого сигнала по несущей частоте. В частности, в каналах связи с существенным доплеровским смещением.

Подводя итог проведенным исследованиям, можно сделать следующие выводы;

- предложен алгоритм начальной синхронизации демодулятора сигналов с прямым расширением спектра, реализованный на основе быстрого преобразования Фурье;
- анализ, проведенный методами компьютерного моделирования, показывает высокую эффективность предложенного алгоритма;
- применение современных аппаратных средств обеспечивает реализацию процедуры начальной синхронизации в реальном масштабе времени.

Продолжение следует...

Список источников

1. Ipatov V.P. Spread Spectrum and CDMA. Principles and Applications. John Wiley & Sons, 2005.
2. Almeida A.P., Dinis R., Cercas F.B. An FFT-based Acquisition Scheme for DS-CDMA Systems // Proceedings of the International Symposium on Communication and Information Technologies (Sydney, Australia, 17–19 October 2007). IEEE, 2007. DOI:10.1109/ISCIT.2007.4392144
3. Liu N.Q., Sun B., Guan C. Research on An Improved PMF-FFT Fast PN Code Acquisition Algorithm // Communications and Network. 2013. Vol. 5. PP. 266–270. DOI:10.4236/cn.2013.53B2049

4. Guo L.L., Sun Z.G., Chen S., Wang B.C., Ning X.Y. Research on Time-Frequency Domain Acquisition Algorithm of Parallel Combinatory Spread Spectrum System Based on FFT // Proceedings of the International Conference on Computer Information Systems and Industrial Applications (CISIA 2015, Bangkok, Thailand, 28–29 June 2015). Advances in Computer Science Research. Vol. 18. Atlantis Press, 2015. DOI:10.2991/cisia-15.2015.5
5. Костров В.В., Ракитин А.В., Сидоров А.А. Повышение вычислительной эффективности алгоритмов выполнения БПФ при их реализации на ПЦОС семейства «Мультикор» // Радиотехнические и телекоммуникационные системы. 2011. № 1. С. 59–62.
6. Li X., Blinka E. Very large FFT for TMS320C6678 processors // Texas Instruments. 2015 URL: https://www.ti.com/lit/wp/spry277/spry277.pdf?ts=1668435787405&ref_url=https%253A%252F%252Fwww.google.com%252F (дата обращения 08.10.2021)
7. Application Report SPRACN4 (2019-08). Using DSPLIB FFT Implementation for Real Input and Without Data Scaling // Texas Instruments. URL: https://www.ti.com/lit/an/spracn4/spracn4.pdf?ts=1668396727839&ref_url=https%253A%252F%252Fwww.google.com.hk%252F (дата обращения 08.10.2021)
8. Гребенников А. Модуль быстрого преобразования Фурье // Современная электроника. 2012. № 7. С. 62–67.
9. Брусин Е.А. Начальная синхронизация демодулятора сигнала с прямым расширением спектра с использованием быстрого преобразования Фурье // 11-я Международная научно-техническая и научно-методическая конференция «Актуальные проблемы инфотелекоммуникаций в науке и образовании» (АПИНО-2022, Санкт-Петербург, Россия, 15–16 февраля 2022). СПб.: СПбГУТ, 2022. Т. 2. С. 522–527.

References

1. Ipatov V.P. *Spread Spectrum and CDMA. Principles and Applications*. John Wiley & Sons; 2005.
2. Almeida A.P., Dinis R., Cercas F.B. An FFT-based Acquisition Scheme for DS-CDMA Systems. *Proceedings of the International Symposium on Communication and Information Technologies*, 17–19 October 2007, Sydney, Australia. IEEE; 2007. DOI:10.1109/ISCIT.2007.4392144
3. Liu N.Q., Sun B., Guan C. Research on An Improved PMF-FFT Fast PN Code Acquisition Algorithm. *Communications and Network*. 2013;5:266–270. DOI:10.4236/cn.2013.53B2049
4. Guo L.L., Sun Z.G., Chen S., Wang B.C., Ning X.Y. Research on Time-Frequency Domain Acquisition Algorithm of Parallel Combinatory Spread Spectrum System Based on FFT. *Proceedings of the International Conference on Computer Information Systems and Industrial Applications, CISIA 2015, 28–29 June 2015, Bangkok, Thailand. Advances in Computer Science Research. Vol. 18. Atlantis Press; 2015. DOI:10.2991/cisia-15.2015.*
5. Kostrov V.V., Rakitin A.V., Sidorov A.A. Increase of Computing Efficiency of Algorithms of Performance FFT at Their Realisation on PDSP Families "Multicore". *Radio and telecommunication systems*. 2011;1:59–62. (in Russ.)
6. Li X., Blinka E. Very large FFT for TMS320C6678 processors. *Texas Instruments*. 2015 URL: https://www.ti.com/lit/wp/spry277/spry277.pdf?ts=1668435787405&ref_url=https%253A%252F%252Fwww.google.com%252F [Accessed 08th October 2021]
7. Application Report SPRACN4 (2019-08). Using DSPLIB FFT Implementation for Real Input and Without Data Scaling. *Texas Instruments*. URL: https://www.ti.com/lit/an/spracn4/spracn4.pdf?ts=1668396727839&ref_url=https%253A%252F%252Fwww.google.com.hk%252F [Accessed 08th October 2021]
8. Grebennikov A. Fast Fourier Transform Module. *Sovremennaya elektronika*. 2012;7:62–67. (in Russ.)
9. Brusin E.A. Initial Timing of a Direct Spread Demodulator Using Fast Fourier Transform. *Proceedings of the XIth International Conference on Infotelecommunications in Science and Education*, 15–16 February 2022, St. Petersburg, Russia. St. Petersburg: The Bonch-Bruевич Saint-Petersburg State University of Telecommunications Publ., 2022. vol.2. p.522–527. (in Russ.)

Статья поступила в редакцию 23.09.2022; одобрена после рецензирования 02.11.2022; принята к публикации 10.11.2022.

The article was submitted 23.09.2022; approved after reviewing 02.11.2022; accepted for publication 10.11.2022.

Информация об авторе:

БРУСИН
Ефим Александрович

кандидат технических наук, руководитель проектного направления АО «Российский институт радионавигации и времени», доцент кафедры электроники и схемотехники Санкт-Петербургского государственного университета телекоммуникаций им. проф. М.А. Бонч-Бруевича,
 <https://orcid.org/0000-0002-6742-2705>

Научная статья

УДК 681.7.068.4

DOI:10.31854/1813-324X-2022-8-4-28-38



Многосердцевинное оптическое волокно со ступенчатыми одномодовыми сердцевинами. Часть 1. Изоляция сплошными оболочками

✉ Мария Сергеевна Былина, BylinaMaria@mail.ru

✉ Людмила Александровна Гульяева, lyudmila150@gmail.com

Санкт-Петербургский государственный университет телекоммуникаций им. М.А. Бонч-Бруевича, Санкт-Петербург, 193232, Российская Федерация

Аннотация: Оптическое волокно с несколькими несвязанными сердцевинами внутри общей оболочки (многосердцевинное волокно) применяется для увеличения пропускной способности линейных трактов систем связи. Количество сердцевины в одном волокне ограничивается взаимными влияниями между ними, для уменьшения которого применяются различные конструктивные решения. Целью работы является сравнение различных многосердцевинных волокон и выявление конструкций, позволяющих разместить наибольшее число сердцевины в общей оболочке стандартного диаметра 125 мкм.

В первой части данной работы проведено моделирование одномодовых волокон с сердцевинами, изолированными дополнительными сплошными оболочками. В результате моделирования рассчитаны характеристики фундаментальных мод сердцевины каждого из волокон – распределение напряженности электрического поля, хроматическая дисперсия и диаметр поля фундаментальной моды, предложена методика и проведена оценка взаимных влияний, определено максимальное возможное число сердцевины. Показано, что изолирующая оболочка снижает взаимные влияния и позволяет увеличить количество сердцевины за счет уменьшения расстояния между ними.

Ключевые слова: многосердцевинное волокно, одномодовая сердцевина, фундаментальная мода, взаимные влияния, перекрестные помехи, затухание перекрестных помех, моделирование

Ссылка для цитирования: Былина М.С., Гульяева Л.А. Многосердцевинное оптическое волокно со ступенчатыми одномодовыми сердцевинами. Часть 1. Изоляция сплошными оболочками // Труды учебных заведений связи. 2022. Т. 8. № 4. С. 28–38. DOI:10.31854/1813-324X-2022-8-4-28-38

Multi-Core Optical Fiber with Stepped Single-Mode Cores. Part 1. Insulation with Solid Clads

✉ Maria Bylina, BylinaMaria@mail.ru

✉ Ludmila Gulyaeva, lyudmila150@gmail.com

The Bonch-Bruevich Saint-Petersburg State University of Telecommunications, St. Petersburg, 193232, Russian Federation

Abstract: An optical fiber with several unrelated cores inside a common clad (multi-core fiber) is used to increase the capacity of linear paths of communication systems. The number of cores in one fiber is limited by mutual influences between them, to reduce which various design solutions are used. The aim of the work is to compare various multi-core fibers and identify structures that allow placing the largest number of cores in a common shell with a standard diameter of 125 microns.

In the first part of this paper, modeling of single-mode fibers with cores isolated by additional solid shells is carried out. As a result of modeling, the characteristics of the fundamental modes of the cores of each fiber are calculated – the distribution of the electric field strength, chromatic dispersion and the diameter of the field of the fundamental mode, a technique is proposed and an assessment of mutual influences is carried out, the maximum possible number of cores is determined. It is shown that the insulating clad reduces mutual influences and allows increasing the number of cores by reducing the distance between them.

Keywords: multi-core fiber, single-mode core, fundamental mode, mutual influences, crosstalk, crosstalk attenuation, simulation

For citation: Bylina M., Gulyaeva L. Multi-Core Optical Fiber with Stepped Single-Mode Cores. Part 1. Core Insulation with Solid Clads. *Proc. of Telecom. Universities*. 2022;8(4):28–38. (in Russ.) DOI:10.31854/1813-324X-2022-8-4-28-38

1. ВВЕДЕНИЕ

Общей тенденцией развития оптических сетей связи является увеличение объемов информации, передаваемой по одному одномодовому оптическому волокну (ОВ). Увеличение объемов может быть достигнуто за счет увеличения канальной скорости передачи и количества каналов при использовании технологии плотного спектрального мультиплексирования (DWDM, аббр. от англ. Dense Wavelength Division Multiplexing). В настоящее время канальные скорости передачи могут составлять $B = 100\text{--}800$ Гбит/с, а количество каналов в одном ОВ измеряется десятками. Однако в ряде случаев этого оказывается недостаточно. Ограничивающим фактором уже являются размеры самого ОВ.

Для увеличения пропускной способности предлагаются схемы пространственного мультиплексирования. Одним из вариантов его реализации является применение многосердцевинных волокон (МСВ) [1–3]. МСВ представляет собой оптическое волокно с несколькими несвязанными сердцевинами, объединенными общей оболочкой, диаметр которой составляет 125 мкм, то есть равен диаметру оболочки обычного телекоммуникационного волокна с одной сердцевиной [2–7]. Если сердцевинки имеют одинаковые параметры, то они могут использоваться для параллельной передачи информации.

Каждая сердцевина в МСВ является аналогом обычного одномодового световода, в котором может быть реализована любая из существующих технологий передачи информации.

Максимальная скорость передачи B_{tot} , реализуемая по МСВ, составляет:

$$B_{tot} = N_{core} \cdot B, \quad (1)$$

где B – скорость передачи информации по одной сердцевине МСВ, N_{core} – количество сердцевин.

Из (1) следует, что для повышения пропускной способности необходимо увеличивать число сердцевин N_{core} , которое при фиксированном диаметре

общей оболочки ограничено их взаимными влияниями.

Целью данной работы является сравнительный анализ различных конструкций МСВ, позволяющих разместить наибольшее число сердцевин внутри общей оболочки стандартного диаметра 125 мкм. Для этого необходимо, во-первых, предложить методику оценки взаимных влияний между сердцевинами МСВ; во-вторых, предложить критерий оценки минимально допустимого расстояния между соседними сердцевинами в МСВ, при котором достигается максимальное количество сердцевин; в-третьих, сравнить эффективность различных конструктивных решений, позволяющих уменьшить взаимные влияния между сердцевинами:

1) увеличение расстояния между ближайшими друг к другу сердцевинами, путем уменьшения числа сердцевин или изменения их взаимного расположения внутри общей оболочки;

2) формирование вокруг каждой сердцевины изолирующей оболочки с показателем преломления ниже показателя преломления общей оболочки [2, 3, 8];

3) формирование между соседними сердцевинами защитного барьера из воздушных капилляров [2, 3, 9].

В первой части работы рассмотрены МСВ с сердцевинами без изолирующей оболочки и с изолирующими оболочками различной толщины.

2. МЕТОДИКА ОЦЕНКИ ВЗАИМНЫХ ВЛИЯНИЙ МЕЖДУ СЕРДЦЕВИНАМИ В МСВ

2.1. Затухание перекрестной помехи

Взаимные влияния между сердцевинами МСВ будем характеризовать затуханием перекрестной помехи:

$$A = 10 \lg \left(\frac{P_s}{P_n} \right), \quad (2)$$

где P_s – мощность сигнала в подверженной влиянию сердцевине; P_n – суммарная мощность перекрестных помех, созданных всеми остальными сердцевинами.

Будем считать, что МСВ содержит N_{core} одинаковых сердцевин. Мощность сигнала P_s в каждой из них можно рассчитать по выражению:

$$P_s = \int_{S_1} I \cdot ds, \quad (3)$$

где I – интенсивность излучения фундаментальной моды; S_1 – область сердцевин, по которой осуществляется интегрирование.

Для оценки помехи P_n будем использовать соотношения:

$$P_n = \sum_{i=1}^{N_{core}-1} P_{ni}, \quad P_{ni} = \int_{S_2} I_i \cdot ds, \quad (4)$$

где $N_{core} - 1$ – число влияющих сердцевин; P_{ni} – мощность помехи, созданной i -й влияющей сердцевиной в сердцевине, подверженной влиянию; I_i – интенсивность излучения фундаментальной моды в i -й влияющей сердцевине; S_2 – область сердцевин, подверженной влиянию, по которой осуществляется интегрирование.

Из (3) и (4) следует, что для расчета A необходимо рассчитать интенсивность I поля фундаментальной моды каждой сердцевин МСВ, которая связана с напряженностью поля соотношением:

$$I = \frac{1}{2} \sqrt{\frac{\epsilon_a}{\mu_a}} \cdot E \cdot E^*, \quad (5)$$

где $\epsilon_a = \epsilon \cdot \epsilon_0$ и $\mu_a = \mu \cdot \mu_0$ – абсолютные диэлектрическая и магнитная проницаемости среды, в которой распространяется электромагнитная волна; ϵ и μ – относительные диэлектрическая и магнитная проницаемости этой среды; $\epsilon_0 = 8,85 \cdot 10^{-12}$ Ф/м и $\mu_0 = 1,257 \cdot 10^{-6}$ Гн/м – электрическая и магнитная постоянные; E^* – комплексно сопряженная к напряженности электрического поля величина.

2.2. Конструкция МСВ

Рассмотрим сначала простейшую конструкцию МСВ с двумя одинаковыми одномодовыми сердцевинами, расположенными на расстоянии h друг от друга. Каждая сердцевина имеет радиус r_1 и собственную изолирующую оболочку с радиусом r_2 (рисунок 1). Показатели преломления сердцевины и изолирующей оболочки обозначим n_1 и n_2 , соответственно. Сердцевины окружены общей оболочкой с радиусом r_3 и показателем преломления n_3 . Будем полагать, что показатели преломления в пределах сердцевин и оболочек не меняются.

Назначением изолирующей оболочки является уменьшение радиуса модового поля, и доли мощности фундаментальной моды, распространяющейся в общей оболочке, что должно снизить взаимные влияния.

Для достижения данного эффекта необходимо, чтобы выполнялось следующее соотношение между показателями преломления:

$$n_1 > n_3 \geq n_2. \quad (6)$$

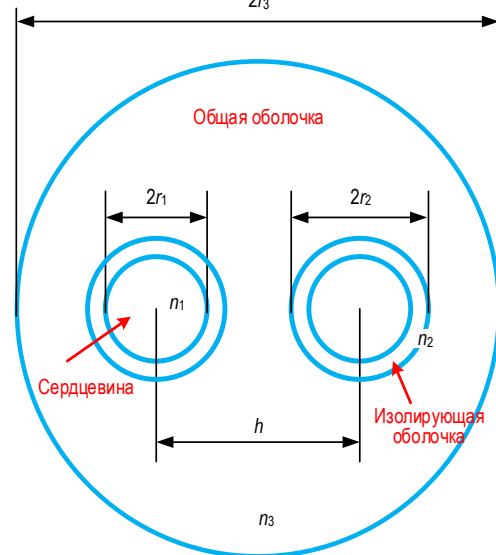


Рис. 1. Конструкция МСВ с двумя сердцевинами в изолирующих оболочках

Fig. 1. The Design of the MCF with Two Cores in Insulating Clads

Очевидно, что волновод, образованный сердцевиной и двумя оболочками – изолирующей и общей, имеет профиль показателя преломления (ППП), отличный от волновода, образованного сердцевиной и одной общей оболочкой. Поэтому их оптические характеристики будут отличаться. Это нужно учитывать при выборе параметров изолирующей оболочки (показателя преломления n_2 и радиуса r_2).

2.3. Поле в уединенной сердцевине. Расчет мощности сигнала P_s

Предположим сначала, что излучение вводится только в одну из сердцевин. Будем считать, что $r_3 \gg r_1$, $h \gg 2r_1$ и $h \gg 2r_2$. Тогда для расчета амплитуды напряженности электрического поля в самой влияющей сердцевине, в ее изолирующей оболочке и в общей оболочке можно использовать известную методику для слаборадиационного оптического волокна с осесимметричным ППП [10], согласно которой напряженность электрического поля в поперечном сечении может быть представлена в виде:

$$E(r, \varphi) = E_{\max} \cdot R(r) \cdot \exp(jl\varphi), \quad (7)$$

где r, φ – цилиндрические координаты; $E_{\max}$ – амплитуда напряженности электрического поля; $R(r) \cdot \exp(jl\varphi)$ – периодическая по координате φ функция, описывающая изменение напряженности электрического поля в поперечном сечении; l – целое число, представляющее собой азимутальный порядок моды; j – мнимая единица.

Полагаем, что сердцевина работает в одномодовом режиме, тогда можно считать, что $l = 0$, то есть:

$$E(r, \varphi) = E(r) = E_{\max} \cdot R(r). \quad (8)$$

Таким образом, для расчета E достаточно найти функцию $R(r)$, которая является решением скалярного волнового уравнения:

$$\frac{d^2 R(r)}{dr^2} + \frac{1}{r} \frac{dR(r)}{dr} + \left[k^2 n^2(r) - \beta^2 - \frac{l^2}{r^2} \right] R(r) = 0, \quad (9)$$

где $k = 2\pi / \lambda$ – волновое число; λ – длина волны; $n(r)$ – осесимметричный ППП.

В нашем случае ППП $n(r)$ влияющей сердцевины имеет вид:

$$n(r, \lambda) = \begin{cases} n_1(\lambda), & r \leq r_1 \\ n_2(\lambda), & r_1 < r \leq r_2. \\ n_3(\lambda) & r > r_2 \end{cases} \quad (10)$$

Теперь для каждого из трех слоев (10) можно записать отдельное уравнение (9), которое будет иметь аналитическое решение вида:

$$R_i(r) = A_i Z_1(u_i r) + B_i Z_2(u_i r), \quad (11)$$

где A_i, B_i – постоянные интегрирования; i – номер слоя.

В (11) использованы следующие обозначения:

$$u_i = \begin{cases} \sqrt{k^2 n_i^2 - \beta^2}, & k^2 n_i^2 - \beta^2 \geq 0 \\ \sqrt{\beta^2 - k^2 n_i^2}, & k^2 n_i^2 - \beta^2 < 0 \end{cases}, \quad (12)$$

$$Z_1(u_i r) = \begin{cases} J_0(u_i r), & k^2 n_i^2 - \beta^2 \geq 0 \\ I_0(u_i r), & k^2 n_i^2 - \beta^2 < 0 \end{cases} \quad (13)$$

$$Z_2(u_i r) = \begin{cases} Y_0(u_i r), & k^2 n_i^2 - \beta^2 \geq 0 \\ K_0(u_i r), & k^2 n_i^2 - \beta^2 < 0 \end{cases} \quad (14)$$

где β – постоянная распространения; J_0 и Y_0 – функции Бесселя первого и второго рода нулевого по-

рядка; I_0 и K_0 – модифицированные функции Бесселя первого и второго рода нулевого порядка.

Поле в центральном слое не может описываться функциями Бесселя второго рода Y_0 и K_0 , так как они не определены при $r = 0$. Поля направляемых мод во внешнем слое спадают по экспоненте в радиальном направлении. Это поведение определяется только функцией Z_2 .

Поэтому общее решение уравнения (9) следует записать в виде:

$$R(r) = \begin{cases} A_1 Z_1(u_1 r), & r \leq r_1 \\ A_2 Z_1(u_2 r) + B_2 Z_2(u_2 r), & r_1 < r \leq r_2. \\ B_3 Z_2(u_3 r), & r > r_2 \end{cases} \quad (15)$$

Постоянная распространения фундаментальной моды β и постоянные интегрирования A_i и B_i могут быть найдены из граничных условий, которые заключаются в непрерывности $R(r)$ и ее производной $dR(r)/dr$ на границах между соседними слоями.

Для рассматриваемого случая граничные условия будут состоять из 4 уравнений:

$$\begin{cases} A_1 Z_1(u_1 r_1) - A_2 Z_1(u_2 r_1) - B_2 Z_2(u_2 r_1) = 0 \\ A_1 Z_1'(u_1 r_1) - A_2 Z_1'(u_2 r_1) - B_2 Z_2'(u_2 r_1) = 0 \\ A_2 Z_1(u_2 r_2) + B_2 Z_2(u_2 r_2) - B_3 Z_2(u_3 r_2) = 0 \\ A_2 Z_1'(u_2 r_2) + B_2 Z_2'(u_2 r_2) - B_3 Z_2'(u_3 r_2) = 0 \end{cases} \quad (16)$$

Поскольку общее число неизвестных в (16) равно 5, одну из постоянных интегрирования, например, A_1 нужно задать. Система (16) является однородной системой линейных уравнений, то есть имеет нетривиальное решение только в случае, если ее определитель равен 0 (17).

Выражение (17) представляет собой характеристическое уравнение, из которого можно найти (18) постоянную распространения β (1/м). Вместо β часто приводят безразмерный эффективный показатель преломления n_{eff} .

$$\begin{vmatrix} Z_1(u_1 r_1) & -Z_1(u_2 r_1) & -Z_2(u_2 r_1) & 0 \\ Z_1'(u_1 r_1) & -Z_1'(u_2 r_1) & -Z_2'(u_2 r_1) & 0 \\ 0 & Z_1(u_2 r_2) & Z_2(u_2 r_2) & -Z_2(u_3 r_2) \\ 0 & Z_1'(u_2 r_2) & Z_2'(u_2 r_2) & -Z_2'(u_3 r_2) \end{vmatrix} = 0. \quad (17)$$

$$n_{eff} = \frac{\beta}{k}. \quad (18)$$

Для постоянных интегрирования из (16) получаем:

$$A_2 = A_1 \frac{Z_1(u_1 r_1) \eta_1(u_1 r_1) - \eta_2(u_2 r_1)}{Z_1(u_2 r_1) \eta_1(u_2 r_1) - \eta_2(u_2 r_1)}, \quad (19)$$

$$B_2 = A_1 \frac{Z_1(u_1 r_1) \eta_1(u_1 r_1) - \eta_1(u_2 r_1)}{Z_2(u_2 r_1) \eta_2(u_2 r_1) - \eta_1(u_2 r_1)}, \quad (20)$$

$$B_3 = A_2 \frac{Z_1(u_2 r_2)}{Z_2(u_3 r_2)} + B_2 \frac{Z_2(u_2 r_2)}{Z_2(u_3 r_2)}, \quad (21)$$

$$\text{где } \eta_1(u_i r) = \frac{Z_1'(u_i r)}{Z_1(u_i r)}, \eta_2(u_i r) = \frac{Z_2'(u_i r)}{Z_2(u_i r)}. \quad (22)$$

Зависимости β и n_{eff} от длины волны позволяют рассчитать хроматическую дисперсию D_{chr} сердцевин МСВ [11]:

$$D_{chr} = -\frac{\lambda}{2\pi c} \left(2 \frac{d\beta}{d\lambda} + \lambda \frac{d^2\beta}{d\lambda^2} \right) = -\frac{\lambda}{c} \frac{d^2 n_{eff}}{d\lambda^2}. \quad (23)$$

Используя (15), можно рассчитать радиус модового поля сердцевин МСВ по известному выражению Петермана [13]:

$$w = \sqrt{2 \frac{\int_0^\infty R^2(r) r dr}{\int_0^\infty \left(\frac{dR(r)}{dr} \right)^2 r dr}}. \quad (24)$$

Рассчитаем мощность P_s сигнала в сердцевине.

С учетом (8) перепишем (5) в виде:

$$I(r) = \frac{|E_{\max}|^2}{2} \sqrt{\frac{\epsilon_a}{\mu_a}} \cdot R^2(r). \quad (25)$$

Используем соотношение $n = \sqrt{\mu \cdot \epsilon}$ и учтем, что для прозрачных диэлектриков и, в том числе для кварцевых стекол, $\mu = 1$.

Теперь из (3) и (25) можно получить:

$$P_s = 2\pi \cdot \frac{|E_{\max}|^2}{2} \sqrt{\frac{\epsilon_0}{\mu_0}} \cdot n_1 \cdot \int_0^{r_1} r \cdot R^2(r) \cdot dr = 2\pi \cdot P_{\max} \cdot \int_0^{r_1} r \cdot R^2(r) \cdot dr. \quad (26)$$

В работе было проведено моделирование сердцевин МСВ с изолирующими оболочками различной толщины. Параметры, при которых проведены расчеты, представлены в таблице 1.

Для расчета приведенных в таблице 1 показателей преломления и их зависимости от длины волны использовалось известное уравнение Селлмейера [11]:

$$n^2(\lambda) = \sum_{i=1}^k \frac{S_i \lambda^2}{\lambda^2 - \lambda_i^2} + 1, \quad (27)$$

где λ_i – резонансные длины волн; S_i – безразмерные коэффициенты Селлмейера.

ТАБЛИЦА 1. Параметры сердцевин МСВ с изолирующими оболочками на длине волны 1550 нм

TABLE 1. Parameters of the Core with Insulating Shells in MCF at a Wavelength of 1550 nm

Параметр	Значение
Материал сердцевин	Кварцевое стекло, легированное GeO ₂ с концентрацией 4.1 молярных процентов
Показатель преломления n_1 сердцевин	1,45030996
Материал изолирующей оболочки	Кварцевое стекло, легированное F с концентрацией 2 молярных процента
Показатель преломления n_2 изолирующей оболочки	1,43942439
Материал общей оболочки	Кварцевое стекло
Показатель преломления n_3 общей оболочки	1,44402362
Радиус сердцевин r_1 , мкм	4,1
Длина волны, мкм	1,55

Для кварцевых стекол обычно учитывают три резонанса ($k = 3$). Значения λ_i и S_i для расчета показателей преломления материалов сердцевин и общей оболочки приведены в таблице 2.

Для расчета показателя преломления изолирующей оболочки n_2 использовалось выражение, предложенное в [12]:

$$n_2(\lambda) = n_1(\lambda) - \Delta n \cdot d_F, \quad (28)$$

где d_F – концентрация F в молярных процентах, $\Delta n = 0,0045992$.

ТАБЛИЦА 2. Резонансные длины волн и коэффициенты Селлмейера [11]

TABLE 2. Resonant Wavelengths and Sellmeier Coefficients [11]

Материал	S_1	S_2	S_3	λ_1 , мкм	λ_2 , мкм	λ_3 , мкм
Кварцевое стекло	0,6961663	0,4079426	0,8974794	0,0684043	0,1162414	9,896161
Кварцевое стекло, легированное GeO ₂ с концентрацией 4.1 молярных процентов	0,68671749	0,43481505	0,89656582	0,072675189	0,11514351	10,002398

На рисунке 2 представлены результаты моделирования распределения полей фундаментальной моды в сердцевинах без изолирующей оболочки и с изолирующей оболочкой толщиной 1 мкм. Разные цвета на рисунке соответствуют разным значениям напряженности электрического поля в соответствии с приведенной цветовой шкалой. Черными сплошными линиями на рисунках показаны границы сердцевин и изолирующей оболочки.

На рисунке 3 представлены нормированные распределения полей фундаментальной моды (рисунок 3а), дисперсионные характеристики сердцевин (рисунок 3б) без изолирующей оболочки и с изолирующими оболочками разной толщины $t_2 = r_2 - r_1$ и радиус модового поля (рисунок 3с), рассчитанные по выражениям (10–24).

Из рисунков 2, 3а и 3с видно, что изолирующая оболочка значительно уменьшает диаметр модо-

вого поля с 4,6 до 4,1 мкм при толщине оболочки 1 мкм и 3,8 мкм при толщине оболочки 2 мкм. Это способствует большей концентрации излучения в сердцевине. Дальнейшее увеличение толщины обо-

лочки не дает большого эффекта. Наличие изолирующей оболочки значительно изменяет дисперсионную характеристику сердцевин от 20 до 12 пс/(нм·км) на длине волны 1550 нм (рисунок 3б).

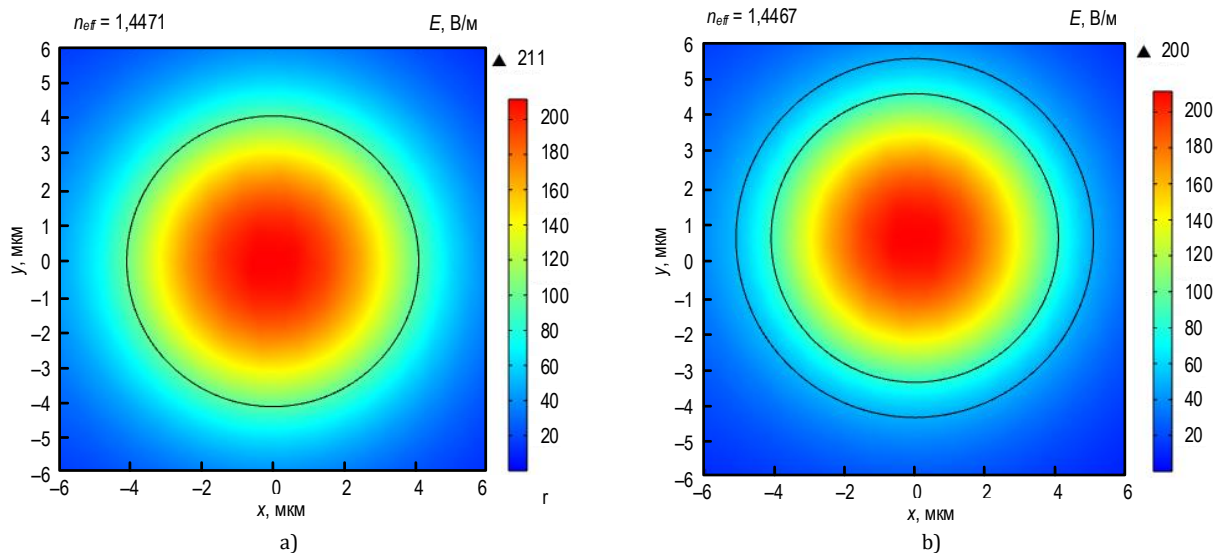


Рис. 2. Распределение поля фундаментальной моды в сердцевине (результат моделирования в COMSOL Multiphysics [14]): без изолирующей оболочки (а) и с изолирующей оболочкой (б) толщиной 1 мкм

Fig. 2. Distribution of the Fundamental Mode Field in the Core (the Result of Modeling in COMSOL Multiphysics [14]): without an insulating clad (a) and with an insulating clad 1 microns thick (b)

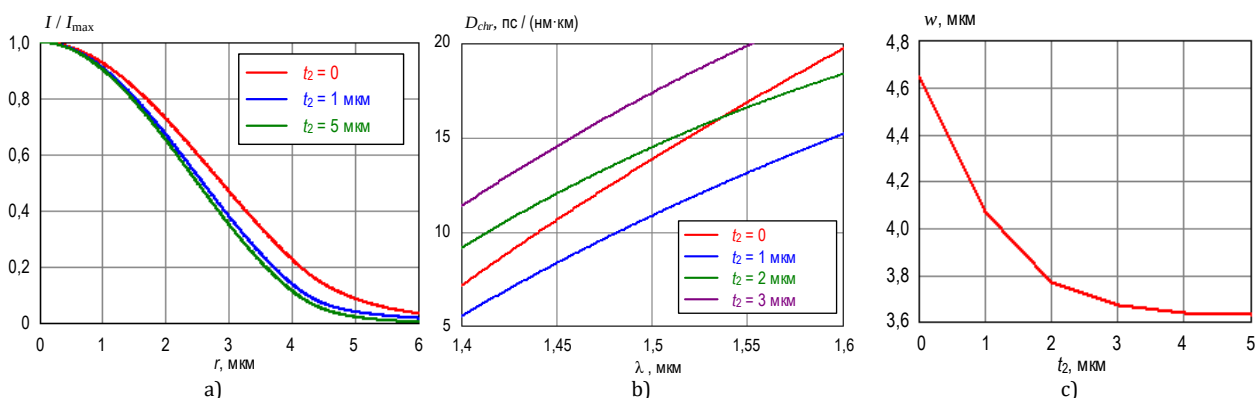


Рис. 3. Характеристики сердцевин без изолирующей оболочки и с изолирующими оболочками разной толщины: а) нормированное распределение интенсивности фундаментальной моды на длине волны 1550 нм; б) зависимость хроматической дисперсии от длины волны; в) зависимость радиуса модового поля от толщины изолирующей оболочки на длине волны 1550 нм

Fig. 3. Characteristics of Cores without Insulating Clads and with Insulating Clads of Different Thicknesses: a) Normalized Distribution of the Intensity of the Fundamental Mode at 1550 nm; b) Dependence of the Chromatic Dispersion on the Wavelength; c) Dependence of the Mode Field Radius on the Insulating Clad Thickness at 1550 nm

2.4. Поле в МСВ с двумя сердцевинами.

Расчет мощности P_n и затухания A перекрестной помехи

В МСВ с двумя сердцевинами одну из них условно будем считать влияющей, а вторую подверженной влиянию. На рисунке 4 представлена часть поперечного сечения МСВ, содержащая влияющую и подверженную влиянию сердцевину. Для расчета по

выражению (4) введем полярную систему координат с началом в центре влияющей сердцевин. Пунктирной окружностью показан контур одного из сечений распределения интенсивности $I(r)$ электромагнитного поля влияющей сердцевин, пересекающий область S_2 сердцевин, подверженной влиянию. Из рисунка видно, что интегрирование по координате r следует производить в пределах от $h - r_1$ до $h + r_1$, а по координате φ – от $-\Phi$ до $+\Phi$.

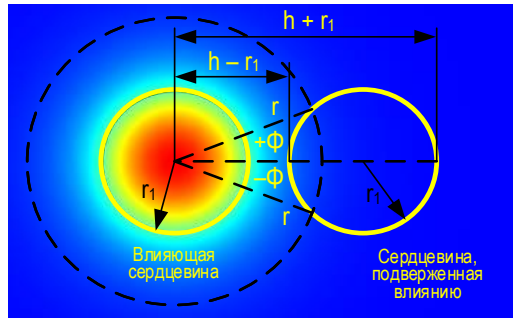


Рис. 4. К расчету мощности помехи P_n
Fig. 4. To Calculate the Interference Power P_n

Перепишем (4) в виде:

$$P_n = \int_{h-r_1}^{h+r_1} \int_{-\Phi}^{\Phi} r \cdot I(r) \cdot dr \cdot d\varphi. \quad (29)$$

Для угла Φ из геометрических соображений получим:

$$\Phi(r) = \arccos\left(\frac{r^2 - r_1^2 + h^2}{2 \cdot h \cdot r}\right). \quad (30)$$

Учитывая, что $I(r)$ не зависит от φ , а также используя (30) и соотношения, примененные при выводе (25), перепишем (29) в виде:

$$\begin{aligned} P_n &= 2 \cdot \frac{|E_{\max}|^2}{2} \sqrt{\frac{\epsilon_0}{\mu_0}} \cdot n_1 \times \\ &\times \int_{h-r_1}^{h+r_1} r \cdot R^2(r) \cdot \arccos\left(\frac{r^2 - r_1^2 + h^2}{2 \cdot h \cdot r}\right) \cdot dr = \\ &= 2 \cdot P_{\max} \cdot \int_{h-r_1}^{h+r_1} r \cdot R^2(r) \times \\ &\times \arccos\left(\frac{r^2 - r_1^2 + h^2}{2 \cdot h \cdot r}\right) \cdot dr. \end{aligned} \quad (31)$$

3. МИНИМАЛЬНОЕ РАССТОЯНИЕ МЕЖДУ СЕРДЦЕВИНАМИ В МСВ. МАКСИМАЛЬНОЕ ЧИСЛО СЕРДЦЕВИН

3.1. Минимальное расстояние между сердцевинами в двухсердцевинном МСВ

На рисунке 5 представлены зависимости затухания перекрестной помехи в сердцевине от расстояния между сердцевинами h в двухсердцевинном МСВ. Расчет проведен по выражениям (2), (26) и (31) для сердцевин без изолирующей оболочки и с изолирующими оболочками разной толщины t_2 на длине волны 1550 нм. Из рисунка 5 видно, что затухание перекрестной помехи A возрастает при увеличении расстояния между сердцевинами. Поэтому, задавшись допустимым уровнем A , диаметром сердцевин $2r_1$ и толщиной изолирующей оболочки t_2 , можно определить минимальное допустимое расстояние $h_{\min}$ между сердцевинами.

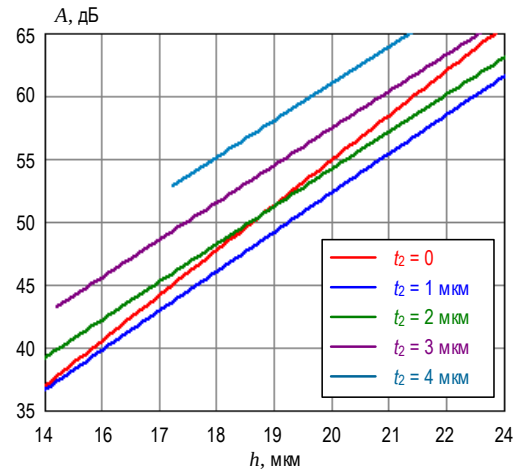


Рис. 5. Затухание перекрестной помехи в МСВ с двумя одинаковыми сердцевинами в изолирующих оболочках разной толщины

Fig. 5. Attenuation of Crosstalk in MCF with Two Identical Cores in Insulating Clads of Different Thickness

На рисунке 6 представлена зависимость $h_{\min}$ от толщины изолирующей оболочки при $A = 60$ дБ. Видно, что без дополнительной изолирующей оболочки $h_{\min} = 20,5$ мкм. Расчеты показывают, что использование тонких изолирующих оболочек даже увеличивает $h_{\min}$ до 21,5 мкм. Однако увеличение толщины оболочки свыше 2,5 мкм позволяет уменьшить $h_{\min}$. При толщине оболочки 4,5 мкм $h_{\min} = 18$ мкм.

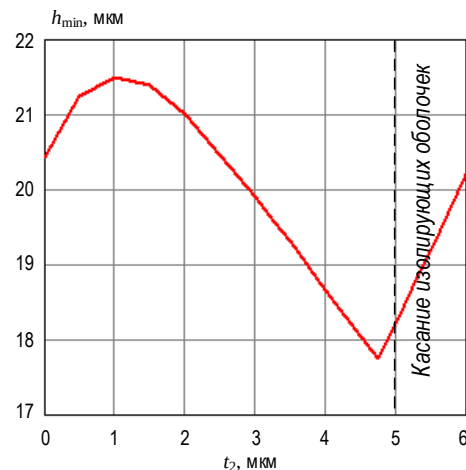


Рис. 6. Минимальное расстояние $h_{\min}$ между сердцевинами в двухсердцевинном волокне (здесь и далее – при котором на длине волны 1550 нм обеспечивается A не менее 60 дБ)

Рис. 6. Minimum Distance $h_{\min}$ between Cores in a Double-Core Fiber (Here and Further – at which A at Least 60 dB is Provided at 1550 nm)

Проведенные расчеты доказывают эффективность изолирующей оболочки, однако наибольшее уменьшение расстояния между сердцевинами достигается практически при касании оболочек, что равносильно отказу от них и уменьшению показателя преломления общей оболочки. При этом конструкция МСВ даже упрощается.

3.2. Максимальное число сердцевин в МСВ

Рассмотрим МСВ с несколькими одинаковыми сердцевинами. Установленное в п. 3.1 расстояние $h_{\min}$ можно считать эквивалентным диаметром сердцевины, являющимся основным параметром при определении максимального количества сердцевин, которые можно расположить в общей оболочке МСВ. Определим максимально возможное количество одинаковых сердцевин N_{core} в МСВ при заданном значении $h \geq h_{\min}$. Для этого нужно решить задачу упаковки кругов с меньшим диаметром $d = h_{\min}$ в круг с большим диаметром $D = 2r_3$ [15]. В нашем случае выбираем $D = 125$ мкм. Результатом решения этой задачи будет число сердцевин N_{core} и диаграмма их размещения в поперечном сечении МСВ. Методика оптимальной упаковки для различных отношений d / D приведена в [16].

На рисунке 7 показан пример размещения 19 сердцевин в МСВ на равных расстояниях h друг от друга. В этом случае перекрестные помехи в каждой сердцевине будут создавать $(N_{\text{core}} - 1) = 18$ влияющих сердцевин.

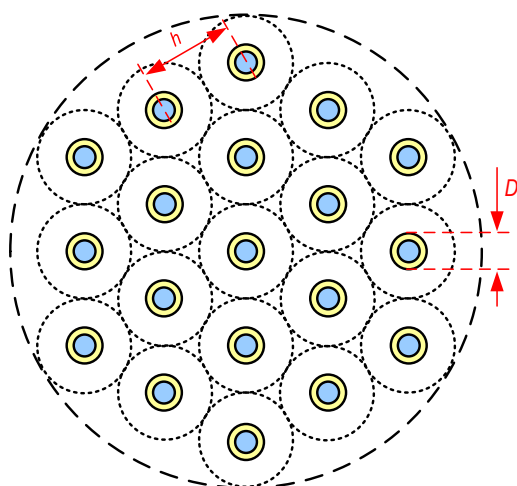


Рис. 7. Размещение сердцевин в МСВ на равных расстояниях h друг от друга

Fig. 7. Placement of Cores in MCF at Equal Distances h from Each Other

Из рисунка 5 видно, что увеличение расстояния между влияющей и подверженной влиянию сердцевинами в 1,7 раза приводит к возрастанию затухания перекрестной помехи более чем на 30 дБ. Поэтому при расчете перекрестных помех можно учитывать только влияние сердцевин, расположенных в непосредственной близости от сердцевины, подверженной влиянию. Из рисунка 7 видно, что их количество в зависимости от расположения подверженной влиянию сердцевины составляет от 3 до 6. Таким образом, максимальная перекрестная помеха в первом приближении составит $P_{n \max} = 6P_n$.

На рисунке 8 показана зависимость минимального допустимого расстояния $h_{\min}$ между соседними сердцевинами, при условии:

$$A_{\min} = 10 \lg \left(\frac{P_s}{P_{n \max}} \right) \geq 60 \text{ дБ.}$$

Расстояние $h_{\min}$ для сердцевин без изолирующей оболочки составляет 22,65 мкм (см. рисунок 8), то есть при $2r_3 = 125$ мкм получаем $h_{\min} / 2r_3 = 0,181$. Для этого отношения существует решение с размещением $N_{\text{core}} = 19$ сердцевин по схеме с одинаковыми расстояниями между соседними сердцевинами, что представлено на рисунке 7, или $N_{\text{core}} = 22$ сердцевин, если расстояния между соседними сердцевинами могут отличаться (рисунок 9) [16].

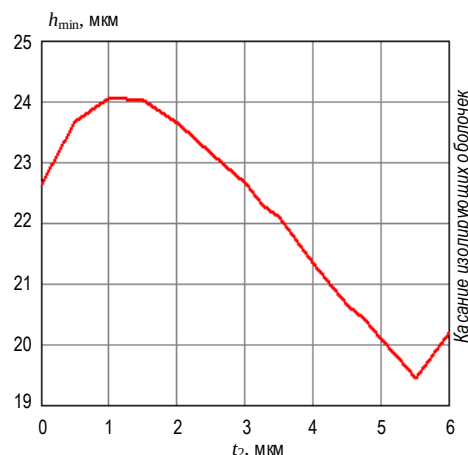


Рис. 8. Минимальное расстояние $h_{\min}$ между сердцевинами в МСВ, концентрация F в изолирующих оболочках 2 %

Fig. 8. The Minimum Distance $h_{\min}$ between the Cores in MCF, Concentration of F in Insulating Clads 2 %

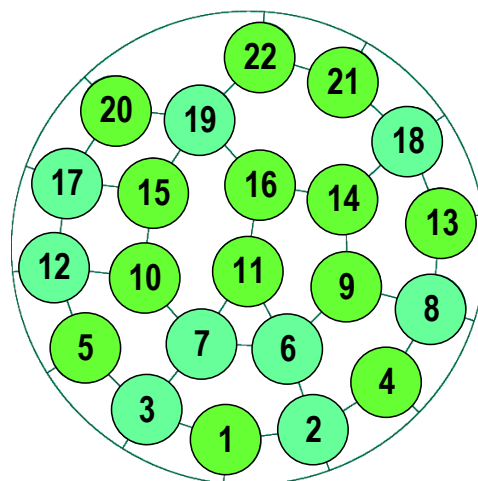


Рис. 9. Размещение максимально возможного числа сердцевин без изолирующей оболочки в МСВ с общей оболочкой диаметром 125 мкм при $h_{\min} = 22,65$ мкм

Fig. 9. Placement of the Maximum Possible Number of Cores without an Insulating Clad in MCF with a Common Clad with a Diameter of 125 microns at $h_{\min} = 22,65$ microns

Минимальное значение $h_{\min}$ на рисунке 8 достигается при использовании изолирующей оболочки толщиной 5,5 мкм и составляет 19,44 мкм. При $2r_3 = 125$ мкм получаем $h_{\min} / 2r_3 = 0,156$. Для этого отношения существует решение с расположением

$N_{core} = 31$ сердцевин по схеме с одинаковыми расстояниями между соседними сердцевинами. Диаграмма размещения сердцевин приведена на рисунке 10а. При касании изолирующих оболочек соседних сердцевин (изолирующая оболочка толщиной 6 мкм) получаем $h_{min} = 20.2$ мкм, $h_{min} / 2r_3 =$

$= 0,162$ и $N_{core} = 29$ (рисунок 10б). Этот случай равносителен отказу от изолирующих оболочек и уменьшению показателя преломления общей оболочки, например, с помощью повышения концентрации F в общей оболочке.

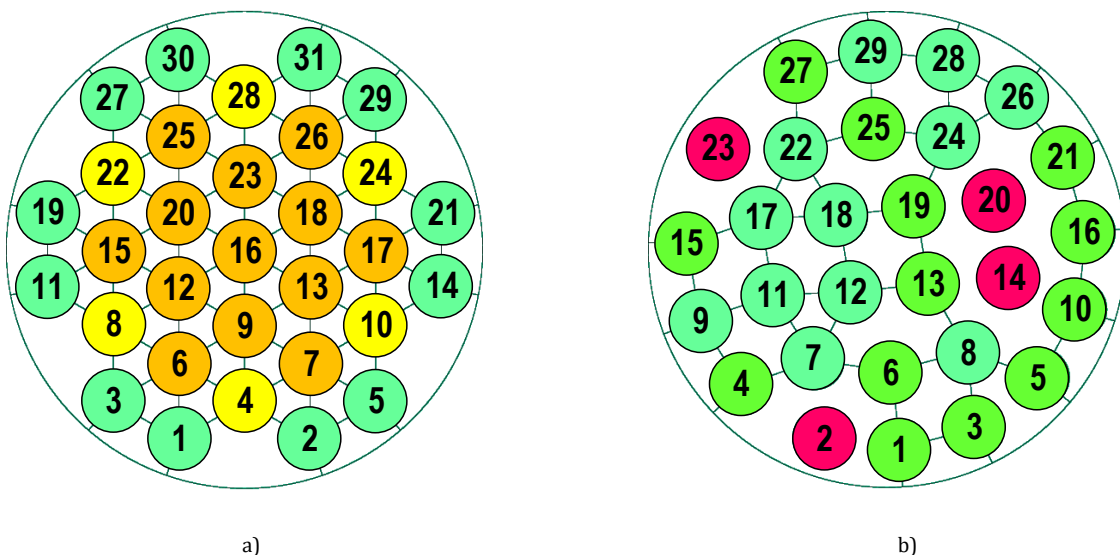


Рис. 10. Размещение сердцевин в МСВ с общей оболочкой диаметром 125 мкм при $h_{min} = 19,44$ мкм (а) и $h_{min} = 20,2$ мкм (б)

Fig. 10. Placement of Cores in MCF with a Common Clad with a Diameter of 125 microns at: a) $h_{min} = 19,44$ microns; b) $h_{min} = 20,2$ microns

На рисунке 11 представлены зависимости h_{min} от t_2 для изолирующей оболочки из кварцевого стекла, легированного 3 % F.

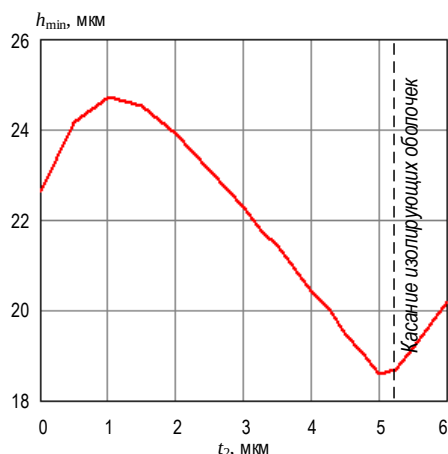


Рис. 11. Минимальное расстояние h_{min} между сердцевинами в МСВ, концентрация F в изолирующих оболочках 3 %

Fig. 11. The Minimum Distance h_{min} between the Cores in MCF, Concentration of F in Insulating Clads 3 %

Видно, что в этом случае наибольшее число сердцевин можно разместить на расстоянии 18,59 мкм при толщине изолирующей оболочки 5 мкм ($h_{min} / (2r_3) = 0,149$). МСВ в этом случае может иметь до 35 сердцевин [16]. Однако практически такой же результат (34 сердцевин) получается при касании изолирующих оболочек соседних сердцевин ($t_2 = 5,25$ мкм).

При изменении показателей преломления общей и изолирующих оболочек нужно следить за изменением дисперсионных характеристик и диаметров модовых полей сердцевин. В рассмотренных выше примерах материал и радиусы изолирующей оболочки выбирались так, чтобы характеристики сердцевин оставались близкими к характеристикам стандартного одномодового волокна G.652.

4. ЗАКЛЮЧЕНИЕ ПО ЧАСТИ 1

Проведенные в работе исследования доказывают возможность создания кварцевых МСВ, имеющих общую оболочку стандартного для телекоммуникационных волокон диаметра 125 мкм, с несколькими одномодовыми сердцевинами. Величиной возникающих перекрестных помех можно управлять, изменяя расстояние между отдельными сердцевинами, а также с помощью изолирующих элементов различной конструкции.

Анализ параметров МСВ с сердцевинами в изолирующих оболочках из фторсиликатного стекла и МСВ с сердцевинами без изолирующих оболочек выявил преимущество первой конструкции. Расчеты показали, что в МСВ диаметром 125 мкм в общей оболочке можно разместить 22 одномодовых сердцевин диаметром 8,2 мкм без изолирующих оболочек. Использование изолирующей оболочки с пониженным по отношению к общей оболочке показателем преломления из фторсиликатного

стекла позволяет увеличить количество сердцевин до 31 при концентрации 2 %F и до 35 при концентрации 3 %F. Однако достигаются эти результаты при относительно большой толщине изолирующей оболочки, когда оболочки соседних сердцевин почти касаются друг друга.

В некоторых случаях размещение в общей оболочке максимально возможного числа сердцевин возможно только при условии отказа от их симметричного расположения, что усложняет технологию производства и работу с готовым МСВ.

Отказ от изолирующих оболочек и, следовательно, упрощение конструкции МСВ практически эквивалентен использованию общей оболочки с

пониженным показателем преломления. Такая конструкция позволяет разместить 29 сердцевин при концентрации 2 %F и 34 – при концентрации 3 %F в общей оболочке.

Таким образом, эффективность применения изолирующих оболочек можно считать доказанной, но вопрос о целесообразности их использования должен решаться в каждом конкретном случае с учетом технологических и экономических факторов.

Во второй части работы будут рассмотрены МСВ с сердцевинами, изолированными друг от друга защитными барьерами из воздушных капилляров.

Продолжение следует...

Список источников

1. Семенов А.Б. Параллельная волоконно-оптическая передача в ЛВС и СКС. Подходы к реализации физического и канального уровней. М.: Горячая линия – Телеком, 2018. 272 с.
2. Hayashi T. Multi-core optical fibers realizing high-density/-capacity transmissions // Proceedings of the IEEE CPMT Symposium Japan (ICSJ, Kyoto, Japan, 07–09 November 2016). IEEE, 2016. DOI:10.1109/ICSJ.2016.7801252
3. Былина М.С., Гуляева Л.А. Новые типы многосерцевинных волокон для центров обработки данных // Всероссийская научно-методическая конференция магистрантов и их руководителей «Подготовка профессиональных кадров в магистратуре для цифровой экономики ПКМ» ПКМ-2021, Санкт-Петербург, Россия, 30 ноября–02 декабря 2021). Сборник лучших докладов конференции. СПб.: Санкт-Петербургский государственный университет телекоммуникаций им. проф. М.А. Бонч-Бруевича, 2021. С. 175–179.
4. Ortiz A.M., Sáez R.L. Multi-Core Optical Fibers: Theory, Applications and Opportunities // In: Xu F., Mou C. (eds.) Selected Topics on Optical Fiber Technologies and Applications. Rijeka: InTech, 2018. PP. 63–102. DOI:10.5772/intechopen.72458
5. Kaminow I.P., Li T., Willner A.E. Optical Fiber Telecommunications Volume VIA: Components and Subsystems. Oxford: Academic Press, 2013. 794 p.
6. Фокин В.Г., Ибрагимов Р.З. Оптические системы с терабитными и петабитными скоростями передачи: учебное пособие. Новосибирск: Сибирский государственный университет телекоммуникаций и информатики, 2016. 156 с.
7. Портнов Э.Л. Новые типы оптических волокон в телекоммуникациях и их применение // T-Comm. 2013. Т. 7. № 8. С. 96–98.
8. Дианов Е.М., Семёнов С.Л., Буфетов И.А. Новое поколение волоконных световодов // Квантовая электроника. 2016. Т. 46. № 1. С. 1–10.
9. Ziolkowicz A., Szymanski M., Szostkiewicz L., Tenderenda T., Napierala M., Murawski M., et al. Hole-assisted multicore optical fiber for next generation telecom transmission systems // Applied Physics Letters. 2014. Vol. 105. Iss. 8. P. 081106. DOI:10.1063/1.4894178
10. Былина М.С., Глаголев С.Ф. Методика и результаты расчетов параметров оптических волокон с осесимметричным профилем показателя преломления // Фотон-экспресс. 2017. Т. 6(142). С. 159–160.
11. Адамс М. Введение в теорию оптических волноводов. М.: Мир, 1984.
12. Brückner V. To the use of Sellmeier formula. 2014. URL: https://www.researchgate.net/publication/262294649_To_the_use_of_Sellmeier_formula (дата обращения 21.11.2022)
13. Бурдин А.В., Жуков А.Е., Прапорщиков Д.Е. Расчет вносимых потерь на стыке слабонаправляющих волоконных световодов с произвольным профилем показателя преломления в маломодовом режиме передачи оптических сигналов // T-Comm: Телекоммуникации и транспорт. 2015. Т. 9. № 4. С. 60–66.
14. Программное обеспечение COMSOL Multiphysics®. Понимание, прогнозирование, оптимизация реалистичных физических процессов и устройств с помощью численного моделирования // COMSOL. URL: <https://www.comsol.ru/comsol-multiphysics> (дата обращения 07.08.2022)
15. Reis G.E. Dense Packing of Equal Circles Within a Circle // Mathematics Magazine. 1975. Vol. 48. Iss. 1. PP. 33–37. DOI:10.1080/0025570X.1975.11976434
16. The best known packings of equal circles in a circle (complete up to N = 2600) // E. Specht. URL: <http://hydra.nat.uni-magdeburg.de/packing/cci/cci.html> (дата обращения 21.11.2022)

References

1. Semenov A.B. *Parallel Fiber-Optic Transmission in LAN and SCS. Approaches to the Implementation of the Physical and Channel Layers*. Moscow: Goriachaia liniia – Telekom Publ.; 2018. 272 p. (in Russ.)
2. Hayashi T. Multi-core optical fibers realizing high-density/-capacity transmissions. *Proceedings of the IEEE CPMT Symposium Japan, ICSJ, 07–09 November 2016, Kyoto, Japan*. IEEE; 2016. DOI:10.1109/ICSJ.2016.7801252
3. Bylina M.S., Gulyaeva L.A. New Types of Multi-Core Fibers for Data Centers. *Collection of the best reports of the All-Russian Scientific and Methodological Conference of Undergraduates and Their Leaders on Training of Professional Staff in the Master's*

Program for the Digital Economy of the PKM, PKM-2021, 30 November–02 December 2021, St. Petersburg, Russia. St. Petersburg: The Bonch-Bruевич Saint-Petersburg State University of Telecommunications Publ.; 2021. p.175–179. (in Russ.)

4. Ortiz A.M., Sáez R.L. Multi-Core Optical Fibers: Theory, Applications and Opportunities. In: Xu F., Mou C. (eds.) *Selected Topics on Optical Fiber Technologies and Applications*. Rijeka: InTech; 2018. p.63–102. DOI:10.5772/intechopen.72458

5. Kaminow I.P., Li T., Willner A.E. *Optical Fiber Telecommunications Volume VIA: Components and Subsystems*. Oxford: Academic Press; 2013. 794 p.

6. Fokin V.G., Ibragimov R.Z. *Optical Systems with Terabit and Petabit Transmission Rates*. Novosibirsk: Siberian State University of Telecommunications and Information Sciences Publ.; 2016. 156 p. (in Russ.)

7. Portnov E.L. New types of optical fibers in telecommunications and their application. *T-Comm*. 2013; 7(8):96–98. (in Russ.)

8. Dianov E.M., Semenov S.L., Bufetov I.A. New Generation of Optical Fibres. *Quantum Electronics*. 2016;46(1):1–10. DOI:10.1070/QE2016v046n01ABEH015963

9. Ziolkowicz A., Szymanski M., Szostkiewicz L., Tenderenda T., Napierala M., Murawski M., et al. Hole-assisted multicore optical fiber for next generation telecom transmission systems. *Applied Physics Letters*. 2014;105(8):081106. DOI:10.1063/1.4894178

10. Bylina M.S., Glagolev S.F. Methods and results of calculations of parameters of optical fibers with an axisymmetric refractive index profile. *Foton-ekspress*. 2017;6(142):159–160. (in Russ.)

11. Adams M. *Introduction to the Theory of Optical Waveguides*. Moscow: Mir Publ.; 1984. (in Russ.)

12. Brückner V. *To the use of Sellmeier formula*. 2014. URL: https://www.researchgate.net/publication/262294649_To_the_use_of_Sellmeier_formula [Accessed 21st November 2022]

13. Burdin A.V., Zhukov A.E., Praporshchikov D.E. Method for estimation the insertion loss at splice of weakly guiding optical fibers with arbitrary refractive index profile under a few-mode regime of signal transmission. *T-Comm*. 2015;9(4):60–66. (in Russ.)

14. COMSOL. Software COMSOL Multiphysics®. Understanding, forecasting, optimization of realistic physical processes and devices using numerical modeling. (in Russ.) URL: <https://www.comsol.ru/comsol-multiphysics> [Accessed 7th August 2022]

15. Reis G.E. Dense Packing of Equal Circles Within a Circle. *Mathematics Magazine*. 1975;48(1):33–37. DOI:10.1080/0025570X.1975.11976434

16. E. Specht. The best known packings of equal circles in a circle (complete up to N = 2600). URL: <http://hydra.nat.uni-magdeburg.de/packing/cci/cci.html> [Accessed 21st November 2022]

Статья поступила в редакцию 02.09.2022; одобрена после рецензирования 18.11.2022; принята к публикации 21.11.2022.

The article was submitted 02.09.2022; approved after reviewing 18.11.2022; accepted for publication 21.11.2022.

Информация об авторах:

БЫЛИНА
Мария Сергеевна

кандидат технических наук, доцент, заведующая кафедрой фотоники и линий связи Санкт-Петербургского государственного университета телекоммуникаций им. проф. М.А. Бонч-Бруевича,

 <https://orcid.org/0000-0001-9818-4060>

ГУЛЬТЯЕВА
Людмила Александровна

ассистент кафедры фотоники и линий связи Санкт-Петербургского государственного университета телекоммуникаций им. проф. М.А. Бонч-Бруевича,

 <https://orcid.org/0000-0002-6064-9691>

Научная статья

УДК 621.396

DOI:10.31854/1813-324X-2022-8-4-39-47



Применение виртуальных магнитных диполей в антенной решетке для повышения точности пеленгации

Евгений Алексеевич Ищенко¹ ✉, kursk1998@yandex.ru

Юрий Геннадьевич Пастернак¹, pasternakyg@mail.ru

Владимир Андреевич Пендюрин², infonpp-acc.ru@yandex.ru

Сергей Михайлович Фёдоров¹, fedorov_sm@mail.ru

¹Воронежский государственный технический университет,
Воронеж, 394006, Российская Федерация

²АО НПП «Автоматизированные системы связи»,
Воронеж, 394062, Российская Федерация

Аннотация: В статье рассматривается способ формирования виртуальной антенной решетки на основе магнитных диполей. Для проверки его эффективности проводилось моделирование БПЛА с пеленгационным комплексом из четырех векторных антенных элементов. Рассматриваются два способа пеленгации – на основе электрического и магнитного поля. В результате проведенного исследования было обнаружено, что использование магнитных диполей позволяет значительно повысить стабильность и точность пеленга как для электромагнитных волн с линейной поляризацией, так и с эллиптической. Приводятся основные математические выражения, используемые для определения характеристик пеленгации, а также зависимости пеленгов в исследуемом диапазоне частот.

Ключевые слова: виртуальная антенная решетка, пеленгация, магнитные диполи, БПЛА

Источник финансирования: Исследование выполнено за счет гранта Российского научного фонда № 19-79-10109, <https://rscf.ru/project/19-79-10109>.

Ссылка для цитирования: Ищенко Е.А., Пастернак Ю.Г., Пендюрин В.А., Фёдоров С.М. Применение виртуальных магнитных диполей в антенной решетке для повышения точности пеленгации // Труды учебных заведений связи. 2022. Т. 8. № 4. С. 39–47. DOI:10.31854/1813-324X-2022-8-4-39-47

Application of a Virtual Magnetic Dipoles in Antenna Array to Increase the Direction Finding Accuracy

Evgeny Ishchenko¹ ✉, kursk1998@yandex.ru

Yuri Pasternak¹, pasternakyg@mail.ru

Vladimir Pendyurin², infonpp-acc.ru@yandex.ru

Sergei Fedorov¹, fedorov_sm@mail.ru

¹Voronezh State Technical University,
Voronezh, 394006, Russian Federation

²Research and Development Enterprise “Automated Communication Systems”, JSC,
Voronezh, 394062, Russian Federation

Abstract: *The article discusses the method of forming a virtual antenna array based on magnetic dipoles. To test the effectiveness of the formation of a virtual antenna array, a simulation of an unmanned aerial vehicle with a direction-finding complex of four vector antenna elements was carried out. To perform direction finding, two methods are considered – based on the electric field and magnetic. On the basis of the study, it was found that the use of direction finding based on magnetic dipoles can significantly improve the stability and accuracy of the bearing for both linear and elliptical electromagnetic waves. The article presents the main mathematical expressions that are used to determine the characteristics of the direction finding, as well as the dependence of the bearings in the studied frequency range.*

Keywords: *virtual antenna array, direction finding, magnetic components of the electromagnetic field, unmanned aerial vehicle*

Funding: This research was supported by the Russian Science Foundation, grant No. 19-79-10109, <https://rscf.ru/en/project/19-79-10109>.

For citation: Ishchenko E., Pasternak Yu., Pendyurin V., Fedorov S. Application of a Virtual Magnetic Dipoles in Antenna Array to Increase the Direction Finding Accuracy. *Proc. of Telecom. Universities*. 2022;8(4):39–47. (in Russ.) DOI:10.31854/1813-324X-2022-8-4-39-47

Введение

Пеленгация электромагнитных волн востребована во многих задачах. Благодаря определению направления прихода электромагнитных волн становится возможным улучшение покрытия сети, обнаружение источника излучения и повышения качества связи. Для выполнения таких задач применяются радиопеленгационные комплексы, которые, как правило, помещаются на подвижных носителях. При выборе позиции для размещения комплекса важно обеспечить минимальное искажение волн, так как это внесет погрешность в измерение характеристик волн. Для решения этой задачи используется несколько способов: исследование диаграмм обратного рассеяния объекта (ДОР) и выбор наиболее «чистого» от искажений места; обработка сигналов с повышением отношения сигнал-шум (ОСШ), что повышает эффективность обработки и обнаружения; применение способов аппроксимации поля и технологии виртуальных антенных решеток (ВАР). Именно о последнем из перечисленных способов в данной работе пойдет речь.

Формирование ВАР основано на математическом аппарате, который используется для обработки измеренных характеристик электромагнитных волн комплексом пеленгации. В работе [1] приводится ряд алгоритмов, которые позволяют сформировать ВАР для разных реальных антенных решеток. В результате применения математических способов становится возможным обеспечить не только повышение точности обработки сигналов, улучшить характеристики диаграмм направленности, а также выбрать оптимальное расположение реальных антенных элементов.

Благодаря возможности выполнения аппроксимации и обработки электромагнитных волн технология ВАР может быть использована для формирования требуемой диаграммы направленности антенной решетки, при этом достигая минимального

числа антенных элементов в конструкции. Как показано в работе [2], применение технологии ВАР позволяет значительно снизить уровень боковых лепестков для цилиндрических антенных решеток, что значительно повышает точность обнаружения направления прихода волн, а также помехозащищенность канала. Для радаров технологию ВАР можно использовать для формирования узкого и направленного лепестка [3], при этом пик диаграммы направленности будет наблюдаться именно в направлении прихода волны. Для повышения точности результатов и эффективности обработки измерений используются способы ортогонального кодирования и цифровой обработки сигналов. Другим примером управления характеристиками диаграмм направленности является математическая обработка, которая приводится в работе [4]. В результате применения новых способов удалось повысить чувствительность ВАР к углу прихода волн, что является востребованной задачей в пеленгаторах.

Формирование ВАР возможно в любых диапазонах частот, что подтверждается работой [5]. За счет гибкости математических методов аппроксимация поля возможна не только на низких частотах, а также и в миллиметровом диапазоне волн, который востребован в сетях 5G. Полученные результаты показывают, что применение технологии ВАР возможно даже при использовании технологии ММО. Использование теории ВАР может повысить качество и эффективность технологии формирования луча для сетей пятого поколения и радаров диапазонов K и Ka .

Пеленгация с использованием ВАР является одним из основных способов, который повышает эффективность обнаружения электромагнитных волн, а также позволяет уменьшить число антенных элементов в комплексе пеленгации, как показано в работе [6]. Для формирования ВАР в данной работе

используется метод MUSIC, который является сейчас самым распространенным для этих целей.

Применение беспилотных летательных аппаратов (БПЛА) позволяет значительно повысить эффективность пеленгации [7]. Благодаря их малым размерам, высокой мобильности возможно выполнить быстрое исследование большого участка пространства. Поэтому размещение малого пеленгационного комплекса на БПЛА является важной и востребованной задачей, а применение способов повышения точности пеленгации гипотетически позволит также повысить эффективность применения таких систем.

На основе проведенного выше анализа можно заметить, что использование ВАР гипотетически позволяет повысить эффективность пеленгации, а размещение комплекса пеленгации на БПЛА – обеспечить мобильность и увеличить область применения.

Математические методы пеленгации и формирование магнитных диполей

В процессе решения задачи формирования ВАР на основе магнитных диполей использовались кубические антенные элементы, из которых возможно сформировать комплекс пеленгации. Вид антенного элемента приводится на рисунке 1.

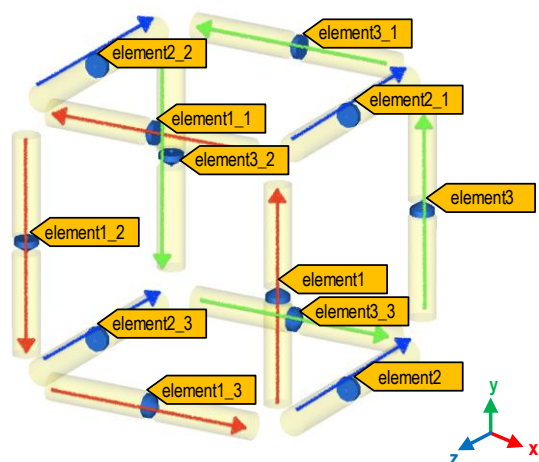


Рис. 1. Вид векторного антенного элемента (стрелки указывают направление тока)

Fig. 1. View of the Vector Antenna Element (Arrows Indicate Direction of Current)

Для формирования пеленгатора используется векторный антенный элемент из 12 симметричных диполей, которые располагаются в ребрах куба с гранями длиной 50 мм. В качестве нагрузок выступают эквивалентные схемы высокочастотных усилителей – последовательное соединение резистора с сопротивлением 50 Ом и конденсатором с емкостью 1,5 пФ.

Компоненты векторов напряженности магнитного поля, которые измерит антенна, связаны

напрямую со вторым уравнением Максвелла в интегральной форме:

$$\oint_L \vec{E} d\vec{l} = -\frac{d}{dt} \int_S \vec{B} d\vec{s}, \quad (1)$$

где $d\vec{l}$ – единичный векторный элемент контура интегрирования L , который ориентирован против часовой стрелки; $d\vec{s}$ – единичный элемент площади, ориентированный по нормали к поверхности S , опирающейся на контур L ; $\vec{B}$ – вектор магнитной индукции, пронизывающей поверхность S .

На основе этого уравнения можно получить значения магнитных компонент, которые можно применить для пеленгации. Ниже рассмотрим способы пеленгации, которые могут быть использованы для определения угла прихода электромагнитных волн.

При падении электромагнитной волны на антенный элемент в нагрузках будут возбуждаться напряжения, которые можно определить в комплексной форме:

$$\dot{u} = u_{Re} + ju_{Im}. \quad (2)$$

На основе измеренных напряжений для каждого антенного элемента можно сформировать электрическое поле, при этом важно сохранить направление обхода контура для нагрузок (их полярность).

Так, для антенного элемента (см. рисунок 1) компоненты электрического поля будут иметь вид:

$$E_x = \frac{\dot{u}_{13} - \dot{u}_{11} + \dot{u}_{33} - \dot{u}_{31}}{4}, \quad (3)$$

$$E_y = \frac{\dot{u}_1 - \dot{u}_{12} + \dot{u}_{13} - \dot{u}_{32}}{4}, \quad (4)$$

$$E_z = \frac{-\dot{u}_2 - \dot{u}_{21} - \dot{u}_{22} - \dot{u}_{23}}{4}, \quad (5)$$

где $\dot{u}_{nm}$ – напряжения в нагрузках с соответствующими индексами n, m .

После этого компоненты электрического поля можно объединить в матрицы с присвоением им порядковых номеров, а также координат, то есть провести их параметризацию. Тогда суммарное поле для пеленгации по электрическим компонентам (проводилась по суммарному полю по всем трем компонентам, а также по z -компонентам поля) будет иметь вид (6, 7).

Далее на основе выражений (6, 7) и корреляционно-интерферометрического способа пеленгации определяется градусная мера угла прихода электромагнитной волны. Недостатком такой процедуры является то, что электрические компоненты поля являются более чувствительными к шумам и помехам, поэтому рассмотрим формирование ВАР на основе магнитных компонент поля (магнитных диполей).

$$D_{E_z} = \left| \sum_{n=1}^N E_{x_n} \cdot \exp(-jk_0(x_n \cos(\psi) + y_n \sin(\psi))) + \sum_{n=1}^N E_{y_n} \cdot \exp(-jk_0(x_n \cos(\psi) + y_n \sin(\psi))) + \sum_{n=1}^N E_{z_n} \cdot \exp(-jk_0(x_n \cos(\psi) + y_n \sin(\psi))) \right|, \quad (6)$$

$$D_{E_z} = \left| \sum_{n=1}^N E_{z_n} \cdot \exp(-jk_0(x_n \cos(\psi) + y_n \sin(\psi))) \right|, \quad (7)$$

где $E_{x_n}, E_{y_n}, E_{z_n}$ – матрицы на основе объединения E_x, E_y, E_z компонент, соответственно; k_0 – волновое число; x, y – координаты векторных антенных элементов в пеленгационном комплексе; ψ – угол сканирования и наблюдения; N – число антенных элементов в комплексе

Изначальными данными при начале пеленгации также являются напряжения, которые будут измерены в нагрузках, представленных формой (2). На их основе определяются компоненты магнитного поля по x, y, z , однако в таком случае они базируются на двух частичных компонентах:

$$H_{x1} = - \left(\frac{\dot{u}_3 - \dot{u}_{21} - \dot{u}_1 + \dot{u}_2}{j\omega\mu_0 a} \right), \quad (8)$$

$$H_{x2} = - \left(\frac{-\dot{u}_{32} - \dot{u}_{22} + \dot{u}_{12} + \dot{u}_{23}}{j\omega\mu_0 a} \right), \quad (9)$$

$$H_{y1} = - \left(\frac{\dot{u}_{31} - \dot{u}_{22} - \dot{u}_{11} + \dot{u}_{21}}{j\omega\mu_0 a} \right), \quad (10)$$

$$H_{y2} = - \left(\frac{\dot{u}_{13} + \dot{u}_2 - \dot{u}_{33} - \dot{u}_{23}}{j\omega\mu_0 a} \right), \quad (11)$$

$$H_{z1} = - \left(\frac{\dot{u}_1 + \dot{u}_{11} + \dot{u}_{12} + \dot{u}_{13}}{j\omega\mu_0 a} \right), \quad (12)$$

$$H_{z2} = - \left(\frac{\dot{u}_3 + \dot{u}_{31} + \dot{u}_{32} + \dot{u}_{33}}{j\omega\mu_0 a} \right), \quad (13)$$

где a – длина плеча векторной антенны (50 мм); μ_0 – магнитная постоянная свободного пространства; тогда с учетом частичных компонент полные будут определяться в соответствии с:

$$H_x = \frac{H_{x1} + H_{x2}}{2}, \quad (14)$$

$$H_y = \frac{H_{y1} + H_{y2}}{2}, \quad (15)$$

$$H_z = \frac{H_{z1} + H_{z2}}{2}. \quad (16)$$

Затем формируется суммарное поле, на основе которого будет проводиться пеленгация, где будет использоваться корреляционно-интерферометрический способ пеленгации для суммарного поля и его z -компонент (17, 18). Теперь на основе описанных способов рассмотрим ситуацию, когда пеленгационный комплекс устанавливается на БПЛА для определения направления прихода электромагнитных волн.

$$D_{H_z} = \left| \sum_{n=1}^N H_{x_n} \cdot \exp(-jk_0(x_n \cos(\psi) + y_n \sin(\psi))) + \sum_{n=1}^N H_{y_n} \cdot \exp(-jk_0(x_n \cos(\psi) + y_n \sin(\psi))) + \sum_{n=1}^N H_{z_n} \cdot \exp(-jk_0(x_n \cos(\psi) + y_n \sin(\psi))) \right|, \quad (17)$$

$$D_{H_z} = \left| \sum_{n=1}^N H_{z_n} \cdot \exp(-jk_0(x_n \cos(\psi) + y_n \sin(\psi))) \right|. \quad (18)$$

Исследуемая модель. Проверка работы метода пеленгации для плоской волны

При исследовании эффективности работы предложенного способа был сформирован пеленгатор из 4-х векторных антенных элементов, которые располагались в нижней части малого БПЛА, как

показано на рисунке 2, где: а) изометрический вид с установленными в нижней части векторными антенными элементами (указана длина корпуса); б) вид сбоку с указанием расстояния между крайними элементами комплекса пеленгации; с) вид спереди с указанием размеров комплекса пеленгации.

Для того, чтобы учесть влияние корпуса и отследить, как он искажает электромагнитное поле, была построена ДОР, а также найдена эффективная площадь рассеяния, при этом в ходе моделирования у БПЛА были указаны материалы: верхняя крышка, ножки, векторные антенные элементы – алюминий; остальные компоненты – пластик.

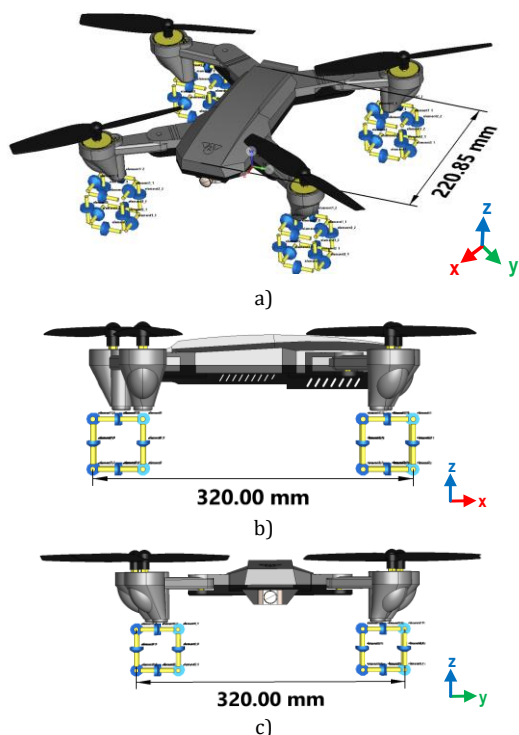


Рис. 2. Исследуемый БПЛА с четырьмя векторными антенными элементами,

Fig. 2. The Investigated UAV with Four Vector Antenna Elements

На рисунке 3 приводится картина ДОР на частоте 500 МГц (так как в процессе пеленгации исследуется диапазон от 300 до 700 МГц). Как видно, картина обратного рассеяния изрезана и соответственно изменяет характеристики электромагнитного поля, так как возникают отражения.

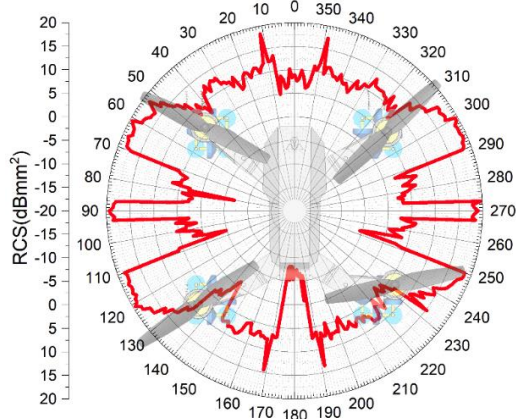
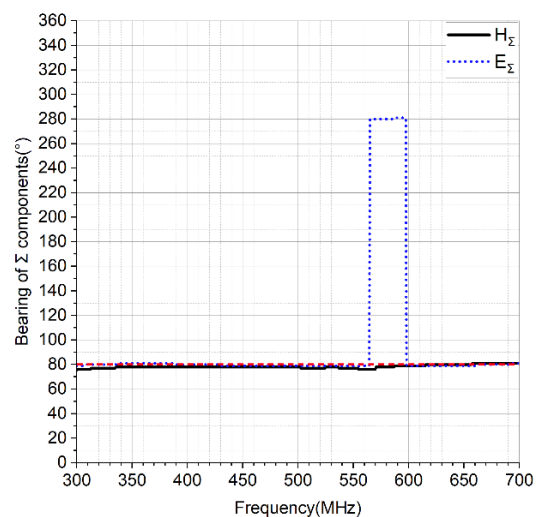


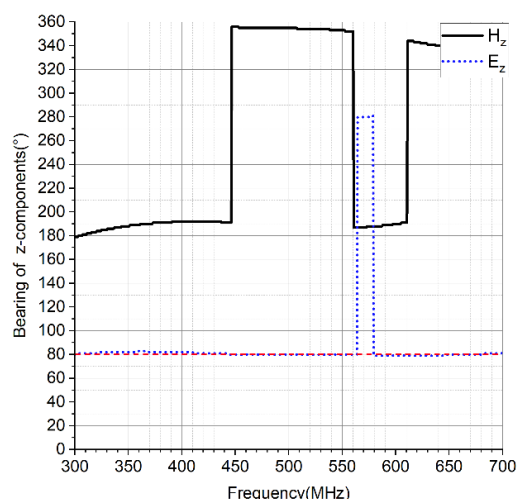
Рис. 3. Картина эффективной площади рассеяния БПЛА с векторными антенными элементами

Fig. 3. Pattern of the Radar Cross-Section of a UAV with Vector Antenna Elements

Для анализа возможности использования предложенного способа пеленгации БПЛА с векторными антенными элементами был облучен плоской электромагнитной волной с линейной поляризацией с углом прихода волны в 80° (азимут). Полученные картины пеленгов приводятся на рисунке 4.



a)



b)

Рис. 4. Пеленгация с использованием рассмотренного способа: а) определение направления прихода волны по суммарным компонентам поля; б) использование z-компонент поля

Fig. 4. Direction Finding Using Careful Analysis: a) Determining the Direction of Wave Arrival from the Cumulative Field Component; b) Using the z-Components of the Field

Так как исследование происходит в широком диапазоне частот, то для оценки точности выполнения пеленгации удобно использовать статистические показатели:

1) математическое ожидание пеленга:

$$m_1 = \frac{\sum_{n=1}^N x_n}{N}; \quad (19)$$

2) среднее квадратическое отклонение пеленга:

$$\sigma = \sqrt{\frac{\sum_{n=1}^N (x_n - tg)^2}{N}}; \quad (20)$$

3) ошибка пеленга:

$$er = \frac{\sum_{n=1}^N |x_n - tg|}{N}; \quad (21)$$

где x_n – мгновенные значения случайной величины (в нашем случае значение пеленга на частоте); N – число точек, в которых производится измерение пеленга; tg – истинное значение пеленга.

В данном случае, который приводится на рисунке 4, статистические показатели приводятся в таблице 1 (истинный угол волны 80°).

ТАБЛИЦА 1. Статистические показатели пеленгации при приходе плоской волны с горизонтальной поляризацией

TABLE 1. Statistical Indicators of Direction Finding at the Arrival of a Plane Wave with Horizontal Polarization

Параметр	H_Σ	E_Σ	H_z	E_z
m_1	78,567	101,359	296,743	89,994
σ	2,005	66,374	229,017	44,701
er	1,721	22,677	216,743	10,453

Полученные статистические данные показывают, что в диапазоне частот от 300 до 700 МГц наблюдается стабилизация результатов, а наиболее точное значение пеленга – при использовании суммарного поля магнитной компоненты. Таким образом видно, что магнитное поле является наименее подверженным к искажениям, которые возникают при измерении. Аналогичная ситуация сохраняется и при изменении угла элевации. Но зачастую пеленгационный комплекс облучается электромагнитной волной с эллиптической поляризацией, поэтому следует провести такое исследование для нее, чтобы оценить эффективность способа формирования ВАР.

Оценка точности метода формирования ВАР при падении эллиптической волны

Рассмотрим более сложную задачу, которая заключается в том, что пеленгатор облучается плоской волной с эллиптической поляризацией. Последняя возникает, когда значения компонент поля не совпадают, а разность фаз между составляющими кратна $\pi/2$ или вне зависимости от величины компонент поля разность фаз не кратна $\pi/2$.

Выражения, которые определяют такое поле, имеют вид:

$$|\mathcal{E}_x| \neq |\mathcal{E}_y| \Rightarrow E_{x0} \neq E_{y0}, \quad (22)$$

$$\begin{aligned} \Delta\varphi &= \varphi_y - \varphi_x = \\ &= \begin{cases} +\left(\frac{1}{2} + 2n\right)\pi, n = 0, 1, 2, 3, \dots RH \\ -\left(\frac{1}{2} + 2n\right)\pi, n = 0, 1, 2, 3, \dots LH \end{cases} \end{aligned} \quad (23)$$

или

$$\Delta\varphi = \varphi_y - \varphi_x \neq \pm \frac{n}{2}\pi = \begin{cases} > 0, RH \\ < 0, LH \end{cases}. \quad (24)$$

Так как вектор напряженности поля изобразит в пространстве эллипс, то у такой поляризации будет осевое отношение (AR):

$$AR = \frac{\text{большая ось}}{\text{малая ось}} = \frac{OA}{OB}, \quad 1 \leq AR < \infty, \quad (25)$$

где OA и OB определяются по выражениям (26 и 27).

При исследовании осевое отношение было выбрано 10 к 1, разность фаз между компонентами 90° . Моделирование выполнялось в диапазоне от 300 до 700 МГц для азимутальных углов от 0° до 180° с шагом в 20° . На рисунке 5 приводятся картины пеленгов для эллиптической поляризации.

Полученные графики показывают, что применение предложенного способа позволяет сохранить высокую точность обнаружения при формировании ВАР, однако чуть уменьшается диапазон частот, в котором возможна точная пеленгация – от 400 до 700 МГц. Также можно отметить, что при облучении эллиптической волной высокой точностью обладает пеленгация на основе H_z -компоненты поля, что, однако, дает промахи при облучении плоской волной. В таблице 2 приводятся статистические показатели при использовании магнитных диполей при пеленгации электромагнитной волны с эллиптической поляризацией. Значения выделены цветом в соответствии с величиной СКО (см. примечание к таблице 2).

Таким образом, по статистическим показателям отчетливо видно, что использование виртуальных магнитных диполей позволяет значительно повысить точность по сравнению с классической пеленгацией на основе электрических компонент поля. При выполнении пеленгации эллиптической волны отчетливо видно, что наибольшую точность обеспечивает пеленгация по z -компоненте магнитного поля.

$$OA = \left[\frac{1}{2} \left\{ E_{x0}^2 + E_{y0}^2 + [E_{x0}^4 + E_{y0}^4 + 2E_{x0}^2 E_{y0}^2 \cos(2\Delta\varphi)]^{1/2} \right\} \right]^{1/2}, \quad (26)$$

$$OB = \left[\frac{1}{2} \left\{ E_{x0}^2 + E_{y0}^2 - [E_{x0}^4 + E_{y0}^4 + 2E_{x0}^2 E_{y0}^2 \cos(2\Delta\varphi)]^{1/2} \right\} \right]^{1/2}. \quad (27)$$

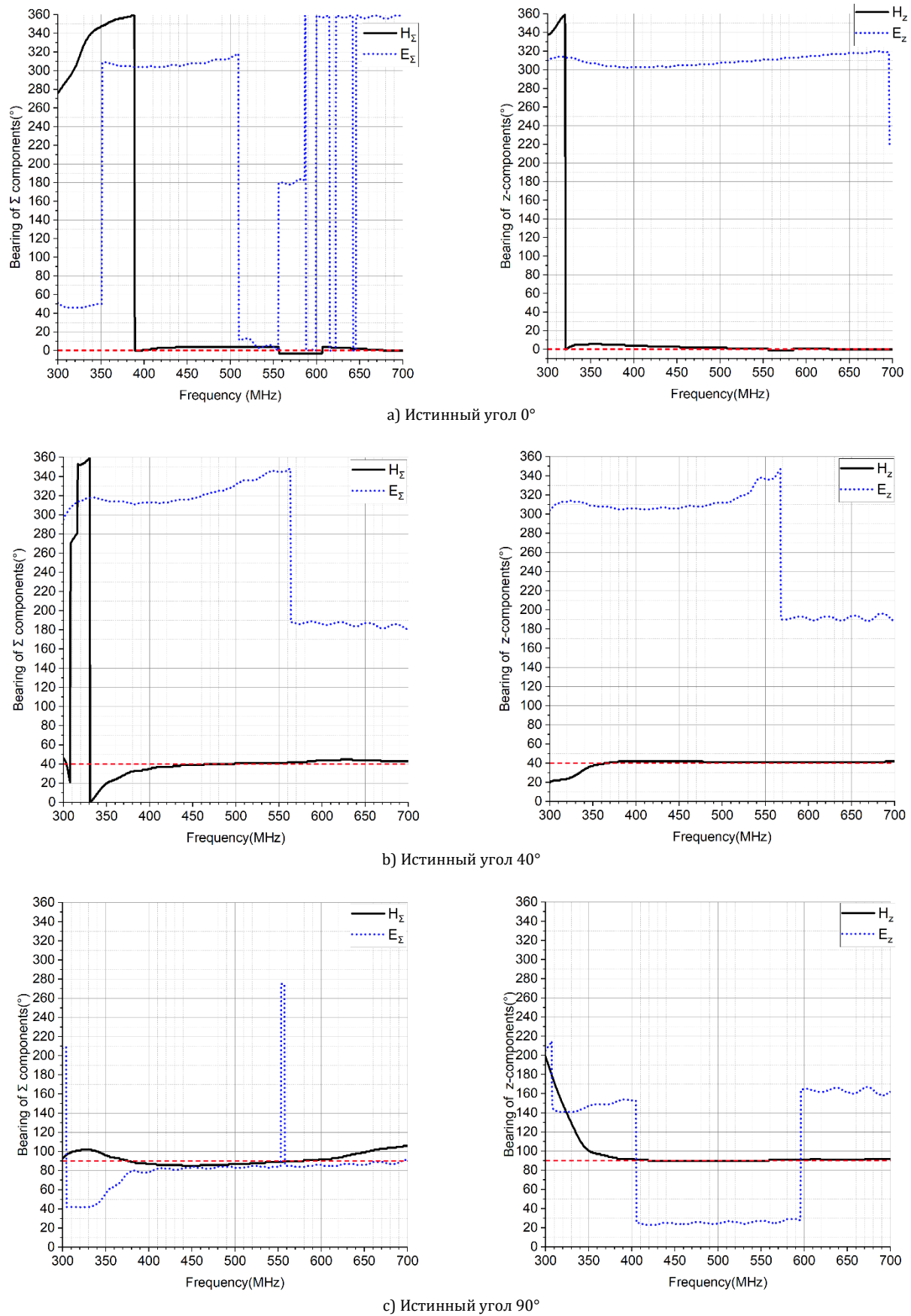


Рис. 5. Значения истинных пеленгов при облучении эллиптической электромагнитной волной: а) 0°; б) 40°; в) 90°

Fig. 5. Values of True Bearings when Irradiated by an Elliptical Electromagnetic Wave: a) 0°; b) 40°; c) 90°

ТАБЛИЦА 2. Статистические показатели пеленгации при приходе плоской волны с эллиптической поляризацией

TABLE 2. Statistical Indicators of Direction Finding at the Arrival of a Plane Wave with Elliptical Polarization

Истинный пеленг, °	H_x			E_x			H_z			E_z		
	m_1	σ	er	m_1	σ	er	m_1	σ	er	m_1	σ	er
0	1,9	3,2	3,0	236,7	274,1	236,7	1,2	1,8	1,4	310,6	310,6	310,6
20	23,9	4,4	4,0	273,8	267,9	255,8	23,6	3,7	3,6	299,9	282,0	279,9
40	41,3	2,7	2,3	265,6	236,4	225,6	41,3	1,4	1,3	263,1	231,5	223,0
60	58,7	4,6	4,0	52,9	52,2	43,8	59,0	1,6	1,4	143,1	98,8	96,7
80	77,2	5,4	4,3	110,4	87,0	43,0	79,6	2,0	1,8	157,0	78,9	78,8
90	90,9	5,8	4,4	87,2	23,0	8,1	90,6	0,9	0,6	72,7	67,5	67,4
100	105,0	6,3	5,0	101,8	35,7	13,2	101,7	2,0	1,7	64,8	65,8	65,6
120	122,5	2,9	2,5	128,9	45,2	23,1	121,8	1,9	1,8	104,9	49,5	37,7
140	141,2	3,6	3,2	130,5	11,3	9,5	140,4	0,8	0,6	211,8	91,9	85,7
160	161,2	7,3	6,2	101,2	84,0	58,8	158,8	1,3	1,2	224,9	73,0	71,4
180	176,7	6,5	3,9	191,4	48,6	27,3	181,0	1,6	1,0	128,5	51,8	51,5
среднее	–	4,8	3,9	–	105,9	85,9	–	1,7	1,5	–	127,4	124,4

Условные обозначения:

 $\sigma = 0 \dots 1,0$ $\sigma = 1,1 \dots 5,0$ $\sigma = 5,1 \dots 10,0$ $\sigma = 10,1 \dots 20,0$ $\sigma \geq 20,1$

Заключение

Предложенный в данной статье способ формирования виртуальных магнитных диполей позволяет значительно повысить точность пеленгации электромагнитных волн по сравнению с пеленгацией на основе электрических компонент волн. Можно выделить, что наиболее оптимальным является использование суммарного поля магнитной компоненты H_x , так как их применение позволяет сохранить высокую точность пеленгации при любом типе электромагнитных волн. Применение предложенной конструкции пеленгатора обеспечивает обнаружение в диапазоне от 0° до 360° по азимуту, при этом угол элевации может быть любым от -90° до 90° . Если требуется выполнить обнаружение электромагнитной волны с эллиптической поляризацией, то наиболее оптимальным является использование H_z -компоненты электромагнитных волн. Проведенное исследование показывает высокую эффективность методов ВАР при формировании комплексов пеленгации

Подтверждена гипотеза о том, что корпус носителя радиопеленгаторной антенной системы явля-

ется рассеивателем электрического типа, в ближней зоне рассеянных волн которого отношение напряженности электрической компоненты поля к ее магнитной компоненте существенно превышает величину характеристического сопротивления свободного пространства. В результате корпус носителя существенно в большей степени искажает электрическое поле падающих волн. Поэтому для минимизации инструментальной погрешности измерений пеленгов, вызванных дифракцией волн на носителе, предпочтительным является пеленгование по магнитному полю.

Однако измерять электрическое поле гораздо проще с точки зрения технической реализации, т. к. электрически экранированные рамочные антенны имеют огромную добротность и сложны для согласования с трактом с волновым сопротивлением 50 Ом. Поэтому в статье предложено измерять сильно искаженное электрическое поле с помощью векторных антенных элементов, далее вычислять значения магнитных компонент поля и оценивать угловые координаты источников радиоизлучения с их использованием.

Список источников

1. Vaskelainen L.I. Virtual array synthesis method for planar array antennas // IEEE Transactions on Antennas and Propagation. 1998. Vol. 46. Iss. 3. PP. 391–396. DOI:10.1109/8.662658
2. Dawood H.S., El-Khobby H.A., Elnaby M.M.A., Hussein A.H. Optimized VAA Based Synthesis of Elliptical Cylindrical Antenna Array for SLL Reduction and Beam Thinning Using Minimum Number of Elements // IEEE Access. 2021. Vol. 9. PP. 50949–50960. DOI:10.1109/ACCESS.2021.3069795.
3. Deng H., Himed B. A Virtual Antenna Beamforming (VAB) Approach for Radar Systems by Using Orthogonal Coding Waveforms // IEEE Transactions on Antennas and Propagation. 2009. Vol. 57. Iss. 2. PP. 425–435. DOI:10.1109/TAP.2008.2011387

4. Li W., Li Y., Guo L., Yu W. Adaptive beamforming method for arc length based virtual antenna array // IEEE International Workshop on Electromagnetics, Applications and Student Innovation (IWEM, Taipei, Taiwan, 08–10 August 2011). IEEE, 2011. PP. 135–139. DOI:10.1109/IWEM.2011.6021492
5. Mudonhi A., D'Errico R., Oestges C. Indoor mmWave Channel Characterization with Large Virtual Antenna Arrays // Proceedings of the 14th European Conference on Antennas and Propagation (EuCAP, Copenhagen, Denmark, 15–20 March 2020). IEEE, 2020. PP. 1–5. DOI:10.23919/EuCAP48036.2020.9135628
6. Hirota A., Arai H., Nakano M. Characteristics of Virtual Planar Array Antenna for Direction-of-arrival Estimation // Proceedings of the European Conference on Wireless Technology (Manchester, UK, 10–12 September 2006). IEEE, 2006. PP. 51–54. DOI:10.1109/ECWT.2006.280432
7. Yang X., Lin D., Zhang F., Song T., Jiang T. High Accuracy Active Stand-off Target Geolocation Using UAV Platform // Proceedings of the International Conference on Signal, Information and Data Processing (ICSIDP, Chongqing, China, 11–13 December 2019). IEEE, 2019. PP. 1–4. DOI:10.1109/ICSIDP47821.2019.9172919

References

1. Vaskelainen L.I. Virtual array synthesis method for planar array antennas. *IEEE Transactions on Antennas and Propagation*. 1998;46(3):391–396. DOI:10.1109/8.662658
2. Dawood H.S., El-Khobby H.A., Elnaby M.M.A., Hussein A.H. Optimized VAA Based Synthesis of Elliptical Cylindrical Antenna Array for SLL Reduction and Beam Thinning Using Minimum Number of Elements. *IEEE Access*. 2021;9:50949–50960. DOI:10.1109/ACCESS.2021.3069795
3. Deng H., Himed B. A Virtual Antenna Beamforming (VAB) Approach for Radar Systems by Using Orthogonal Coding Waveforms. *IEEE Transactions on Antennas and Propagation*. 2009;57(2):425–435. DOI:10.1109/TAP.2008.2011387
4. Li W., Li Y., Guo L., Yu W. Adaptive beamforming method for arc length based virtual antenna array. *IEEE International Workshop on Electromagnetics, Applications and Student Innovation, IWEM, 08–10 August 2011, Taipei, Taiwan*. IEEE; 2011. p.135–139. DOI:10.1109/IWEM.2011.6021492
5. Mudonhi A., D'Errico R., Oestges C. Indoor mmWave Channel Characterization with Large Virtual Antenna Arrays. *Proceedings of the 14th European Conference on Antennas and Propagation, EuCAP, 15–20 March 2020, Copenhagen, Denmark*. IEEE; 2020. p.1–5. DOI:10.23919/EuCAP48036.2020.9135628
6. Hirota A., Arai H., Nakano M. Characteristics of Virtual Planar Array Antenna for Direction-of-arrival Estimation. *Proceedings of the European Conference on Wireless Technology, 10–12 September 2006, Manchester, UK*. IEEE; 2006. p.51–54. DOI:10.1109/ECWT.2006.280432
7. Yang X., Lin D., Zhang F., Song T., Jiang T. High Accuracy Active Stand-off Target Geolocation Using UAV Platform. *Proceedings of the International Conference on Signal, Information and Data Processing, ICSIDP, 11–13 December 2019, Chongqing, China*. IEEE; 2019. p.1–4. DOI:10.1109/ICSIDP47821.2019.9172919

Статья поступила в редакцию 13.10.2022; одобрена после рецензирования 31.10.2022; принята к публикации 01.11.2022.

The article was submitted 13.10.2022; approved after reviewing 31.10.2022; accepted for publication 01.11.2022.

Информация об авторах:

ИЩЕНКО
Евгений Алексеевич

аспирант кафедры «Радиоэлектронных устройств и систем» Воронежского государственного технического университета,
 <https://orcid.org/0000-0002-5270-0792>

ПАСТЕРНАК
Юрий Геннадьевич

доктор технических наук, профессор кафедры «Радиоэлектронных устройств и систем» Воронежского государственного технического университета,
 <https://orcid.org/0000-0002-2031-5531>

ПЕНДЮРИН
Владимир Андреевич

генеральный директор АО НПП «Автоматизированные системы связи»,
 <https://orcid.org/0000-0002-4697-5976>

ФЁДОРОВ
Сергей Михайлович

кандидат технических наук, доцент кафедры «Радиоэлектронных устройств и систем» Воронежского государственного технического университета,
 <https://orcid.org/0000-0001-9027-6163>

Научная статья

УДК 681.5

DOI:10.31854/1813-324X-2022-8-4-48-54



Современный подход к сбору и обработке данных от автоматической идентификационной системы в целях организации управления движением судов

Владимир Владимирович Каретников, karetnikovvv@gumrf.ru

Яна Владимировна Косяк ✉, kosjakjv@gumrf.ru

Олег Олегович Данилов, oleg-danelov@yandex.ru

Александр Павлович Беспалов, bespalov.aleksandr.p@gmail.com

Государственный университет морского и речного флота имени адмирала С.О. Макарова,
Санкт-Петербург, 198035, Российская Федерация

Аннотация: Статья посвящена вопросу сбора и обобщения автоматической идентификационной системой (АИС) данных о движении судов, как по внутренним водным путям, так и в прибрежных морских районах. Определен перечень информации, необходимой для дальнейшего проведения исследований по организации движения. В работе уделено внимание особенностям получения данных, поступающих от технических средств связи и открытых онлайн-ресурсов. Предложен подход к накоплению статистических данных от приемника АИС с применением одноплатного микрокомпьютера Raspberry Pi. Реализовано приложение, осуществляющее чтение данных с последовательного порта и их передачу в библиотеку, а затем на сервер системы управления базами данных PostgreSQL. Сделан вывод о конструктивности и потенциальной эффективности предложенного подхода.

Ключевые слова: система управления движением судов, организация движения, автоматическая идентификационная система (АИС), Raspberry Pi, приемник АИС

Ссылка для цитирования: Каретников В.В., Косяк Я.В., Данилов О.О., Беспалов А.П. Современный подход к сбору и обработке данных от автоматической идентификационной системы в целях организации управления движением судов // Труды учебных заведений связи. 2022. Т. 8. № 4. С. 48–54. DOI:10.31854/1813-324X-2022-8-4-48-54

Modern Approach to Data Collection and Processing from Automatic Identification System for Ship Traffic Organization

Vladimir Karetnikov, karetnikovvv@gumrf.ru

Yana Kosiak ✉, kosjakjv@gumrf.ru

Oleg Danilov, oleg-danelov@yandex.ru

Alexander Bespalov, bespalov.aleksandr.p@gmail.com

Admiral Makarov State University of Maritime and Inland Shipping,
St. Petersburg, 198035, Russian Federation

Abstract: The article is devoted to the collection and generalization of automatic identification system (AIS) data on the movement of ships, both on inland waterways and in coastal marine areas. The list of information necessary for the further carrying out of researches on the organization of movement is defined. Attention is paid to the peculiarities of obtaining data from technical means of communication and open online resources. The approach to statistical data accumulation from AIS receiver using Raspberry Pi single-board microcomputer has been offered. The application, which reads data from the serial port and transfers them to the library and then to the PostgreSQL database management system server, is implemented. It is concluded that the proposed approach is constructive and potentially effective.

Keywords: vessel traffic control system, traffic organization, automatic identification system (AIS), Raspberry Pi, AIS receiver

For citation: Karetnikov V., Kosiak Ya., Danilov O., Bespalov A. Modern Approach to Data Collection and Processing from Automatic Identification System for Ship Traffic Organization. *Proc. of Telecom. Universities.* 2022;8(4):48–54. (in Russ.) DOI:10.31854/1813-324X-2022-8-4-48-54

Введение

В настоящее время оперативный контроль за безопасностью судоходства в прибрежных морских акваториях и на внутренних водных путях осуществляется специализированными системами управления движением судов [1]. Жизнедеятельность этих систем взаимосвязана с решением определенного рода задач, а именно:

- 1) постоянный мониторинг и получение сведений о навигационной обстановке от различного рода источников информации;
- 2) синтезирование данных в табличном виде и перевод их в графический вид в совокупности с многослойными электронными картами;
- 3) систематический и оперативный контроль за движением судов;
- 4) анализ текущей навигационной обстановки;
- 5) предоставление вспомогательной навигационной и прочей информации;
- 6) непрерывная запись информации для последующего ее воспроизведения [2].

Как известно [3], управление судном может быть автоматизированным процессом в определенной степени. Кроме того, увеличивается нагрузка на операторов вышеуказанных систем и судоводителей из-за постоянного роста интенсивности движения судов, что влечет за собой снижение времени на принятие решения по обеспечению безопасности судоходства. Это может быть мотивом для повышения уровня автоматизации контроля навигационной ситуации с целью обеспечения безопасности судоходства в акватории. В таком случае для обеспечения необходимого уровня безопасности движения судоходства нужно разрабатывать эффективные алгоритмы оценки навигационной безопасности плавания судов, надежность которых можно оценить, например, на основе сопоставительного анализа расчетных и натурных данных. Постановка натурных экспериментов, как правило, ведет к существенным временным и финансовым затратам, поэтому часто прибегают к вычислительным экспериментам и математическому моделированию.

В таком случае предпочтение стоит отдавать данным, получаемым от береговых автоматических идентификационных систем (АИС), так как они содержат информацию о реальном перемещении судов в исследуемой акватории. Кроме того, предложенный подход позволит собрать значительные объемы натурных данных для их последующей обработки.

Отечественный опыт применения технологии АИС

Разработка СУДС началась в начале 1990-х гг. [4]. Одним из основных элементов таких систем являются базовые станции АИС. Рассмотрим отечественный опыт внедрения СУДС с применением технологии АИС.

Система AIS-Monitor производства Группы «Транзас» предлагает широкий спектр возможностей для применения технологии АИС. Система предоставляет информацию о судах, оснащенных АИС, при этом программа имеет удобный и интуитивно понятный интерфейс, а также расширенный набор функций для эффективного управления навигацией. [5].

AIS-Monitor применяется в портах и гаванях средних размеров, где нет необходимости использовать береговые радиолокационные станции. Система значительно снижает риски, которые могут возникнуть при морских операциях, и помогает предотвратить опасные ситуации, связанные с движением судов. Основными функциями системы являются фильтрация и интеграция данных из различных источников АИС, автоматический захват, переопределение и идентификация целей АИС, визуализация данных АИС и передача данных.

Программный продукт «Речная Информационная Система» (РИС) производства Группы «Транзас» был разработан специально для обеспечения безопасной навигации на внутренних водных путях. Система предоставляет широкие возможности планирования движения судов по рекам и прибрежным водам, внося, таким образом, весомый

вклад в процесс эффективного использования внутренних водных путей. Функциональность данной системы: поддерживает АИС внутренних водных путей; отображение динамической и статической информации АИС; отображение специализированной речной информации АИС, отображение дополнительных статических данных АИС для внутренних водных путей; передача и получение текстовых телеграмм АИС, включая специализированные телеграммы для внутренних водных путей [6].

Федеральное бюджетное учреждение «Администрация Волго-Балтийского бассейна внутренних водных путей» (ФБУ «Волго-Балт») отвечает за организацию судоходства и его безопасность на внутренних водных путях Северо-Запада России [7]. Для работы АИС необходима сеть береговых станций, а каждое судно, совершающее плавание в зоне действия АИС, должно иметь на борту судовое оборудование АИС (транспондер). Береговая сеть АИС ФБУ «Волго-Балт» состоит из 23 центральных серверных береговых приемных станций и сетевых устройств, позволяющих каждому диспетчеру на линии получать общую картину движения по Волго-Балтийскому водному пути.

Астраханский филиал ФГУП «Росморпорт» предоставляет судам, осуществляющим судозаходы в морские порты Астрахань и Оля или следующие через акватории морских портов транзитом, навигационные услуги с использованием системы управления движением судов в морских портах Астрахань и Оля (далее – СУДС портов Астрахань и Оля) [8]. Были установлены базовые станции АИС, АИС-приемники и рабочие места диспетчеров. Данные АИС от СУДС и от сенсоров АИС Волжского ГБУ собираются на серверах ФГУП Росморпорт. Все данные АИС в реальном режиме времени регистрируются в БД с возможностью воспроизведения, а также статистического анализа.

Модели, методы и алгоритмы, реализованные современными СУДС, привлекают внимание исследователей. Разработка наиболее эффективных алгоритмов, обеспечивающих максимальную безопасность движения судов, является актуальной научной задачей.

Для изучения задач коллективного движения судов необходимы массивы данных, содержащие координаты нескольких судов, движущихся одновременно и влияющих на безопасность друг друга, т. е. находящихся в одной акватории, помимо этого, данные должны храниться и накапливаться с течением времени. Требуются непрерывные выборки данных небольшой продолжительности и небольшого расстояния между местоположениями судов. С учетом типичных размеров корабля точность определения координат должна быть достаточно высокой [9]. Важными для последующего

анализа параметрами движения являются скорость и курс судна.

Методы и материалы

Для проведения исследований по организации движений судов необходимо наличие следующей информации:

- статической – номер MMSI (*аббр. от англ.* Maritime Mobile Service Identity), позывной, габариты, тип судна и т. д.;
- динамической – координаты судна, время, курс, скорость, угловая скорость поворота, навигационный статус и т. д.;
- рейсовой – пункт назначения, время прибытия и т. д. [10].

Указанные данные можно получать из различных источников. Во-первых, – напрямую от базовой станции, транспондера или приемника АИС; во-вторых, – из открытых источников данных специализированных информационных ресурсов в среде Internet. К таким информационным ресурсам можно отнести: Marine-Traffic [11]; FleetMon [12]; VesselFinder [13] и др. Использование подобных ресурсов позволяет практически полностью отказаться от покупки реального оборудования, что позволяет сократить финансовые затраты на получение данных. Однако стоит отметить, что без организации физического доступа к оборудованию и своевременного получения данных с АИС затрудняется задача исследования. Кроме того, необходимо отметить, что в отдельных случаях сервер может работать с перебоями, что приводит к задержке передачи информации. Это влечет за собой непригодность использования таких данных в реальном времени без предварительного ее накопления.

Также указанные ресурсы не обладают пользовательским интерфейсом для автоматической загрузки данных. Если нет возможности прямого подключения к базовой станции АИС или их сетям, достаточно актуальным решением с точки зрения поставленной задачи может считаться применение приемника АИС.

Варианты решений и настройка программного обеспечения

С целью эффективного онлайн-мониторинга флота необходимо, чтобы на судах было установлено специализированное радиотехническое оборудование и высокоточные измерительные устройства, в совокупности, позволяющие обеспечить сбор и передачу данных в диспетчерское специализированное программное обеспечение (СПО). На сегодняшний день эта задача решается за счет установки бортовых контроллеров (навигационных блоков), которые определяют координаты судна по навигационным сигналам Глобальной

навигационной спутниковой системы и передают их на сервер. Данные о местоположении и параметрах движения судна передаются вместе с информацией, которая поступает от дополнительных датчиков информации [10]. Исходя из этого, СПО системы мониторинга должно обладать достаточным функционалом для визуализации местоположения судов и отображения контролируемых параметров в реальном времени.

АИС-приемник в основном имеет два интерфейса для передачи данных: UART (*аббр. от англ. Universal Asynchronous Receiver-Transmitter* – универсальный асинхронный приемопередатчик) и USB (*аббр. от англ. Universal Serial Bus* – универсальная последовательная шина).

UART – узел вычислительных устройств, организующий связи с другими цифровыми устройствами, а также изменяющий в последовательный вид данные, передаваемые по одной физической цифровой линии другому аналогичному устройству. Указанный выше способ преобразования стандартизован и довольно часто используется в компьютерной технике, в частности во встраиваемых устройствах [14]. UART представляет из себя логическую схему, которая с одной стороны подключена к шине вычислительного устройства, а с другой – имеет два или более выводов для внешнего соединения, и применяется для передачи данных через последовательный порт компьютера. Интерфейс USB равносителен UART. Он реализует виртуальный последовательный порт в системе. Существенным отличием является то, что через данный порт есть возможность обеспечивать питание АИС.

В случае данного проекта для чтения данных из АИС и ее дальнейшей передачи в базу данных на одноплатный микрокомпьютер Raspberry Pi была установлена операционная система (ОС) Raspberry Pi OS, основанная на ОС Debian. Raspberry Pi представляет собой миниатюрный одноплатный модуль с подключаемой периферией и питанием, который работает на базе Linux на бесплатной операционной системе Raspbian. С годами развития Raspberry Pi претерпела несколько модификаций и изменений, которые отличались от предшественников различными параметрами. Тем самым появилась возможность регулировать цену изделия, ориентируясь на потребности пользователей, что повысило популярность данного устройства. На рисунке 1 показан внешний вид использованной в работе платы Raspberry Pi B+.

При подключении АИС к микрокомпьютеру в системе автоматически появляется виртуальный последовательный порт «/dev/ttyACM0», который можно использовать для чтения данных с АИС (рисунк 2); байты сообщения АИС побитно передаются через него. После получения массива дан-

ных и последующей расшифровки с использованием кодировки ASCII получается сообщение вида, указанного на рисунке 3.

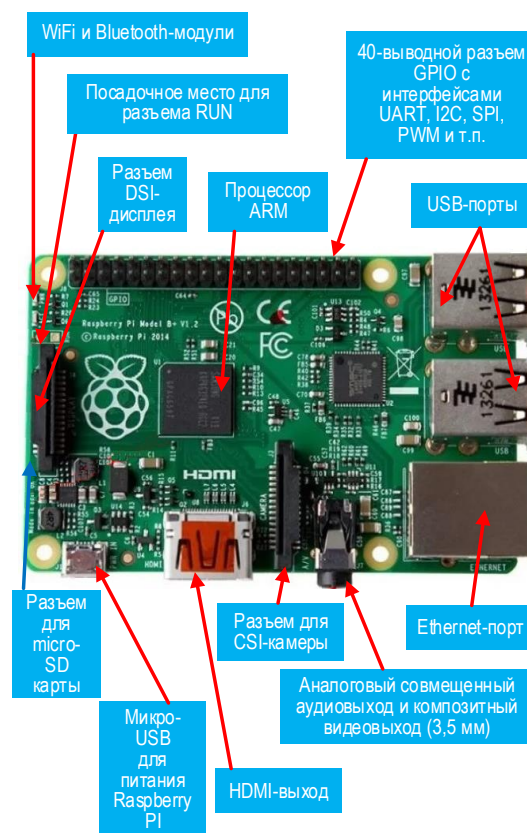


Рис. 1. Обзор составных элементов Raspberry Pi B+

Fig. 1. Raspberry Pi B+ Component Overview

Первоначально для проверки и настройки порта использовалось приложение Minicom (рисунк 4), доступное в диспетчере пакетов APT (*аббр. от англ. Advanced Packaging Tool*). Оно представляет из себя набор утилит для управления программными пакетами в ОС, которые основаны на Debian, и предоставляет следующие возможности: искать пакеты по заданным критериям; устанавливать, удалять и обновлять пакеты; манипулировать ключами от репозитория; решать зависимости; просматривать подробную информацию о пакете.

Minicom – это свободно распространяемая программа последовательной связи, которая работает под управлением LINUX и других вариантов ОС UNIX. Он работает, предоставляя эмулятор терминала для связи с другими устройствами через последовательный порт компьютера. Данное приложение позволяет настроить подключения через консольный интерпретатор, это позволяет быстро найти необходимые настройки для корректной работы порта. В последующем эти настройки будут использоваться для получения данных АИС, реализованным приложением. В данном случае наиболее приемлемый результат был получен при следующих настройках, указанных в таблице 1.


```

pi@raspberrypi: /dev $ ls
autofs      disk      griomem  loop3     mem       pts       ram2     raw       stderr    tty13    tty21    tty3     tty38    tty46    tty54    tty62    uinput    vcs3     vcsa4    vcsu4    video14
block       dma_heap hwrng    loop4     mmcblk0   ram0      ram3     rkill     stdin     tty14    tty22    tty30    tty39    tty47    tty55    tty63    urandom   vcs4     vcsa5    vcsu5    video15
bsg         fb0      initctl  loop5     mmcblk0p1 ram1      ram4     sda       stdout    tty15    tty23    tty31    tty4     tty48    tty56    tty7      v4l       vcs5     vcsa6    vcsu6    video16
btfs-control fd        input    loop6     mmcblk0p2 ram10     ram5     sda1      tty      tty16    tty24    tty32    tty40    tty49    tty57    tty8      vchig     vcs6     vcsa7    vcsu7    watchdog
bus         full     kmsg     loop7     mqeuqe    ram11     ram6     serial    tty0      tty17    tty25    tty33    tty41    tty5     tty58    tty9      vcio      vcs7     vcsm-cma vhsi     watchdog0
cachefiles  fuse     log      loop-control net       ram12     ram7     serial1   tty1      tty18    tty26    tty34    tty42    tty50    tty59    ttyACM0   vc-mem    vcsa     vcsu     video10  zero
char        gpiochip0 loop0     mapper    null      ram13     ram8     sg0       tty10     tty19    tty27    tty35    tty43    tty51    tty6     ttyAMA0   vcs       vcsa1    vcsu1    video11
console     gpiochip1 loop1     media0    ppp       ram14     ram9     shm       tty11     tty2     tty28    tty36    tty44    tty52    tty60    ttyprintk vcs1      vcsa2    vcsu2    video12
cuse        gpiochip2 loop2     media1    ptmx      ram15     random   snd       tty12     tty20    tty29    tty37    tty45    tty53    tty61    unid      vsc2     vcsa3    vcsu3    video13
pi@raspberrypi: /dev $

```

Рис. 2. Пример содержимого папки «/dev»

Fig. 2. Example Contents of the «/dev» Folder

!AIVDM,1,1,,B,177KQJ5000G?tO`K>RA1wUbN0TKH,0*5C

A B C

Рис. 3. Сообщение АИС после расшифровки с использованием кодировки ASCII

Fig. 3. AIS Message after Decoding Using ASCII Encoding

A – Последовательный порт	: /dev/ttyACM0
B – Размещение Lock-Файла	: /var/lock
C – Программа при выходе	
D – Программа при запуске	
E – Скорость/Четность/Биты	: 115200 8N1
F – Аппаратное управление потоком	: Да
G – Программное управление потоком	: Нет

Какую настройку изменить? |

Экран и клавиатура
 Сохранить настройки как dfi
 Сохранить настройки как...
 Выход
 Выход из Minicom

Рис. 4. Вид стартовой страницы приложения Minicom

Fig. 4. View of the Start Page of the Minicom Application

ТАБЛИЦА 1. Параметры для настройки последовательного порта

TABLE 1. Parameters for Configuring the Serial Port

Символьная скорость, бод	115200
Количество бит информации в пакете	8
Проверка на четность	нет
Стоп бит	1

Для дальнейшей работы с сообщением его необходимо проверить на корректность и расшифровать. Для этой задачи была реализована библиотека динамической компоновки «CAIS». Данная библиотека доступна на веб-сервисе для хостинга IT-проектов «GitHub». На вход библиотеки подается строка сообщения АИС, на выходе создается объект класса Message, хранящий в себе тип сообщения, основную информацию сообщения (часть A на рисунке 3) и расшифрованную нагрузку (часть B на рисунке 3) сообщения в зависимости от типа сообщения (рисунок 5).

```

Ссылка: 6
public AISType MessageType { get; set; }
Ссылка: 9
public string AISMessage { get; set; }
Ссылка: 14
public NMEA NMEA { get; set; }
Ссылка: 53
public Decoded Decoded { get; set; }

```

Рис. 5. Создание объекта класса Message с хранением типов сообщений

Fig. 5. Creating an Object of Message Class with Storing Message Types

Для полноценной функциональности описанной ранее библиотеки, реализовано приложение, осуществляющее чтение данных с последовательного порта, и передачу данных в библиотеку. После получения расшифрованного сообщения приложение отправляет его на сервер PostgreSQL. В случае возникновения ошибок при расшифровке или отправки сообщений на сервер, программа создает новое подключение к серверу системы управления базой данных (СУБД) и отправляет код ошибки, нерасшифрованное сообщение в специализированную таблицу. Эти данные в дальнейшем можно использовать для анализа ошибок.

База данных для хранения информации АИС

База данных для хранения информации АИС должна поддерживать как реляционный подход к хранению данных, так и объектный. Необходима поддержка большого количества типов записи информации (битовые строки, массивы данных и т. д.). Большинство СУБД рассчитаны на средние и небольшие проекты, есть ограничения по объему базы и количеству записей в ней, но для данного проекта объем хранимой информации будет достаточно высок, с учетом постоянного накопления данных о движении судов. Следовательно, у базы данных не должно быть ограничений по объему хранимой информации. Система должна справляться с задачами разбора и выполнения трудоемких операций, которые подразумевают и чтение, и запись, и валидацию одновременно. Учитывая особенность данной работы, доступ к базе данных необходимо получать с нескольких устройств, а также необходима возможность написания функций на языке C или Python.

Исходя из вышеперечисленных требований, для хранения и обработки данных, получаемых с АИС, выбрана свободная объектно-реляционная СУБД – PostgreSQL.

Получаемые данные импортируются в таблицы. Таблица «nmea» хранит основную информацию о полученном сообщении: индекс сообщения, его тип, ссылку на судно, ссылку на расшифрованное сообщение, исходное сообщение, дата и время записи данного сообщения в базу данных, ссылка на источник данного сообщения.

Таблица, в которой хранится информация о судне, содержит следующие поля: id (уникальный ID), name (название судна), mmsi (идентификационный номер морской мобильной службы), imo (номер судна Международной морской организации), позывной, тип судна.

Расшифрованные сообщения хранятся в таблицах, созданных для каждого типа сообщения, предусмотренного системой идентификации судов. Однако сообщения первых трех типов имеют одинаковую структуру и назначение, поэтому такие сообщения хранятся в одной таблице.

При возникновении ошибок во время расшифровки или добавления сообщений в базу данных, записывается информация о типе ошибки, исходное сообщение, время и дата записи в таблицу. Благодаря этой таблице можно выявить ошибки при работе системы.

Одной из проблем хранения данных является ссылка на расшифрованную часть сообщения: каждый тип сообщений хранится в специально созданной для него таблице. Ввиду этого, для полноценной работы необходимо реализовать отдельные столбцы, указывающие на каждую таблицу с сообщениями АИС. Следовательно, количество сохраняемой информации возрастает, так как необходимо для каждой записи в таблице «nmea» хранить 23 значения null. Это также влияет на сложность запросов в базу данных и скорость их выполнения.

Для уменьшения количества хранящихся данных и решения проблемы с ссылками была реализована схема, при которой в столбце «data» хра-

нятся индексы на записи в различных таблицах в зависимости от типа сообщения, указанного в столбце «type». Такой способ не решает проблему сложности запросов, так как приходится постоянно изменять тело запроса для различных типов сообщений. Для уменьшения нагрузки на пользователя базы данных создана функция, написанная на языке «С», которая реализует автоматическую замену имени таблицы в зависимости от типа сообщения. Этот язык выбран ввиду предварительно компиляции кода, что увеличивает скорость выполнения запросов с использованием данной функции.

Используя данный подход, возникает проблема удаления расшифрованных сообщений, так как при этом не проверяется существование ссылок на удаляемую запись в связи с отсутствием явного указателя на таблицу. Ввиду чего удаление данных запрещено для всех пользователей базы данных, за исключением администратора; он вручную проверяет наличие ссылки на удаляемую запись и удаляет и ее.

Заключение

Предложенный подход к накоплению статистических данных от приемника АИС с применением одноплатного микрокомпьютера Raspberry Pi прошел практическую апробацию и зарекомендовал себя как точный и эффективный с точки зрения онлайн-мониторинга внутреннего водного транспорта.

Таким образом можно сделать вывод, что предложенный в работе подход вполне конструктивен при решении задач сбора и обработки информации от АИС-подобных систем в целях оптимизации и организации движения судов при условии обеспечения необходимого уровня безопасности судоходства в районе развертывания системы управления движением судов. Причем предложенное решение конструктивно, как для прибрежных морских районов, так и на внутренних водных путях. Накопленные данные представляют собой исключительную ценность для проведения дальнейших исследований в области организации движения судов.

Список источников

1. Причкин О. Системы управления движением судов – горизонты развития // Морские вести России. 2020. № 5. URL: <http://www.morvesti.ru/themes/1693/85498> (дата обращения 14.12.2022)
2. Гриняк В.М. Разработка математических моделей обеспечения безопасности коллективного движения морских судов. Дис. ... докт. техн. наук. Владивосток: Дальневосточный федеральный университет, 2016. С. 297.
3. Шилов К.Ю., Суринов С.Н., Грек Б.В. Опыт разработки перспективной комплексной системы управления техническими средствами // Морской вестник. 2018. № 3(67). С. 93–95.
4. Шикломанова И.А. Водные ресурсы России и их использование. СПб.: ГГИ, 2008. 598 с.
5. Transas. URL: <http://www.transas.ru> (дата обращения 14.12.2022)
6. Титов А.В., Зайкова С.Н., Волынский И.А., Хмельницкая А.А. Современное состояние и проблемы использования внутренних водных путей (на примере Волго-Каспийского морского судоходного канала). Пенза: Научно-издательский центр «Социосфера», 2017. 528 с.
7. Сайт Администрации «Волго-Балт». URL: <https://volgo-balt.ru> (дата обращения 14.12.2022)

8. Баннов К.В., Баскин А.С. Опыт проектирования постов регулирования движения судов на акваториях портов // Морской транспорт. Экспресс-информация. Сер. Судовождение и связь. 1971. № 2(37). С. 3–12.
9. Гриняк В.М., Головченко Б.С., Малько В.Н. Распознавание опасных ситуаций системами управления движением судов // Транспорт: наука, техника, управление. Научный информационный сборник. 2011. № 8. С. 42–45.
10. Asborno M., Hernandez S., Mitchell K., Yves M. Inland waterway network mapping of AIS data for freight transportation planning // The Journal of Navigation. 2022. Vol. 75. Iss. 2. PP. 251–272. DOI:10.1017/S0373463321000953
11. Live Map // MarineTraffic. URL: <https://www.marinetraffic.com/en/ais/home/centerx:-12.0/centery:25.0/zoom:4> (Accessed 28.11.2021)
12. Fleetmon. URL: <https://www.fleetmon.com> (Accessed 28.11.2021)
13. VesselFinder. URL: <https://www.vesselfinder.com/ru> (Accessed 28.11.2021)
14. Навигационное оборудование // PHK. URL: https://radionavcom.ru/equip_radionav (дата обращения 12.11.2021)

References

1. Prichkin O. Vessel Traffic Control Systems – Development Horizons. *Morskije vesti Rossii*. 2020;5. (in Russ.) URL: <http://www.morvesti.ru/themes/1693/85498> [Accessed 14th December 2022]
2. Grinyak V.M. *Development of Mathematical Models to Ensure the Safety of Collective Movement of Ships*. D.Sc Thesis. Vladivostok: Far Eastern Federal University Publ.; 2016. 297 p. (in Russ.)
3. Shilov K.Y., Surin S.N., Grek B.V. Experience in Developing a Promising Integrated Control System for Technical Means. *Morskoy Vestnik*. 2018;3(67):93–95. (in Russ.)
4. Shiklomanova I.A. *Water Resources of Russia and Their Use*. St. Petersburg: State Hydrological Institute Publ.; 2008. 598 p. (in Russ.)
5. *Transas*. (in Russ.) URL: <http://www.transas.ru> [Accessed 14th December 2022]
6. Titov A.V., Zaikova S.N., Volynsky I.A., Khmel'nitskaya A.A. *Modern State and Problems of Using Inland Waterways (on the Example of the Volga-Caspian Marine Navigation Channel)*. Penza: Scientific-Publishing Center «Sotsiosfera» Publ.; 2017. 528 p. (in Russ.)
7. *Administration of the Volga-Baltic Basin of Inland Waterways*. (in Russ.) URL: <https://volgo-balt.ru> [Accessed 14th December 2022]
8. Bannov K.V., Baskin A.S. Experience in Designing Posts for Regulation of Vessel Traffic in Port Water Areas. *Morskoj transport. Ekspress-informaciya. Series: Sudovozhdenie i svyaz'*. 1971;2(37):3–12. (in Russ.)
9. Grinyak V.M., Golovchenko B.S., Malko V.N. Marine Safety Expert Information Systems. *Transport: science, equipment, management (Scientific Information Collection)*. 2011;8:42–45. (in Russ.)
10. Asborno M., Hernandez S., Mitchell K., Yves M. Inland waterway network mapping of AIS data for freight transportation planning. *The Journal of Navigation*. 2022;75(2):251–272. DOI:10.1017/S0373463321000953
11. *MarineTraffic*. Live Map URL: <https://www.marinetraffic.com/en/ais/home/centerx:-12.0/centery:25.0/zoom:4> [Accessed 28th November 2021]
12. *Fleetmon*. URL: <https://www.fleetmon.com> [Accessed 28th November 2021]
13. *VesselFinder*. URL: <https://www.vesselfinder.com/ru> [Accessed 28th November 2021]
14. *RNC*. Navigational Equipment. (in Russ.) URL: https://radionavcom.ru/equip_radionav [Accessed 11th November 2021]

Статья поступила в редакцию 01.06.2022; одобрена после рецензирования 20.07.2022; принята к публикации 01.08.2022.

The article was submitted 01.06.2022; approved after reviewing 20.07.2022; accepted for publication 01.08.2022.

Информация об авторах:

КАРЕТНИКОВ
Владимир Владимирович

доктор технических наук, доцент, заведующий кафедрой Судовождения на внутренних водных путях Государственного университета морского и речного флота имени адмирала С.О. Макарова

 <https://orcid.org/0000-0002-6857-8031>

КОСЯК
Яна Владимировна

директор центра дистанционного обучения управления информатизации Государственного университета морского и речного флота имени адмирала С.О. Макарова

 <https://orcid.org/0000-0002-6878-4273>

ДАНИЛОВ
Олег Олегович

лаборант кафедры Судовождения на внутренних водных путях Государственного университета морского и речного флота имени адмирала С.О. Макарова

 <https://orcid.org/0000-0001-8971-1375>

БЕСПАЛОВ
Александр Павлович

инженер кафедры Судовождения на внутренних водных путях Государственного университета морского и речного флота имени адмирала С.О. Макарова

 <https://orcid.org/0000-0001-7821-2423>

Научная статья

УДК 621.391

DOI:10.31854/1813-324X-2022-8-4-55-63



Usage of LDPC Codes in a Gilbert Channel

Andrey Ovchinnikov, mldoc@guap.ru

Alina Veresova, a.veresova@guap.ru

Anna Fominykh , aawat@ya.ru

Saint Petersburg State University of Aerospace Instrumentation,
Saint Petersburg, 190000, Russian Federation

Abstract: *Although low-density parity-check (LDPC) codes in modern communication standards have been extensively studied over a memoryless channel, their burst error correction capacity in channels with memory has yet to be thoroughly analyzed. The conventional approach to transmission in channels with memory uses interleaving within a buffer of several codewords. However, such an approach reduces the efficiency of the redundancy embedded by the error-correcting code. It is known from information theory that considering channel memory during decoding allows the transmission rate to be increased. An evaluation of the decoding error probability of different types of low-density parity-check codes in channels with memory is presented along with estimates of minimum distance and burst error correction capability for the considered codes. The decoding error probability is estimated for conventional decoding with deinterleaving and decoding taking channel memory into account. The decoding error probability is estimated for several parameters of a channel with memory and different buffer lengths. The obtained results reveal the absence of the unique decoding approach for all parameters of the channel with memory. The best decoding error probability is determined by the degree of channel memory correlation.*

Keywords: *low-density parity-check codes, channels with memory, burst error correction, interleaving*

Funding: This research was supported by Ministry of Science and Higher Education of the Russian Federation, grant No. FSRF-2020-0004, "Scientific basis for architectures and communication systems development of the onboard information and computer systems new generation in aviation, space systems and unmanned vehicles".

For citation: Ovchinnikov A., Veresova A., Fominykh A. Usage of LDPC Codes in a Gilbert Channel. *Proc. of Telecom. Universities*. 2022;8(4):55–63. (in Russ.) DOI:10.31854/1813-324X-2022-8-4-55-63

Об использовании низкоплотностных кодов в канале Гилберта

Андрей Анатольевич Овчинников, mldoc@guap.ru

Алина Максимовна Вересова, a.veresova@guap.ru

Анна Александровна Фоминых , aawat@ya.ru

Санкт-Петербургский государственный университет аэрокосмического приборостроения,
Санкт-Петербург, 190000, Российская Федерация

Аннотация: Коды с низкой плотностью проверок на четность для современных стандартов связи были тщательно изучены при использовании в каналах без памяти, но исправление пакетных ошибок с их помощью не было тщательно проанализировано. В статье исследуется декодирование различных типов кодов с низкой плотностью проверок на четность в каналах с памятью и приводятся оценки

минимального расстояния и пакетной корректирующей способности для набора низкоплотностных кодов. Рассматриваются различные сценарии декодирования для канала Гилберта, включая обычный алгоритм распространения доверия, алгоритм распространения доверия с дополнительным этапом оценки состояния канала, введение буфера с перемежением внутри буфера. Передача по каналу Гилберта сравнивается с каналом без памяти. Полученные результаты показывают, что вероятность ошибки сильно зависит от характеристик, связанных с памятью канала.

Ключевые слова: низкоплотностные коды, каналы с памятью, исправление пакетов ошибок, перемежение

Источник финансирования: Работа выполнена при финансовой поддержке Министерства науки и высшего образования Российской Федерации, соглашение № FSRF-2020-0004, «Научные основы построения архитектур и систем связи бортовых информационно-вычислительных комплексов нового поколения для авиационных, космических систем и беспилотных транспортных средств».

Ссылка для цитирования: Овчинников А.А., Вересова А.М., Фоминых А.А. Об использовании низкоплотностных кодов в канале Гилберта // Труды учебных заведений связи. 2022. Т. 8. № 4. С. 55–63. DOI:10.31854/1813-324X-2022-8-4-55-63

Introduction

Information processing and transmission technologies are a central feature of contemporary civilized life. As such, the corruption of data as a result of the transmission system's qualities, i.e., errors occurring during information transmission, storage, or processing, represents a highly undesirable scenario. Coding theory introduces error-correction methods by adding redundancy into the data, which the receiver may then utilize to recover the original message from the corrupted data [1]. Such redundancy may be added using various error-correcting codes, e.g., low-density parity-check (LDPC) codes, which are used in many modern standards.

LDPC codes, which were invented by R. G. Gallager in 1962 [2], are used to correct errors that appear during information transmission, storage, or processing. Due to the complexity of encoding and decoding procedures and computing limitations applying at that time, LDPC codes remained largely unused for at least 30 years. However, following their rediscovery by David MacKay in the 1990s and coinciding with a breakthrough in available computing power, LDPC codes became the topic of a new wave of interest due to offering near Shannon limit error correcting capability and the development of effective encoding and decoding procedures.

Over the years, use of LDPC codes in memoryless channels piqued the interest of researchers due to their excellent error-correcting characteristics. Furthermore, LDPC codes were chosen as an error correction scheme in the proposed 5G communication standard [3]. However, since the performance of LDPC codes across channels with memory has not been properly investigated, the present work will focus on this area.

When considering mathematical models of channels, the errors that emerge during transmission are usually thought to be independent. However, in real communication channels, errors due to channel

features are not independent: in this situation, the channel is said to have memory. The effect of memory in a channel may arise for several reasons, e.g., multipath propagation in fading channels [4], physical properties of storage systems, and propagation in wired channels. The existence of memory in the channel implies “unused” capacity, which encourages researchers to look for new methods for decoding dependent errors, i.e., bursts, that represent sections in transmitted sequences that may contain multiple errors, but outside of which the errors are absent or unlikely.

Although burst error correction is a well-known direction in coding theory, it is a much less researched area than independent error correction. The correction of error bursts requires the specific construction of codes (and decoding methods) aimed directly at correcting errors that appear in bursts. The typical approach to burst error correction used in modern communication standards is artificial channel decorrelation, which allows using the error-correcting code efficiently to correct independent errors. In many research papers, the estimation of decoding error probability is carried out by means of simulations, where independent errors are assumed following a binary symmetric channel (BSC) or channel with additive white Gaussian noise (AWGN). The decorrelation provided by interleaving decreases the effectiveness of the redundancy that was introduced by the error-correcting code. Another important issue is the adequateness of memoryless models to decorrelated channels with memory. In [5, 6] a method of decoding for channels with memory is described for extending the decoding procedure with an additional step. More specifically, the authors propose a channel state estimation step using the error grouping effect to lower the error probability. A comparison of random block permutation LDPC codes and Reed-Solomon codes in a Gilbert-Elliott channel is presented in [7]. In the present paper, we investigate the performance of the

LDPC codes in channels with memory based on a Gilbert model. The error correcting performance of different types of LDPC codes under conventional decoding with interleaving within the buffer is compared with decoding using knowledge about channel memory. The novelty of the paper is its investigation of decoding error probability provided by LDPC codes (including those from modern communication standards) in a Gilbert channel, considering both the known decoding methods and taking into account the specificity of the noise, as well as the decorrelation procedure for different interleaving depths, as compared to a theoretical memoryless case for infinite buffer size.

Channels with memory

When building both models of communication channels and methods of encoding and decoding the effect of noise on transmitted information is frequently represented using an additive model. The transmission can be expressed as $y = x + e$, where x is the transmitted symbol, y is the received symbol, and e is an error symbol. This formula is easily generalized to the vectors of length n as $\mathbf{y} = \mathbf{x} + \mathbf{e}$, where $\mathbf{y}$ is a received vector, $\mathbf{x}$ is a transmitted vector, $\mathbf{e}$ is an error vector. The error vector in channel models with memory comprises errors that appear in bursts.

Assuming that the channel might appear in different states during transmission and that the channel transitions from state to state over time, such a transition can be characterized in a mathematical model by appropriate transition probabilities.

Consequently, the channel can be described as a Markov chain of states, with the distinguishing feature that the Markov chain is hidden. As a consequence, there is typically no information about the state of the channel on the receiving side, implying that there is no information about the presence in a particular state of the Markov model, even with a given error vector generated by this model.

When the number of states of a communication channel is finite, the channel is called a channel with a finite number of states [8]. Such a finite-state channel model describes the states as binary symmetric channels, each having its own crossover probability. The model is frequently presumed to have only two states, namely “good” and “bad”. In a state G (good) the error probability is very low, while in state B (bad) the probability may differ depending on the channel model. Several derivations can be made using this model, such as the Gilbert model [9] (for which the error probability in the bad state is 0.5) and the Gilbert–Elliott model [10]. The Gilbert model, which is depicted in Figure 1, assumes that there are no errors in the “good” state, while errors appear with some probability in the “bad” state.

The generalization of the Gilbert model presented by E.O. Elliott in 1963 is based on the assumption that the “good” state is not error-free. The Gilbert–Elliott model describes a discrete memory channel in which the state of the channel depends on the previous state. The channel is described by two states $\Sigma = \{B, G\}$. In a “good” state, the bit error probability in the channel is P_G , while in a “bad” state P_B the probability of the channel switching from the bad to a good state is P_{BG} , while the probability of switching from good to bad is P_{GB} .

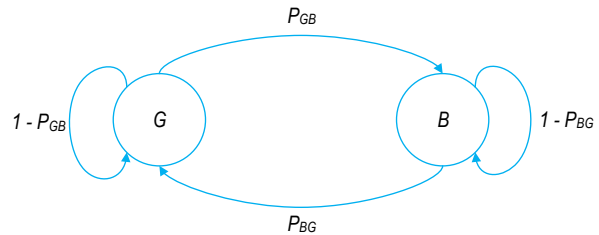


Fig. 1. Gilbert–Elliott Channel Model

LDPC codes

A binary (n, k) linear code is a k -dimensional subspace of an n -dimensional vector space over GF_2 . A LDPC code can be specified by a parity-check matrix $\mathbf{H}$. If the parity-check matrix of a code is sparse, then the corresponding code is called a low-density parity-check (LDPC) code. The sparseness of $\mathbf{H}$ leads to more efficient and faster decoding because, in comparison with a dense matrix, there is a lower number of nodes to process. If the row and column weights of the parity-check matrix are constant, then the LDPC code is said to be regular; otherwise, the LDPC code is said to be irregular. Although regular codes are easier to construct, irregular codes can provide superior performance [11]. A bipartite graph (Tanner graph) is commonly used to represent the parity-check matrix of LDPC code. This graph consists of a set of check nodes and variable nodes. The minimum distance of an (n, k) linear block code C , denoted by $d_{\min}$, is defined as the smallest Hamming distance between two different codewords in C due to the linear property. Finding the minimal distance of the LDPC codes is an NP-hard problem. A probabilistic algorithm described in [12] can be used to discover words of small weight in a linear binary code. Although the work factor of the algorithm is asymptotically quite large, the method can be applied to codes of medium size. In [13], a randomized LDPC code technique that considers the properties of such codes to search for low-weight codewords is presented. In Table 1 the minimum distances for a set of LDPC codes calculated using the aforementioned algorithm are presented. In the table, n is the length of the code, k is a number of information bits, and z is a block size, $d_{\min}$ is a minimum distance, while $b_{\max}$ is a burst error correction capability.

TABLE 1. Code Parameters

Code (n, k, z)	$d_{\min}$	$b_{\max}$
PEG code (1008, 504)	12	218
WiFi LDPC code (1296, 648, 54)	23	53
WiMax LDPC code (1344, 672, 56)	23	55
5G LDPC code (1105, 529, 24)	16	23
Gilbert code (1000, 500, 250)	4	248
RBP LDPC code (1000, 500, 50)	-	49

Code constructions

In the present work, several types of LDPC codes are considered, including progressive-edge growth (PEG) codes [14], codes from communication standards [3], random block-permutation (RBP) codes, and Gilbert codes. Gilbert codes were initially proposed to correct error bursts. In [15], a procedure for obtaining the code error-burst correction capability based on the codes' parameters is described.

The most popular construction of LDPC codes to permit compact representation and a flexible code construction approach is a block-permutation construction. Quasi-cyclic low-density parity-check codes (QC-LDPC codes), representing a special type of the block-permutation construction, are widely used in modern communication standards due to their simple encoding implementation by means of cyclic shift registers. The class of QC-LDPC codes is described by its parity-check matrix, which consists of circulants, i.e., cyclic-permutation matrices with a cyclic shift $i_{k,j}$:

$$\mathbf{H} = \begin{bmatrix} \mathbf{C}^{i_{1,1}} & \mathbf{C}^{i_{1,2}} & \dots & \mathbf{C}^{i_{1,\rho}} \\ \mathbf{C}^{i_{2,1}} & \mathbf{C}^{i_{2,2}} & \dots & \mathbf{C}^{i_{2,\rho}} \\ \dots & \dots & \dots & \dots \\ \mathbf{C}^{i_{\gamma,1}} & \mathbf{C}^{i_{\gamma,2}} & \dots & \mathbf{C}^{i_{\gamma,\rho}} \end{bmatrix},$$

where γ – number of matrices in a column; ρ is a number of matrices in a row; $\mathbf{C} - (z \times z)$ -cyclic permutation matrix:

$$\mathbf{C} = \begin{bmatrix} 0 & 0 & 0 & \dots & 0 & 1 \\ 1 & 0 & 0 & \dots & 0 & 0 \\ 0 & 1 & 0 & \dots & 0 & 0 \\ \dots & \dots & \dots & \dots & \dots & \dots \\ 0 & 0 & 0 & \dots & 1 & 0 \end{bmatrix}.$$

The QC-LDPC code is said to be regular if the matrix solely contains cyclic-permutation matrices. However, if some circulants are substituted with zero matrices, the code is called an irregular code [16]. A special case of block-permutation construction is a Gilbert code construction, whose modifications of the burst error-correcting capability b was analyzed in [15, 17]. A Gilbert code is defined by a parity-check matrix $\mathbf{H}$:

$$\mathbf{H}_l = \begin{bmatrix} \mathbf{I}_z & \mathbf{I}_z & \mathbf{I}_z & \dots & \mathbf{I}_z \\ \mathbf{I}_z & \mathbf{C} & \mathbf{C}^2 & \dots & \mathbf{C}^{l-1} \end{bmatrix},$$

where $\mathbf{I}_z - (z \times z)$ -identity matrix.

Decoding of LDPC codes

The decoding algorithms for LDPC codes are iterative procedures that operate on each symbol individually. These can be described in terms of passing messages over the edges of a Tanner graph between the check and variable nodes. The iterative nature of the algorithms refers to continuing decoding until the codeword has a zero syndrome or a predetermined number of iterations is reached. Since such iterative algorithms operate on each symbol separately, even when a large number of errors in the channel occurs and a wrong decision about the codeword is made, the bit error probability may remain low. The most common message passing algorithm with a hard decision is the bit-flipping (BF) algorithm, while the soft decision is the belief propagation (BP) algorithm, which is also known as a sum-product algorithm (SPA). Although these algorithms can provide low error probabilities, they do not guarantee error correction or burst error correction within the code error correction capability.

In [18], it was shown that, although BF cannot provide an acceptable error probability level in the case of burst error correction, it shows better results if the windowed BF is applied instead of the original BF. The BP algorithm was first presented in Gallager's work [2]. The messages passed along the edges of this algorithm are probabilities or beliefs. However, working with log-likelihoods rather than probabilities might be useful for reducing decoding complexity. The channel log-likelihood ratios for every received value y_j for Gilbert-Elliott channel are calculated as:

$$L(y_j) = 0.5(1 - 2y_j)\log((1 - P_e)/P_e),$$

where P_e – the probability that a bit error occurs in the channel at an arbitrarily selected moment of time:

$$P_e = (P_{GB}P_B + P_{BG}P_G)/(P_{GB} + P_{BG}). \quad (1)$$

For channels with memory, it was proposed in [5] to extend the original belief propagation decoding with a channel state estimation step. In the conventional decoding algorithm, the messages are passed between the variable and check nodes of the LDPC Tanner graph. In the extended version of the algorithm, messages are passed between the nodes of the Tanner graph, between the nodes in the channel subgraph, as well as between these two subgraphs.

The decoding algorithm with an estimation step consists of an iterative message passing between the channel subgraph and code subgraph. Generally speaking, the message passing schedule may vary; in this paper, the message passing is chosen to pursue the following schedule. In the first step, incoming channel messages are sent through the channel subgraph. The messages are passed between the states of the channel subgraph. Forward messages are passed from the initial to the final state, while backward messages are passed from the final state to the initial state. The

passing of messages represents the probabilities of the channel being in a specific state. Each message is a function of the previous message and the message received from the symbol node of the code graph. When the channel subgraph step is completed, the messages from the channel subgraph are passed to the code subgraph. Finally, conventional belief propagation decoding is performed.

Simulation results

In this section, the simulation results for different types of LDPC codes will be presented to evaluate the error-correcting performance using frame error rate (FER) criteria in the channel with memory. The goal of simulation is to estimate the decoding error probability per transmitted codeword in a Gilbert channel using various strategies to combat the correlated nature of the channel. On the one hand, the decoders which either use LLRs according to channel state estimation or providing single-burst correction, are considered. On the other hand, the effect of decorrelation is estimated for different buffer sizes and compared to theoretical memoryless infinite buffer case.

The general simulation scheme is presented in Figure 2. The source generates the binary data stream of length k , which is encoded by (n, k) LDPC code, obtaining an encoded binary stream of length n . Then, the buffer stores L codewords and applies interleaving within the buffer. The obtained stream is passed through the channel. Finally, the received data is deinterleaved and either fed to the channel estimator and channel decoder or passed directly to the channel decoder. In the case when buffer size is set to 1, the simulation assumes no interleaving. Thus, the considered model may be used to simulate a Gilbert channel, decorrelated Gilbert channel, or memoryless binary symmetric channel (BSC). Gilbert channel with parameters $P_{GB} = 0.01$ and $P_{GB} = 0.0001$, $P_B = 0.5$ and $P_G = 0$, as well as the corresponding BSC channel with P_e , are calculated according to (1). The value of P_{BG} varies: low values of P_{BG} mean long rare bursts and high values mean frequent short bursts.

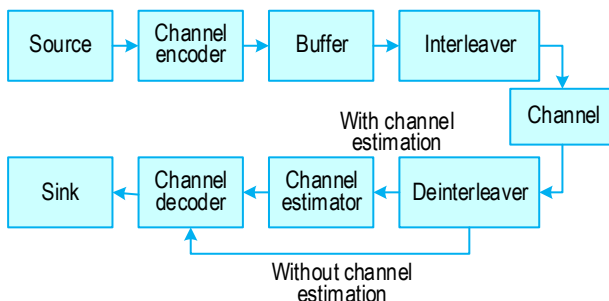


Fig. 2. Transmission Scheme

The codes and their parameters for which the simulations are obtained are presented in the Table 1. The decoding with interleaving is compared with decoding using knowledge about channel memory. The following scenarios are compared:

- 1) Belief propagation decoding (BP) in a Gilbert channel;
- 2) Belief propagation decoding with an additional channel estimation step (GE-BP) in a Gilbert channel;
- 3) Belief propagation decoding with interleaving inside the buffer in a Gilbert channel (the interleaving is applied inside the buffer, where L erroneous codewords are stored);
- 4) Belief propagation decoding in BSC channel with corresponding error probability (BP (BSC));
- 5) Decoding using an algorithm that is able to correct every single burst of length less than code error correction capability $b_{\max}$ in a Gilbert channel.

The simulation results for $P_{GB} = 0.01$, when the bursts are frequent, are presented in Figure 3. From the figures, it may be seen that GE-BP allows achieving a lower error probability due to the additional channel estimation step. It should be noted that introducing the buffer and using interleaving within the buffer permits a trade-off between FER performance and latency. The bigger the buffer, the better FER performance (gets closer to the decoding performance in the BSC channel) and the greater the latency. Both BP and GE-BP present better FER when considering lower values of P_{BG} , since the situation appears with long bursts and small gaps between bursts, which results in the big crossover probability in the corresponding BSC channel. In this case, decoding with interleaving performs worse than BP and GE-BP. The decoder that corrects every single burst of length less than code error correction capability $b_{\max}$ demonstrates unsatisfactory error correction since with $P_{GB} = 0.01$ and increasing P_{BG} , the bursts are short and frequent which is an unpleasant scenario for such a decoder.

Figure 4 present results for $P_{GB} = 0.0001$, when the bursts become rare. For small values of P_{BG} BP and GE-BP, the scheme with a buffer achieves lower values of FER comparing to the scheme with infinite buffer. Except for the last decoder that corrects single bursts, it may be seen that the curves behave similarly to the previous case with frequent bursts. Since the bursts have a sparser nature with $P_{GB} = 0.0001$, the decoder is able to correct a single burst within the codeword in contrast to the multiple bursts within the codeword when considering $P_{GB} = 0.01$.

From the simulation results, it can be seen that the range of values of the P_{BG} parameter may be divided into two areas: for small P_{BG} and high values of P_{BG} . For small P_{BG} (i.e., long error bursts), decoding considering the specifics of the presence of memory in the channel provides a gain in error probability compared to channel decorrelation. With increasing P_{BG} (with decreasing length of error bursts), the channel memory appears to a lesser extent, especially with frequent bursts, while the use of decorrelation shows a significantly better result; however, error probabilities provided by finite length buffer sizes may be far from infinite case.

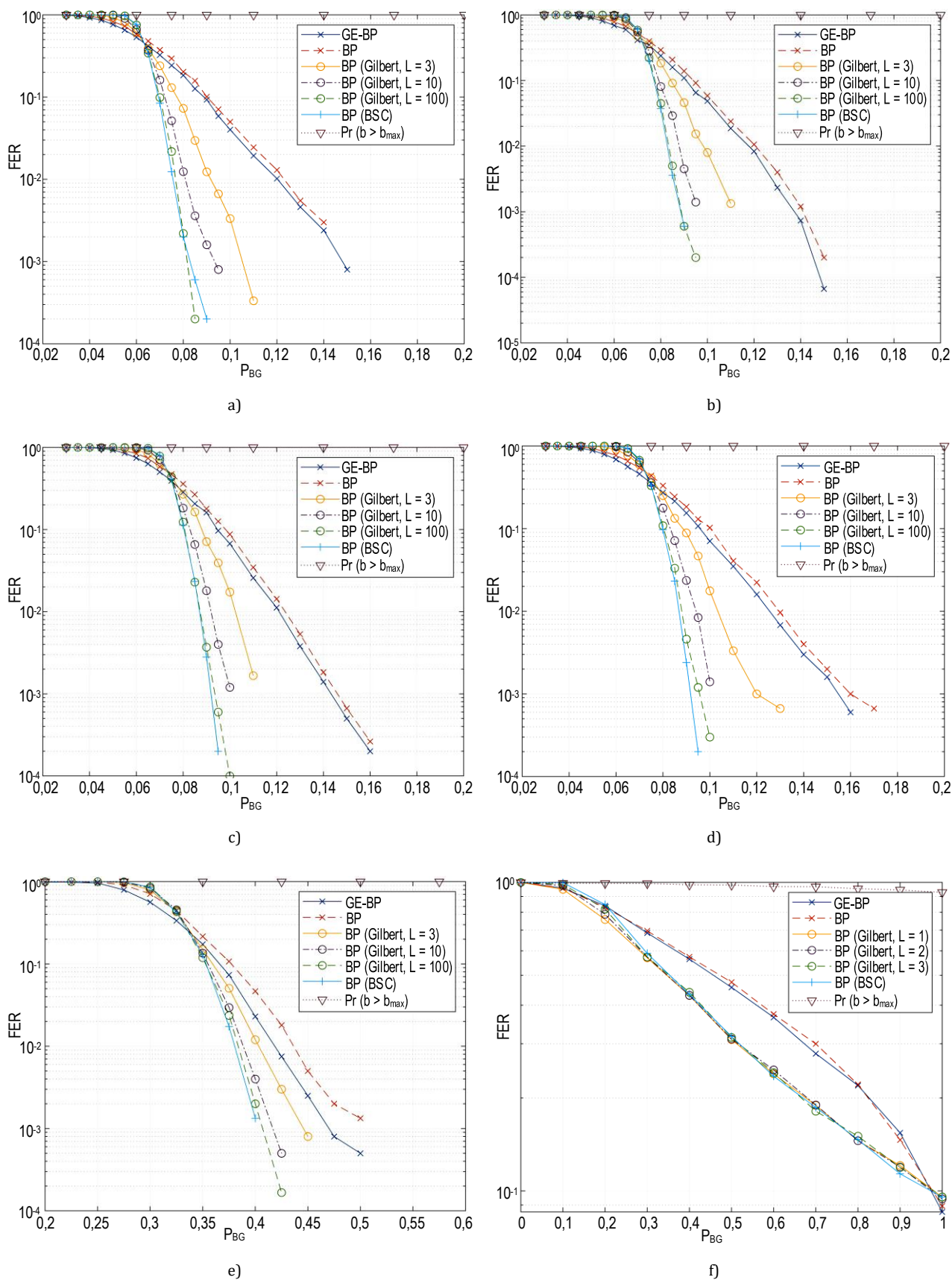


Fig. 3. FER for 5G LDPC code (a), WiFi LDPC code (b), WiMax LDPC code (c), PEG LDPC code (d), RBP LDPC code (e), Gilbert LDPC code (f) ($P_{GB} = 0.01$)

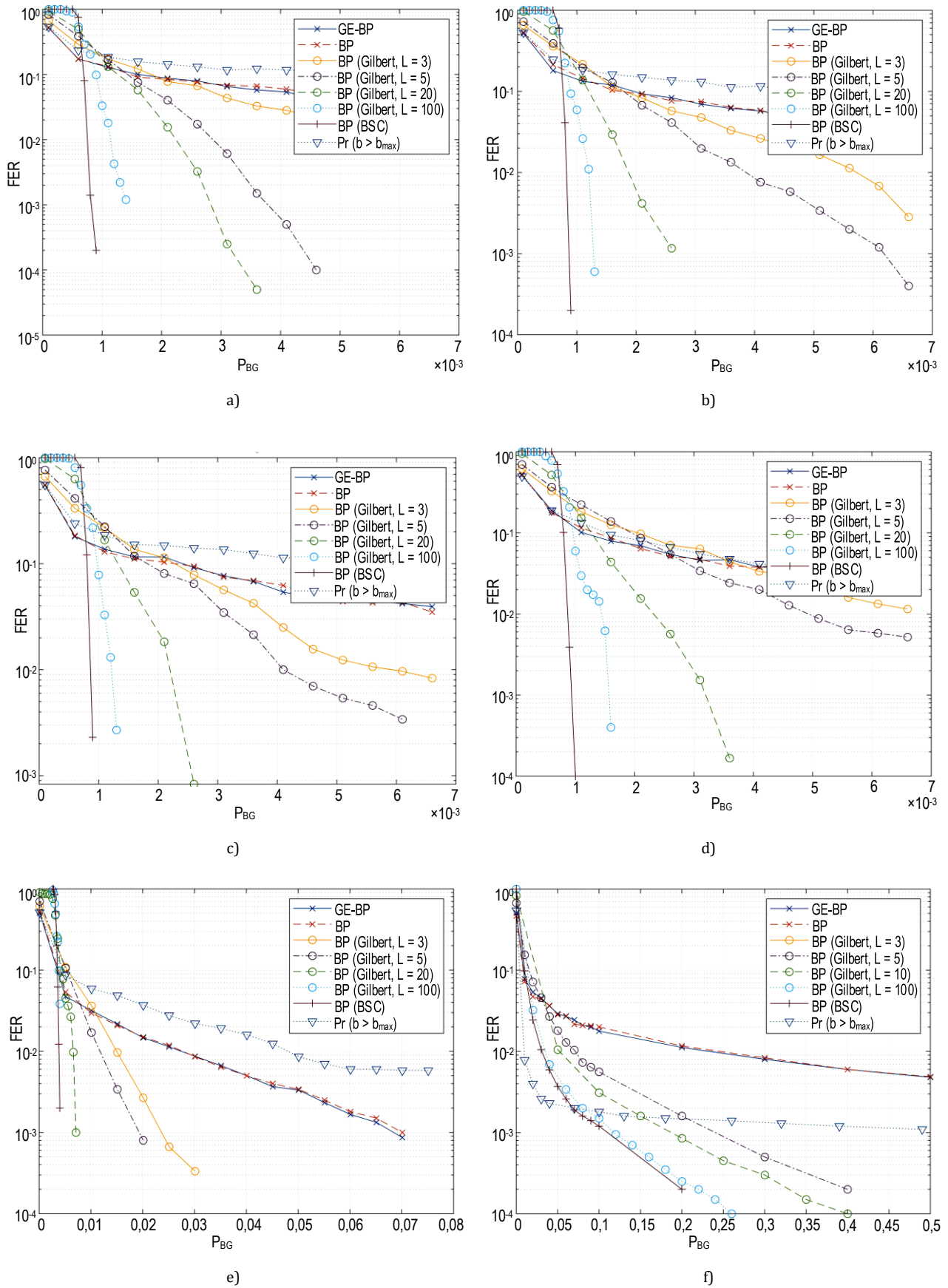


Fig. 4. FER for 5G LDPC code (a), WiFi LDPC code (b), WiMax LDPC code (c), PEG LDPC code (d), RBP LDPC code (e), Gilbert LDPC code (f) ($P_{GB} = 0.0001$)

Conclusion

The paper analyzes the decoding error correction performance of different types of LDPC codes in channels with memory. A conventional decoding approach with interleaving within the buffer is compared to decoding using knowledge of channel memory. The paper presents the estimations of the minimum distance and burst error correction capability of the considered codes. The investigated decoding error probability under different parameters of a channel with memory for various decoding scenarios demonstrates the existing gap between the decoding with interleaving and usage of channel memory. The specific point between the two scenarios, which represents the trade-off between the decoding

performance, is determined. For $P_{GB} = 0.01$, this point is observed at $P_{BG} = 0.07$ for codes from the modern standards and at $P_{BG} = 0.0007$ for $P_{GB} = 0.0001$. Decoding using knowledge about channel memory achieves a lower decoding error probability compared to the decoding with interleaving for long bursts. However, the opposite situation, when interleaving produces lower error probability, is observed for short bursts.

Existing decoding methods that take into account the channel memory do not provide a theoretically possible gain compared to decorrelation. Thus, increasing the reliability of transmission over channels with memory is possible both in the field of constructing new codes and new methods for decoding.

Reference

1. Lin S., Li J. *Fundamentals of Classical and Modern Error-Correcting Codes*. Cambridge: Cambridge University Press; 2022, 840 p.
2. Gallager R. Low-density parity-check codes. *IRE Transactions on Information Theory*. 1962;8(1):21–28. DOI:10.1109/TIT.1962.1057683
3. ETSI TS 138 212 V15.3.0 (2018-10). 5G. NR. Multiplexing and channel coding (3GPP TS 38.212 version 15.3.0 Release 15). Technical Specification. 101 p.
4. Holton T. *Digital Signal Processing: Principles and Applications*. Cambridge: Cambridge University Press; 2021. 1058 p.
5. Eckford A.W., Kschischang F.R., Pasupathy S. Analysis of low-density parity-check codes for the Gilbert-Elliott channel. *IEEE Transactions on Information Theory*. 2005;51(11):3872–3889. DOI:10.1109/TIT.2005.856934
6. Eckford A.W., Kschischang F.R., Pasupathy S. On Designing Good LDPC Codes for Markov Channels. *IEEE Transactions on Information Theory*. 2006;53(1):5–21. DOI:10.1109/TIT.2006.887467
7. Veresova A.M., Ovchinnikov A.A. Comparison of the Probability of Reed – Solomon and LDPC Codes Decoding Error in the Gilbert-Elliott Channel. *Proceedings of the Conference on Wave Electronics and its Application in Information and Telecommunication Systems, WECONF*, 30 May–03 June 2022, St. Petersburg, Russia. IEEE; 2022. DOI:10.1109/WECONF55058.2022.9803501
8. Shannon C.E. A mathematical theory of communication. *The Bell System Technical Journal*. 1948;27(3):379–423. DOI:10.1002/j.1538-7305.1948.tb01338.x
9. Gilbert E.N. Capacity of a Burst-Noise Channel. *Bell System Technical Journal*. 1960;39(5):1253–1265. DOI:10.1002/j.1538-7305.1960.tb03959.x
10. Elliott E.O. Estimates of error rates for codes on burst-noise channels. *The Bell System Technical Journal*. 1963;42(5):1977–1997. DOI:10.1002/j.1538-7305.1963.tb00955.x
11. Richardson T., Urbanke R. *Modern Coding Theory*. Cambridge: Cambridge University Press; 2008. 590 p.
12. Stern J. A method for finding codewords of small weight. *Proceedings of the 3rd International Colloquium on Coding Theory and Applications, 2–4 November 1988, Toulon, France. Lecture Notes in Computer Science, vol.388*. Berlin, Heidelberg: Springer; 1988. p.106–113. DOI:10.1007/BFb0019850
13. Hu X.-Y., Fossorier M.P.C., Eleftheriou E. On the computation of the minimum distance of low-density parity-check codes. *Proceedings of the International Conference on Communications (IEEE Cat. No.04CH37577)*, 20–24 June 2004, Paris, France, vol. 2. IEEE; 2004. p.767–771. DOI:10.1109/ICC.2004.1312605
14. MacKay D.J.C. Good error-correcting codes based on very sparse matrices. *IEEE Transactions on Information Theory*. 1999;45(2):399–431. DOI:10.1109/18.748992
15. Krouk E., Ovchinnikov A. Exact Burst-Correction Capability of Gilbert Codes. *Informatsionno-upravliaiushchie sistemy*. 2016;1:80–87. DOI:10.15217/issn1684-8853.2016.1.80
16. Fossorier M.P.C. Quasi-cyclic low-density parity-check codes from circulant permutation matrices. *IEEE Transactions on Information Theory*. 2004;50(8):1788–1793. DOI:10.1109/TIT.2004.831841
17. Krouk E., Ovchinnikov A. 2-Stripes Block-Circulant LDPC Codes for Single Bursts Correction. *Proceedings of the 9th International KES Conference on Intelligent Interactive Multimedia: Systems and Services, KES-IIMSS-16, 15–17 June 2016, Puerto de la Cruz, Tenerife, Spain. Smart Innovation, Systems and Technologies, vol.55*. Cham: Springer; 2016. p.11–23. DOI:10.1007/978-3-319-39345-2_2
18. Veresova A.M., Ovchinnikov A.A. About One Algorithm for Correcting Bursts Using Block-Permutation LDPC-Codes. *Proceedings of the Conference on Wave Electronics and its Application in Information and Telecommunication Systems, WECONF*, 03–07 June 2019, St. Petersburg, Russia. IEEE; 2019. DOI:10.1109/WECONF.2019.8840580

Список источников

1. Lin S., Li J. *Fundamentals of Classical and Modern Error-Correcting Codes*. Cambridge: Cambridge University Press, 2022. 840 p.
2. Gallager R. Low-density parity-check codes // *IRE Transactions on Information Theory*. 1962. Vol. 8. Iss. 1. PP. 21–28. DOI:10.1109/TIT.1962.1057683

3. ETSI TS 138 212 V15.3.0 (2018-10). *5G. NR. Multiplexing and channel coding (3GPP TS 38.212 version 15.3.0 Release 15). Technical Specification*. 101 p.
4. Holton T. *Digital Signal Processing: Principles and Applications*. Cambridge: Cambridge University Press, 2021. 1058 p.
5. Eckford A.W., Kschischang F.R., Pasupathy S. Analysis of low-density parity-check codes for the Gilbert-Elliott channel // *IEEE Transactions on Information Theory*. 2005. Vol. 51. Iss. 11. PP. 3872–3889. DOI:10.1109/TIT.2005.856934
6. Eckford A.W., Kschischang F.R., Pasupathy S. On designing good LDPC codes for Markov channels // *IEEE Transactions on Information Theory*. 2006. Vol. 53. Iss. 1. PP. 5–21. DOI:10.1109/TIT.2006.887467
7. Veresova A.M., Ovchinnikov A.A. Comparison of the Probability of Reed – Solomon and LDPC Codes Decoding Error in the Gilbert-Elliott Channel // *Proceedings of the Conference on Wave Electronics and its Application in Information and Telecommunication Systems (WECONF, St. Petersburg, Russia, 30 May–03 June 2022)*. IEEE, 2022. DOI:10.1109/WECONF55058.2022.9803501
8. Shannon C.E. A mathematical theory of communication // *The Bell System Technical Journal*. 1948. Vol. 27. Iss. 1. PP. 379–423. DOI:10.1002/j.1538-7305.1948.tb01338.x
9. Gilbert E.N. Capacity of a Burst-Noise Channel // *Bell System Technical Journal*. 1960. Vol. 39. Iss. 5. PP. 1253–1265. DOI:10.1002/j.1538-7305.1960.tb03959.x
10. Elliott E.O. Estimates of error rates for codes on burst-noise channels // *The Bell System Technical Journal*. 1963. Vol. 42. Iss. 5. PP. 1977–1997. DOI:10.1002/j.1538-7305.1963.tb00955.x
11. Richardson T., Urbanke R. *Modern Coding Theory*. Cambridge: Cambridge University Press, 2008. 590 p.
12. Stern J. A method for finding codewords of small weight // *Proceedings of the 3rd International Colloquium on Coding Theory and Applications (Toulon, France, 2–4 November 1988)*. Lecture Notes in Computer Science. Vol. 388. Berlin, Heidelberg: Springer, 1988. PP. 106–113. DOI:10.1007/BFb0019850
13. Hu X.-Y., Fossorier M.P.C., Eleftheriou E. On the computation of the minimum distance of low-density parity-check codes // *Proceedings of the International Conference on Communications (IEEE Cat. No.04CH37577, Paris, France, 20–24 June 2004)*. IEEE, 2004. Vol. 2. PP. 767–771. DOI:10.1109/ICC.2004.1312605
14. MacKay D.J.C. Good error-correcting codes based on very sparse matrices // *IEEE Transactions on Information Theory*. 1999. Vol. 45. Iss. 2. PP. 399–431. DOI:10.1109/18.748992
15. Krouk E., Ovchinnikov A. Exact Burst-Correction Capability of Gilbert Codes // *Informatsionno-upravliaiushchie sistemy*. 2016. Vol. 1. PP. 80–87. DOI:10.15217/issn1684-8853.2016.1.80
16. Fossorier M.P.C. Quasi-cyclic low-density parity-check codes from circulant permutation matrices // *IEEE Transactions on Information Theory*. 2004. Vol. 50. Iss. 8. PP. 1788–1793. DOI:10.1109/TIT.2004.831841
17. Krouk E., Ovchinnikov A. 2-Stripes Block-Circulant LDPC Codes for Single Bursts Correction // *Proceedings of the 9th International KES Conference on Intelligent Interactive Multimedia: Systems and Services (KES-IIMSS-16, Puerto de la Cruz, Tenerife, Spain, 15–17 June 2016)*. Smart Innovation, Systems and Technologies. Vol. 55. Cham: Springer, 2016. PP. 11–23. DOI:10.1007/978-3-319-39345-2_2
18. Veresova A.M., Ovchinnikov A.A. About One Algorithm for Correcting Bursts Using Block-Permutation LDPC-Codes // *Proceedings of the Conference on Wave Electronics and its Application in Information and Telecommunication Systems (WECONF, St. Petersburg, Russia, 03–07 June 2019)*. IEEE, 2019. DOI:10.1109/WECONF.2019.8840580

Статья поступила в редакцию 30.09.2022; одобрена после рецензирования 09.11.2022; принята к публикации 21.11.2022.

The article was submitted 30.09.2022; approved after reviewing 09.11.2022; accepted for publication 21.11.2022.

Информация об авторах:

ОВЧИННИКОВ
Андрей Анатольевич

кандидат технических наук, доцент кафедры инфокоммуникационных технологий и систем связи Санкт-Петербургского государственного университета аэрокосмического приборостроения,

 <https://orcid.org/0000-0002-8523-9429>

ВЕРЕСОВА
Алина Максимовна

аспирант кафедры инфокоммуникационных технологий и систем связи Санкт-Петербургского государственного университета аэрокосмического приборостроения,

 <https://orcid.org/0000-0002-3792-9249>

ФОМИНЫХ
Анна Александровна

ассистент кафедры инфокоммуникационных технологий и систем связи Санкт-Петербургского государственного университета аэрокосмического приборостроения

 <https://orcid.org/0000-0002-1412-5766>

ИНФОРМАЦИОННЫЕ ТЕХНОЛОГИИ И ТЕЛЕКОММУНИКАЦИИ

**2.3.1 – Системный анализ,
управление и обработка
информации**

**2.3.6 – Методы и системы защиты
информации, информационная
безопасность**

Научная статья

УДК 004.75

DOI:10.31854/1813-324X-2022-8-4-65-73



Модели применения блокчейн в государственных информационных системах

Василий Сергеевич Елагин, elagin.vas@gmail.com

Санкт-Петербургский государственный университет телекоммуникаций им. М.А. Бонч-Бруевича,
Санкт-Петербург, 193232, Российская Федерация

Аннотация: Целью статьи является исследование и моделирование отдельных аспектов (методов, алгоритмов обработки заявлений) внедрения технологии блокчейн в отдельные элементы государственных информационных систем. Для достижения поставленной цели в статье последовательно рассмотрены следующие вопросы: анализ технических возможностей блокчейн, анализ алгоритмов обработки заявлений на государственном портале, исследование технологической особенности развертывания сети блокчейн для повышения эффективности предоставления услуг, разработка аналитических соотношений для исследования зависимости времени обработки, разработка имитационной модели для исследования вероятностных характеристик времени обработки. В статье предложена модель применения технологии блокчейн в государственных информационных системах, например, на портале государственных услуг, с учетом большого числа органов власти, участвующих в процессе.

Ключевые слова: блокчейн, государственные информационные системы, портал госуслуг, аутентификация услуг, сетевые характеристики

Ссылка для цитирования: Елагин В.С. Модели применения блокчейн в государственных информационных системах // Труды учебных заведений связи. 2022. Т. 8. № 4. С. 65–73. DOI:10.31854/1813-324X-2022-8-4-65-73

Models of Blockchain Application in Government Information Systems

Vasiliy Elagin, elagin.vas@gmail.com

The Bonch-Bruevich Saint-Petersburg State University of Telecommunications,
St. Petersburg, 193232, Russian Federation

Abstract: The purpose of the article is to study and model certain aspects (methods, algorithms for processing applications) of introducing blockchain technology into individual elements of state information systems. To achieve this goal, the following issues are sequentially considered in the article: analysis of the technical capabilities of blockchain, analysis of algorithms for processing applications on the state portal, study of the technological features of deploying a blockchain network to improve the efficiency of service provision, development of analytical relationships for studying the dependence of processing time, development of a simulation model for research processing time probabilistic characteristics. The article proposes a model for the application of blockchain technology in public information systems, for example, on the portal of public services, taking into account the large number of authorities involved in the process.

Keywords: blockchain, government information systems, public services portal, service authentication, network characteristics

For citation: Elagin V. Models of Blockchain Application in Government Information Systems. *Proc. of Telecom. Universities*. 2022;8(4):65–73. (in Russ.) DOI:10.31854/1813-324X-2022-8-4-65-73

Введение

Технология Blockchain (*акр. от англ.* Blockchain – цепь из блоков; далее по тексту – блокчейн) – это сеть с распределенной базой данных (реестром). Информация в технологии блокчейн не хранится на одном узле, а дублируется на территориально распределенные аппаратно-программные комплексы по всему миру. Данную сеть из равнозначных компьютеров принято называть одноранговой или P2P-сетью (*от англ.* Peer-to-Peer – равный к равному). На каждом из таких компьютеров хранится полная версия блокчейн (полная цепочка блоков) и, при добавлении блока, информация на всех компьютерах обновляется. Это гарантирует, что информация общедоступна, не может быть подделана или удалена, а совершенные действия открыты к просмотру любым пользователям.

Параллельно происходит активное развитие информационных сервисов для государственных нужд. Государственная информационная система о государственных и муниципальных платежах (ГИС ГМП) – система, предназначенная для хранения и обмена информацией о платежах между администраторами доходов, организациями по приему платежей и гражданами, созданная в соответствии с Федеральным законом Российской Федерации от 27 июля 2010 г. № 210-ФЗ «Об организации предоставления государственных и муниципальных услуг».

Система «Управление» представляет собой комплекс информационных систем и информационных ресурсов, включающий центральную информационную систему, ведомственные информационные системы, информационные ресурсы которых предназначены для принятия управленческих решений в сфере государственного управления, а также информационные ресурсы иных информационных систем (в том числе региональных). Доступ к открытой части государственной информационной системы «Управление» осуществляется по адресу: <http://gasu.roskazna.ru>.

Единый портал государственных и муниципальных услуг (или Госуслуги) – это федеральная государственная информационная система. Она обеспечивает гражданам, предпринимателям и юридическим лицам доступ к сведениям о государственных и муниципальных учреждениях и оказываемых ими электронных услугах. Требования к ней перечислены в Постановлении Правительства Российской Федерации от 24 октября 2011 г. № 861 и других нормативно-правовых актах. Оператором портала назначено Министерство цифрового развития, связи и массовых коммуникаций Российской Федерации[1].

Стремительный рост развития и увеличение сфер применения трафика технологии блокчейн заставляет задуматься о применении концепции технологии в ГИС, например, такой системы как портал государственных услуг. Технические возможности, которые открывает блокчейн позволяют повысить эффективность предоставления услуг в государственных информационных системах, однако, первоначально необходимо оценить потенциальное воздействие технологии на сеть, аппаратные и программные ресурсы, для избежания негативных последствий. Поэтому целью статьи является исследование и моделирование отдельных аспектов (методов, алгоритмов обработки заявлений) внедрения технологии блокчейн в государственные информационные системы.

Технологические особенности блокчейн

В контексте поставленной цели следует выделить основные технологические преимущества блокчейн:

- децентрализация и распределенность;
- безопасность и защищенность;
- открытость и прозрачность;
- неизменность уже записанного.

Децентрализация и распределенность. Информация о транзакциях хранится на тысячах компьютерах, находящихся под владением майнеров, которые отвечают за проверку и добавление блокчейн в виде новых блоков. Майнеров может быть тысячи в одной сети, и над ними нет централизованного управления. Таким образом вся информация распределена на сети, а вероятность того, что все компьютеры выйдут из строя, ничтожно мала.

Безопасность и защищенность. Попытки взломать один из блоков и изменить информацию в нем не имеет смысла, поскольку изменять придется все блоки, а также копии базы на всех компьютерах, а для этого нужны колоссальные вычислительные мощности. К тому же препятствием к фальсификации является и мощный алгоритм шифрования с использованием хеш-функций, а также цифровой подписи. Чтобы изменить цифровую подпись на одном из блоков, нужно изменить цифровые подписи на последующих за ним блоках. Таким образом взломщик чисто физически не сможет поменять подписи на всех последующих блоках, так как их тысячи, и скорость создания новых блоков выше, чем скорость, с которой взломщик будет менять подписи на старых блоках.

Открытость и прозрачность. Вся база находится в публичном доступе, а потому посмотреть данные того или иного блока может любой желающий.

Неизменность уже записанного. Каждый вновь созданный блок в блокчейн содержит в зашифрованном виде данные о предыдущих блоках (хеш-сумма предыдущих блоков). Таким образом, технология блокчейн изначально предопределяет невозможность добавления фальшивого блока или изъятие существующего, поскольку это приведет к изменениям во всей системе. При удалении блока система точно такжеотреагирует на изменение глобальной структуры. Как результат – мошенничество, попытки несанкционированного вмешательства или то же пиратство практически исключены.

Однако необходимо отметить и недостатки блокчейн технологии, оказывающие существенное влияние на ее приложения, а именно:

- низкая масштабируемость (с увеличением количества пользователей происходит значительный рост размеров блока);
- мошенничество и ошибки (невозможно обратить ошибочные действия);
- низкая скорость обработки транзакций (медленный процесс обработки, особенно в сравнении с сетевой задержкой при использовании его в синхронных сервисах реального времени);
- отсутствие единого стандарта;
- ограничение объема данных, добавляемых в блок.

Архитектура портала Госуслуг

По мере расширения цифровой экономики неизбежно увеличивается потребность в цифровой трансформации государственных услуг. Формат цифрового сервиса не только удобен для потребителя, но одновременно с этим цифровой сервис позволяет предприятию автоматизировать и оптимизировать процессы и отдельные операции, лежащие в основе его предоставления [2]. Предоставление персонализированных услуг гражданам, предприятиям и некоммерческим организациям требует фундаментальных изменений в работе государственных учреждений путем интеграции процессов, объединения пользовательских данных и предоставления к ним доступа, а также интеграции как существующих, так и разрабатываемых информационных систем [3].

Эффективная информационная архитектура портала позволяет быстро, легко и интуитивно находить на нем интересующий контент. Это дает возможность избежать увеличения времени предоставления услуги при личном посещении государственных органов, предоставляющих услугу, или нахождение в очереди в единых МФЦ России.

Общая архитектура портала представлена на рисунке 1. Она позволяет увеличивать существующий функционал, а также добавлять к проекту новых участников для распараллеливания процесса разработки и совершенствования.

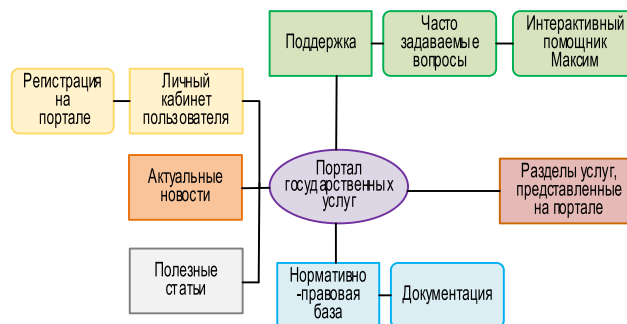


Рис. 1. Общая архитектура портала

Fig. 1. General Architecture of the Public Services Portal

Система межведомственного электронного взаимодействия

Единая система межведомственного электронного взаимодействия (СМЭВ) представляет собой федеральную ГИС, включающую информационные базы данных, в том числе содержащие сведения об используемых органами и организациями программных и технических средствах, гарантирующих возможность доступа посредством информационно-технического взаимодействия к их информационным системам, о программных и технических средствах, поддерживающих единый документированный способ взаимодействия информационных систем органов и организаций посредством технологии очередей электронных сообщений, обеспечивающей взаимодействие программ в асинхронном режиме, не требующим установки между ними прямой связи и гарантирующим получение передаваемых электронных сообщений, а также сведения об истории движения в системе взаимодействия электронных сообщений [4], и еще целый ряд контекстных сведений.

Обмениваться данными через СМЭВ органы власти должны в двух направлениях. Если заявитель запрашивает федеральную услугу, то территориальное подразделение федерального органа власти в случае необходимости должно иметь возможность получить сведения из регионального органа и (или) органа местного самоуправления. В случае, если заявитель обращается за региональной или муниципальной услугой, то чиновники должны суметь получить сведения в федеральном органе.

Общая схема работы сервиса представлена на рисунке 2. Сотрудник ведомства направляет запрос к сервису через СМЭВ. Сервис сохраняет поступивший запрос с указанием ведомства и его регистрирует. Далее сервис обращается к системе «Гостехнадзор Эксперт» для получения сведений. Затем система Гостехнадзора обрабатывает сам запрос и отдает результаты обработки на сервис СМЭВ, откуда отправляется ответ сотруднику ведомства – инициатору запроса.



Рис. 2. Общая схема работы СМЭВ

Fig. 2. Algorithm of Operation of the System of Interdepartmental Electronic Interaction

СМЭВ состоит из сети защищенных каналов связи между узлами, расположенными в центрах обработки данных.

Участники СМЭВ являются поставщиками и потребителями сведений:

- каждый поставщик публикует и регистрирует в СМЭВ свой электронный сервис, который предназначен для обработки запросов и выдачи сведений;
- каждый потребитель получает доступ к опубликованным сервисам в СМЭВ в случае необходимости, реализует адаптер, который умеет правильно запрашивать сведения и получать ответ.

Оператором СМЭВ является Министерство цифрового развития, связи и массовых коммуникаций Российской Федерации; посредством СМЭВ интегрирует между собой многочисленные федеральные и региональные информационные системы.

Обработка заявлений на портале государственных услуг

Порядок обработки заявлений на портале в общем виде представлена на рисунке 3. Пользователь открывает портал государственных услуг, входит в личный кабинет и выбирает категорию услуги. После этого открывается страница всех услуг представленной категории. Пользователь выбирает нужную услугу, заполняет необходимые параметры и формирует заявление на портале. Далее это заявление проходит обработку.

Процесс приема заявлений представлен на рисунке 4. Заявление вместе с необходимыми документами передается с портала Государственных услуг на «Веб-сервис СМЭВ Гостехнадзора». Далее оно проходит этап проверки и сохраняется в ведомственную систему, затем попадает в реестр (где ведется учет всех обработанных заявлений). После этого инспектор вручную проверяет заявление и приложенные к нему документы, через систему «Гостехнадзор Эксперт» отправляет на портал новый статус заявления, дату и время приема или

причину отказа. Сообщение автоматически подписывается электронной подписью органа власти. Таким образом обрабатываются все поступившие на портал заявления, в которых необходимо участие инспектора. Общую картину (архитектуру) можно увидеть на рисунке 5.



Рис. 3. Общая структура обработки заявлений на портале государственных услуг

Fig. 3. General Structure of Application Processing on the Public Services Portal

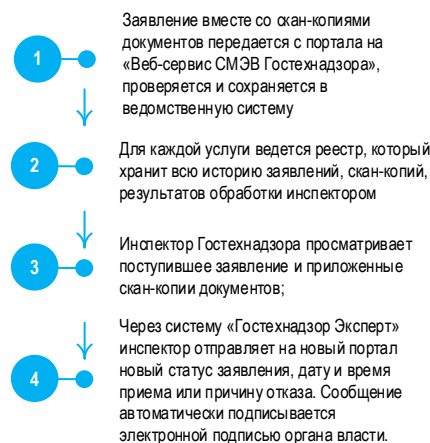


Рис. 4. Прием заявлений с портала

Fig. 4. Acceptance of Applications Via the Website

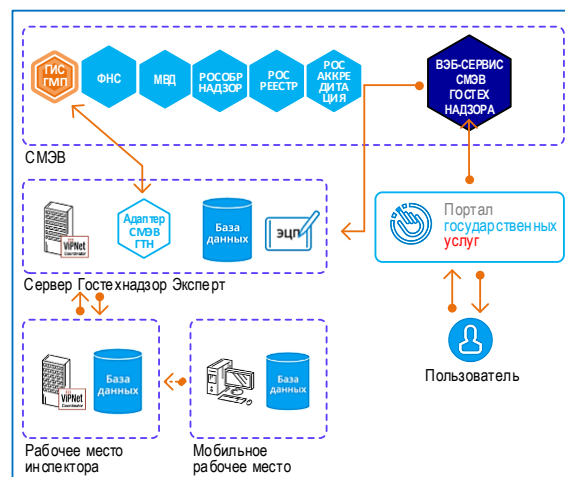


Рис. 5. Общая архитектура системы

Fig. 5. General Interaction Architecture

Алгоритм функционирования портала Госуслуги с использованием технологии блокчейн

Опираясь на вышесказанное, можно сделать вывод, что большая часть государственных услуг (а это примерно больше 170 уникальных услуг) оказывается при непосредственной работе инспектора. На диаграмме (рисунок 6) видно, что преимущественно услуги категорий «Справки и выписки», «Недвижимость/Стройка» и «Налоги/Финансы» обрабатываются инспектором. Инспектор проверяет правильность введенных данных, проверяет, есть ли у лица, подающего документы, необходимая недвижимость или льготы на оказание услуг, а также проверяет иную введенную информацию.



Рис. 6. Диаграмма распределения услуг по категориям

Fig. 6. Diagram of the Distribution of Services by Category

То есть, большая часть работы по проверке производится не автоматически, а при участии инспектора. Поэтому, если будет существовать доверительная система с защитой данных, для которой известно, что данные корректны, достоверны и защищены, это значительно снизит воздействие человеческого фактора на работу всего портала.

Система на базе технологии блокчейн, которая обладает всеми параметрами для этого, может частично заменить ручную обработку инспектора на автоматическую.

В этом случае алгоритм обработки заявки выглядел бы следующим образом:

- 1) пользователь портала выбирает услугу;
- 2) пользователь заполняет необходимые данные;
- 3) услуга формируется и отправляется на проверку;
- 4) система блокчейн заполняет личные данные о пользователе, после чего они подвергаются проверке;
- 5) система блокчейн шифрует данные и формирует блок;
- 6) затем эти данные попадают на систему СМЭВ;
- 7) система СМЭВ сохраняет заявление с документами в ведомственную систему;

8) для заявления на оказание услуги присваивается уникальный номер;

9) система СМЭВ по тегам отправляет заявление в необходимое ведомство;

10) в ведомстве заявление расшифровывается и попадает на рабочий стол сотрудника ведомства для оказания услуг, при этом последнему не нужно проверять правильность заполненных данных, так как он может доверять предыдущей цепочке, через которую прошло заявление;

11) пользователю оказывается услуга и ее результат возвращается ему по тому же алгоритму, только в обратном направлении.

Общий алгоритм оказания услуги с использованием блокчейн-системы представлен на рисунке 7.

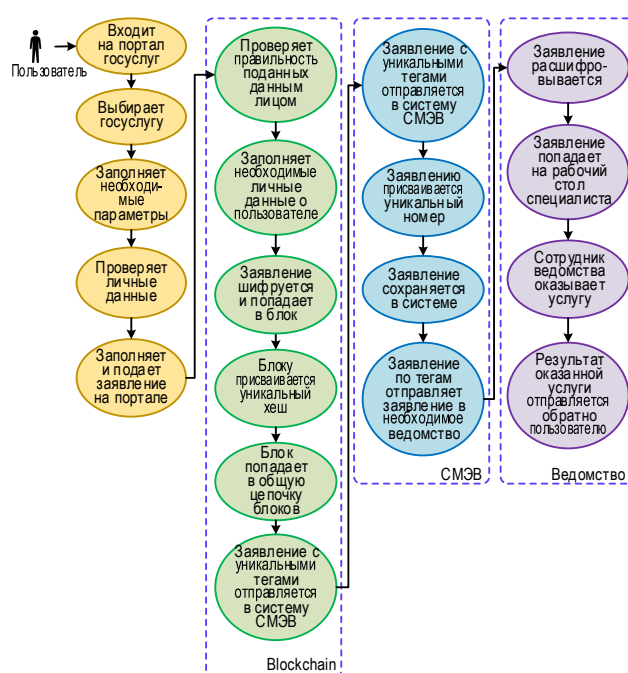


Рис. 7. Общий алгоритм оказания услуги на портале с использованием блокчейн системы

Fig. 7. A Generalized Algorithm for Providing Services on the Portal Using a Blockchain System

Таким образом, технологические решения вопроса использования блокчейн для автоматизации обработки запросов могут быть предоставлены, однако первоначально необходимо оценить вероятностно-временные характеристики работы портала Госуслуг при интеграции с блокчейн-системами. Технологически данная система может потребовать авторизацию услуг инспектором в нескольких государственных и региональных ведомствах для внесения в цепочку [5].

Как показано на рисунке 8, такая системная модель состоит из пяти компонентов: загрузчик (пользователь), список ведомств для авторизации данных, сервер, система блокчейн и Атор (верификатор). Пользователь загружает данные об услуге на портал; они должны быть аутентифицированы,

в нескольких ведомствах. Каждый орган использует функцию (f) подписей, и ему нужно только аутентифицировать свои данные – f (данные). Когда все ведомства успешно аутентифицируют данные, они подписывают ту их часть, за которую отвечают, и совместно создают подпись для общих данных.

Как показано на рисунке 9, информация об этом хранится в блокчейне: подписи, имя органа и дата аутентификации данных; окончательная подпись полных данных хранится в заголовке блока. Сервер отвечает за поддержание блокчейна и предоставление системных параметров для участвующих в процессе ведомств. Верификатор может запросить подпись данных на сервере и убедиться, что она действительна [6, 7].

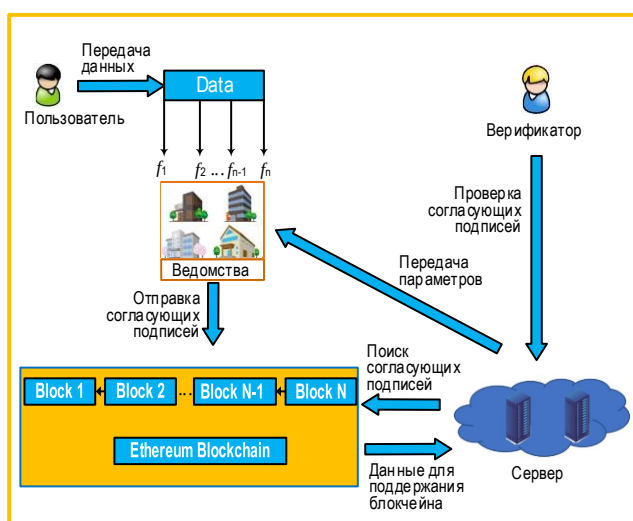


Рис. 8. Структура системной модели применения блокчейн

Fig. 8. The Structure of the System Model of Blockchain Application

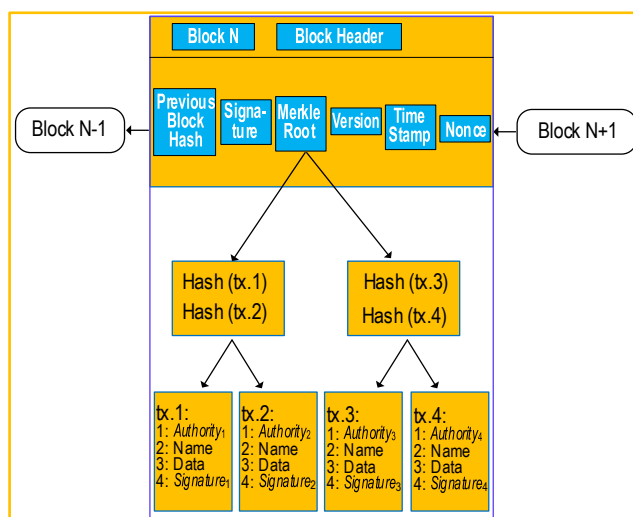


Рис. 9. Внутренняя структура блоков в предлагаемой системе

Fig. 9. The Internal Structure of the Blocks in the System

Модель системы включает в себя три различных этапа работы в смарт-контракте.

Этап 1. $\text{invokeF}(f)$ – алгоритм компилируется сервером и может выполняться законными властями. Сервер определяет, является ли функция f , вызванная этим органом, легитимной по возвращаемому значению.

Этап 2. $\text{addUser}(f, \text{ct.sender})$ – алгоритм может выполняться только сервером. Системная модель может динамически наделять полномочия с использованием функции f .

Этап 3. $\text{deleteUser}(f, \text{ct.sender})$ – алгоритм может выполняться только сервером. Системная модель может динамически отвергать использование органом власти функции f .

Построение децентрализованной сети в целях обеспечения всех преимуществ технологии блокчейн возможно; достаточным будет использование существующей аппаратно-программной инфраструктуры ГИС при соответствующей доустановке и обновлении программного обеспечения.

Так как процесс внедрения децентрализованной сети блокчейн-узлов внесет дополнительный объем трафика в инфокоммуникационную сеть, оценка которого пока не проводилась в рамках других исследований, приведенные ниже соотношения призваны помочь с оценкой влияния блокчейн-узлов на загрузку сети с учетом особенностей функционирования технологии [8].

Сетевые характеристики технологии блокчейн

Процесс сетевого взаимодействия и временные характеристики схемы, включая проблему поиска и хранения информации, нуждаются в оценке их значений в зависимости от параметров сети.

В рамках предложенной схемы можно выделить два основных процесса, формирующих задержку: аутентификацию данных в ведомствах и работу сервера.

В исследуемой схеме каждый орган власти должен выполнять одну хэш-функцию процедуры, связанную с формированием цифровой подписи, и одну – по формированию смарт-контракта. Каждый орган власти должен вызвать один смарт-контракт, чтобы использовать функцию f .

Таким образом, за исключением сетевой задержки, каждому ведомству потребуется время выполнения аутентификации данных:

$$T_{Ai} = T_h + T_{Sig} + T_{Sc},$$

где T_h , T_{Sig} , T_{Sc} – затраты времени на выполнение одной хэш-функции, формирование цифровой подписи и одного смарт-контракта, соответственно.

На сервере, в свою очередь, необходимо несколько раз запустить некоторый алгоритм генерации случайных чисел и обычные операции сложения и умножения (временные затраты на эти шаги незначительны). Кроме того, он запускает n

хэш-функций, а также значительные операции по генерации и проверке цифровых подписей в блоках и $n + 1$ раз просчитывает по расширенному Евклидову алгоритму.

Поэтому обработка операции на сервере требует следующих временных затрат:

$$T_S = nT_h + T_{SigServ} + (n + 1)T_{iny},$$

где T_{inv} , $T_{SigServ}$ – временные затраты на выполнение одного расширенного Евклидова алгоритма и на генерацию с проверкой цифровых подписей в блоках, состоящих из сложений и умножений случайных чисел в рамках криптографических алгоритмов [9].

Сетевую задержку при прохождении цикла транзакций между сервером и аутентифицирующими органами власти можно представить в виде выражения:

$$T_{Net} = (n^2 + 2n)T_{com},$$

где T_{com} – сетевая задержка при передаче одного сообщения между сервером и одним из аутентифицирующих органов власти; n – число аутентифицирующих органов власти; необходимо передать синхронизирующую транзакцию ($2n$), а также обновлять информацию при аутентификации каждым ведомством запроса (n^2).

Таким образом, можно представить результирующее время выполнения процедуры в следующем виде:

$$T_{Proc} = 2 \sum_{i=1}^n T_{Ai} + n^2 T_S + T_{Net}.$$

Для оценки значения временных затрат на выполнение предложенной схемы был использован персональный компьютер (RedmiBook с процессором AMD Ryzen 5 5600H с графикой Radeon @ 3,30 ГГц с 16,0 ГБ оперативной памяти и ОС Windows 10 Home). В рамках имитации была предложена схема взаимодействия с различным числом полномочных органов власти. Для этого была развернута система смарт-контракта с использованием языка Solidity и Ropsten Ethereum [10] для тестирования сети с рядом установленных параметров. Компилятором языка Solidity является Remix IDE и его версия 0.7.4.

В рамках схемы множественной аутентификации пользователей были обозначены основные этапы: установка (MA-FS.Setup), генерация ключа (MA-FS.KeyGen), подпись (MA-FS.Sign) и проверка (MA-FS.Verify).

На этапе установки сервер сначала выбирает параметр безопасности λ и запускает алгоритм настройки подписи ECDSA для генерации публичных параметров, затем случайным образом выбирает главный закрытый ключ (Msk) и вычисляет главный открытый ключ (Mvk).

На этапе генерации ключа производится формирование и обмен парами открытого и закрытого ключей схемы между сервером и каждым аутентифицирующим ведомством. Процессы генерации ключей функционируют в соответствии с алгоритмом ECDSA (аббр. от англ. Elliptic Curve Digital Signature Algorithm – алгоритм построения цифровой подписи с использованием эллиптических кривых). Для каждого аутентифицирующего ведомства формируется его sk^i .

Этап подписи – для подписания сообщения каждое аутентифицирующее ведомство принимает на вход приватный ключ sk^i и формирует дополнительные параметры для генерации подписи сообщения sig_i . Сервер получает sig_i от всех аутентифицирующих ведомств и формирует базу для их хранения.

На этапе проверки для каждого аутентифицирующего ведомства производится проверка подписи, при этом верификатор данных может проверить подпись sig_i , используя алгоритм проверки подписи ECDSA, с учетом параметров каждого отдельного участника.

Операции в каждой модели выполнялись по 1000 раз, и в последующем были вычислены средние значения конечных результатов времени исполнения смарт контракта. Результаты эксперимента приведены на рисунке 10. Можно видеть, что время выполнения предложенной схемы блокчейн увеличивается по мере роста числа полномочных органов власти, участвующих в аутентификации запросов.

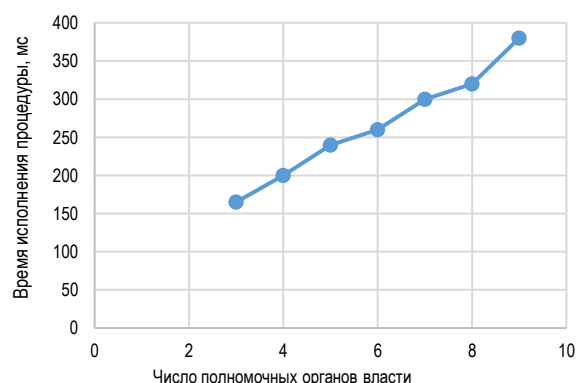


Рис. 10. Результаты моделирования схемы использования блокчейн при наличии более одного аутентифицирующего ведомства

Fig. 10. The Results of Modeling the Blockchain Scheme with More than One Authenticating Agency

Поскольку все больше и больше моделей аутентификации данных с использованием блокчейн находят свое распространение, представляется целесообразным применение схемы функциональных подписей запросов с участием нескольких сторон (полномочных органов) при большом их количестве. Благодаря особенностям организации блокчейн,

схема защищена от подделок и злоупотребления соответствующими инспекторами. Кроме того, имитационное моделирование показало производительность исследуемой схемы с точки зрения задержки по включению и авторизации запроса в цепочку для возможных проверок: около 164,81 мс для трех, 259,30 мс для шести и 388,68 мс для девяти полномочных органов власти.

Вывод

Интеграция технологий блокчейн в систему цифровых сервисов в рамках портала госуслуг РФ имеют очевидную перспективу. В первую очередь, это связано с переориентацией системы госуправления на «цифровое государство».

Использование блокчейна может перевести саму идею электронного правительства на новый уровень. Речь должна идти уже не просто об удобном сервисе предоставления гражданам и бизнесу, а о принципиальном переформатировании самой деятельности государства в контексте безопасности, полном погружении ее в цифровую экосистему блокчейна.

В статье была проанализирована работа технологии блокчейн, построена аналитическая модель ее взаимодействия с порталом ГИС, которая в свою очередь характеризует взаимодействие между узлами сети: блокчейн-узлами и государственными серверами. На основе аналитической модели произведена разработка имитационной модели, позволяющей оценить размер временных задержек для обработки запросов при увеличении числа полномочных органов власти для подтверждения его для включения в цепочку блокчейн.

Так как моделирование работы системы проводилось на одном аппаратном сервере с выделением соответствующего числа виртуальных машин, то сетевая задержка составляет единицы микросекунд, и ее вклад в общее время реализации процедуры ничтожно мал, однако стоит учитывать, что в

реальных системах с территориально распределенными аутентифицирующими органами власти этот параметр может быть значительно выше.

Кроме того, в статье предложено использование известного метода реализации схемы цифровой подписи ECDSA, широко применяемого в блокчейн с внесением дополнительного сервера для обеспечения многопользовательской аутентификации сообщений в рамках смарт-контракта различными ведомствами.

Представленные в статье основные подходы и решения в рамках блокчейн, на базе которых возможно внедрение этой технологии в ГИС, в частности – портал государственных услуг, указывают на технологическую возможность внедрения технологии блокчейн при минимальном влиянии на временные сетевые характеристики системы и с поддержкой многопользовательской аутентификации услуг различными ведомствами.

Здесь стоит отметить, что для полноценного внедрения необходимо еще решить ряд вопросов, связанных с оценкой объемов трафика и команд, необходимых для работы с услугами. Дополнительно следует оценить возможность применения территориально распределенного сервера аутентификации, с учетом иерархической структуры самого портала Госуслуг и СМЭВ, с сохранением быстродействия, безопасности формирования блокчейн-транзакций и их защиты.

Отдельно стоит рассмотреть возможность применения технологии сегментирования в блокчейн для ГИС. Разделение на сегменты позволяет увеличивать пропускную способность по мере расширения сети валидаторов, что неизбежно при текущем развитии госуслуг; однако взаимодействие между сегментами может потребовать дополнительных ресурсов на синхронизацию, т. е. времени, чтобы вновь добавленные узлы загрузили последнее состояние. Потенциал и недостатки этой субтехнологии для внедрения также еще предстоит оценить.

Список источников

1. Госуслуги. URL: <https://www.gosuslugi.ru> (дата обращения 20.12.2022)
2. Зараменских Е.П. Цифровая трансформация государственных услуг // XIII Международная научно-практическая конференция «Государство и бизнес. Современные тенденции и проблемы развития экономики» (Санкт-Петербург, Россия, 21–22 апреля 2021). Санкт-Петербург: Северо-Западный институт управления – филиал РАНХиГС, 2021. С. 23–32.
3. Government as a Platform // Fujitsu Services. 2015. URL: <https://www.fujitsu.com/uk/Images/government-as-a-platform.pdf> (дата обращения 20.12.2022)
4. Система межведомственного электронного взаимодействия (СМЭВ) // TAdviser. 2022. URL: [tadviser.ru/index.php/Продукт:Система_межведомственного_электронного_взаимодействия_\(СМЭВ\)](https://tadviser.ru/index.php/Продукт:Система_межведомственного_электронного_взаимодействия_(СМЭВ)) (дата обращения 20.12.2022)
5. Spirikina A.V., Aptreieva E.A., Elagin V.S., Shvidkiy A.A., Savlieva A.A. Approaches to Modeling Blockchain Systems // Proceedings of the 12th International Congress on Ultra Modern Telecommunications and Control Systems and Workshops (ICUMT, Brno, Czech Republic, 05–07 October 2020). IEEE, 2020. PP. 242–247. DOI:10.1109/ICUMT51630.2020.9222437
6. Елагин В.С., Спиркина А.В., Владыко А.Г., Иванов Е.И., Помогалова А.В., Аптреева Е.А. Основные сетевые характеристики blockchain трафика и подходы к моделированию // Т-Comm: Телекоммуникации и транспорт. 2020. Том 14. № 4. С. 39–45. DOI:10.36724/2072-8735-2020-14-4-39-45

7. Vladko A.G., Spirkina A.V., Elagin V. S., Belozertsev I.A., Aptreva E.A. Blockchain Models to Improve the Service Security on Board Communications // Proceedings of the Systems of Signals Generating and Processing in the Field of on Board Communications (Moscow, Russia, 19–20 March 2020). IEEE, 2020. P. 9078572. DOI:10.1109/IEEECONF48371.2020.9078572
8. Memon R.A., Li J.P., Ahmed J. Simulation Model for Blockchain Systems Using Queuing Theory // Electronics. 2019. Vol. 8. Iss. 2. P. 234. DOI:10.3390/electronics8020234
9. Makolkina M., Koucheryavy A., Paramonov A. Investigation of Traffic Pattern for the Augmented Reality Applications // Proceedings of the 15th IFIP WG 6.2 International Conference on Wired/Wireless Internet Communications (St. Petersburg, Russia, 21–23 June 2017). Lecture Notes in Computer Science. Vol. 10372. PP. 233–246. Cham: Springer, 2017. DOI:10.1007/978-3-319-61382-6_19
10. Ropsten Testnet Explorer // Etherscan. URL: <https://ropsten.etherscan.io> (дата обращения 20.06.2022)

References

1. Gosuslugi. (in Russ.) URL: <https://www.gosuslugi.ru> [Accessed 20th December 2022]
2. Zaramenskikh E. Digital Transformation of Government Services. Государство и бизнес. *Proceedings of the XIII International Scientific-Practical Conference on Current Trends and Problems of Economic Development*, 21–22 April 2021, Saint Petersburg, Russia. Saint-Petersburg: North-West Institute of Management of RANEP Publ.; 2021. PP. 23–32. (in Russ.)
3. Fujitsu Services. Government as a Platform. 2015. URL: <https://www.fujitsu.com/uk/Images/government-as-a-platform.pdf> [Accessed 20th December 2022]
4. TAdviser. Interagency Electronic Interaction System. 2022. (in Russ.) URL: [tadviser.ru/index.php/Продукт: Система межведомственного электронного взаимодействия \(СМЭВ\)](http://tadviser.ru/index.php/Продукт: Система межведомственного электронного взаимодействия (СМЭВ)) [Accessed 20th December 2022]
5. Spirkina A.V., Aptreva E.A., Elagin V.S., Shvidkiy A.A., Savelieva A.A. Approaches to Modeling Blockchain Systems. *Proceedings of the 12th International Congress on Ultra Modern Telecommunications and Control Systems and Workshops, ICUMT*, 05–07 October 2020, Brno, Czech Republic. IEEE; 2020. p.242–247. DOI:10.1109/ICUMT51630.2020.9222437
6. Elagin V.S., Spirkina A.V., Vladko A.G., Ivanov E.I., Pomogalova A.V., Aptreva E.A. The Main Network Characteristics of Blockchain Traffic and Modeling Approaches. *T-Comm*. 2020;14(4):39–45. (in Russ.) DOI:10.36724/2072-8735-2020-14-4-39-45
7. Vladko A.G., Spirkina A.V., Elagin V. S., Belozertsev I.A., Aptreva E.A. Blockchain Models to Improve the Service Security on Board Communications. *Proceedings of the Systems of Signals Generating and Processing in the Field of on Board Communications*, 19–20 March 2020, Moscow, Russia. IEEE; 2020. p.9078572. DOI:10.1109/IEEECONF48371.2020.9078572
8. Memon R.A., Li J.P., Ahmed J. Simulation Model for Blockchain Systems Using Queuing Theory. *Electronics*. 2019;8(2):234. DOI:10.3390/electronics8020234
9. Makolkina M., Koucheryavy A., Paramonov A. Investigation of Traffic Pattern for the Augmented Reality Applications. *Proceedings of the 15th IFIP WG 6.2 International Conference on Wired/Wireless Internet Communications*, 21–23 June 2017, St. Petersburg, Russia. Lecture Notes in Computer Science, vol.10372. p.233–246. Cham: Springer; 2017. DOI:10.1007/978-3-319-61382-6_19
10. Etherscan. Ropsten Testnet Explorer. URL: <https://ropsten.etherscan.io> [Accessed 20th June 2022]

Статья поступила в редакцию 09.09.2022; одобрена после рецензирования 05.12.2022; принята к публикации 16.12.2022.

The article was submitted 09.09.2022; approved after reviewing 05.12.2022; accepted for publication 16.12.2022.

Информация об авторе:

ЕЛАГИН
Василий Сергеевич

кандидат технических наук, доцент кафедры Инфокоммуникационных систем
Санкт-Петербургского государственного университета телекоммуникаций
им. проф. М.А. Бонч-Бруевича,
 <https://orcid.org/0000-0003-4077-6869>

РЕЗУЛЬТАТЫ ИССЛЕДОВАНИЙ МОЛОДЫХ УЧЕНЫХ

*Основой всей научной работы служит убеждение,
что мир представляет собой упорядоченную
и познаваемую сущность...*

Альберт Эйнштейн

1.2.2

2.2.6

2.2.13

2.2.14

2.2.15

2.2.16

2.3.1

2.3.6

Научная статья

УДК 65.011.56

DOI:10.31854/1813-324X-2022-8-4-75-81



Методика поддержки принятия решений на основе оценки клиентского опыта и показателей эффективности оператора связи

Владимир Андреевич Акишин, akishin_vova@mail.ru

Санкт-Петербургский государственный университет телекоммуникаций им. М.А. Бонч-Бруевича,
Санкт-Петербург, 193232, Российская Федерация

Аннотация: В статье рассматривается задача динамического анализа когнитивной модели оценки клиентского опыта в контексте эксплуатационной среды отечественного оператора связи. Актуальность исследования обусловлена потребностью операторов связи в инструменте для поддержки принятия решений, который позволит анализировать зависимость клиентского опыта от эффективности операционной среды компании, а также эмулировать сценарии управления клиентским опытом в контексте основных процессов продаж и обслуживания. Целью исследования является формализация методики динамического анализа модели оценки интегрального клиентского опыта, построенной на основе нечетких когнитивных карт иерархической структуры. В частности, исследуется механика изменения целевых факторов (показателей клиентского опыта) при подаче возмущения на управляющие факторы (показатели операционной деятельности, влияющие на клиентский опыт).

Ключевые слова: методика поддержки принятия решений, когнитивные карты, телекоммуникации, оператор связи, нечеткая логика, клиентский опыт

Ссылка для цитирования: Акишин В.А. Методика поддержки принятия решений на основе оценки клиентского опыта и показателей эффективности оператора связи // Труды учебных заведений связи. 2022. Т. 8. № 4. С. 75–81. DOI:10.31854/ 1813-324X-2022-8-4-75-81

Decision Support Methodology Based on Evaluation of Customer Experience and Telecommunications Operator Efficiency Indicators

Vladimir Akishin, akishin_vova@mail.ru

The Bonch-Bruevich Saint-Petersburg State University of Telecommunications,
St. Petersburg, 193232, Russian Federation

Abstract: The article considers the methodology for dynamic analysis of the cognitive model for assessing customer experience in the context of communication providers. The relevance of the study is due to the need for telecom operators to have a decision support system that allows analyzing dependence of customer experience on the efficiency of the company's operating environment, as well as emulating customer experience management scenarios in the context of the main sales and service processes. The objective of the study is to formalize the methodology of dynamic analysis of the model for assessing the integral customer experience that is based on fuzzy cognitive maps of the hierarchical structure. In particular, the mechanics of changing target factors (i.e., customer experience indicators) when perturbing control factors (i.e., operational performance indicators that affect customer experience) are investigated.

Keywords: decision support methodology, cognitive map, telecommunications, telecom operator, fuzzy logic, customer experience

For citation: Akishin V. Decision Support Methodology Based on Evaluation of Customer Experience and Telecommunications Operator Efficiency Indicators. *Proc. of Telecom. Universities*. 2022;8(4):75–81. (in Russ.) DOI:10.31854/1813-324X-2022-8-4-75-81

Введение

Модель управления современного оператора связи предполагает, что принятие операционных решений требует предварительного анализа их влияния на удовлетворенность клиента от деятельности компании. В подобных условиях становится очевидным востребованность моделей и методик управления операционной средой оператора связи (B/OSS, *аббр. от англ.* Business/Operation Support System) через призму клиентской удовлетворенности и клиентского опыта. Иными словами, субъекты управления оператора связи, а также сотрудники, занимающиеся коммуникациями с клиентами, должны иметь инструмент, который позволит понять, как управленческие решения разного уровня влияют на лояльность и опыт клиентов.

Из вышесказанного следует, что актуальной практической задачей является разработка моделей и методов для оценки клиентского опыта. При этом следует понимать, что клиентский опыт – понятие многомерное, которое определяет множество объективных и субъективных факторов как внутренней среды оператора, так и рыночных аспектов. Проблематика формализации понятия «клиентский опыт», а также модели его оценки, рассматриваются экспертами рынка и научным сообществом последние несколько лет. В частности, одной из моделей, позволяющей установить причинно-следственную связь между понятием «клиентский опыт» и показателями эксплуатационной среды оператора связи, является когнитивная модель оценки интегрального клиентского опыта с использованием аппарата нечетких когнитивных карт иерархической структуры [1–3].

Однако сама по себе подобная модель не является практически применимым инструментом, и для решения реальных задач операционного управления требуется методика, позволяющая проводить динамический анализ модели, в частности анализировать, как изменяется динамика клиентского опыта в зависимости от значений показателей операционных процессов в момент времени. Именно решению задачи динамического анализа когнитивной модели оценки интегрального клиентского опыта посвящена данная статья.

Предметная область и функциональная модель

Оценка значения интегрального клиентского опыта должна формироваться как результат агрегации значений операционных показателей, влияющих на клиентский опыт в разрезе различных измерений компании. Соответственно, основой модели для оценки и анализа клиентского опыта должна яв-

ляться структура, выстраивающая причинно-следственную связь между понятием «клиентский опыт» и показателями операционной деятельности компании. Для построения подобной структуры воспользуемся функциональной моделью оценки интегрального клиентского опыта, описанной автором в более раннем исследовании по данной тематике [1, 3]. Основами данной модели являются 3 ключевых понятия: интегральный клиентский опыт; жизненный цикл клиента и этапы жизненного цикла клиента; метрики клиентского опыта.

Интегральный клиентский опыт – количественная мера, определяющая совокупность впечатлений клиента на протяжении всего его жизненного цикла в компании.

Жизненный цикл клиента и этапы жизненного цикла клиента – понятие, определяющее структуру отношений клиента с оператором связи с момента, когда клиент узнал о нем, и до момента прекращения отношений между клиентом и компанией. Т. е. под жизненным циклом понимается совокупность всех этапов и фаз взаимодействия клиента с компанией, которые проходит клиент последовательно или параллельно, начиная с момента появления у клиента осведомленности о компании и заканчивая точкой прекращения взаимоотношений. Краткое описание этапов жизненного цикла клиента будет представлено в следующем разделе статьи.

Метрики клиентского опыта – предложенная некоммерческой ассоциацией TM Forum совокупность операционных показателей оператора связи, которые оказывают сколь бы то не было значимое влияние на клиентский опыт [4–6]. Метрики, предложенные TM Forum, структурированы по этапам жизненного цикла, и, таким образом, появляется возможность выстраивать причинно-следственную связь между клиентским опытом и операционными показателями как для каждого этапа жизненного цикла, так и в совокупности по всем этапам.

Математическая интерпретация описанной в [1] функциональной модели реализуется с помощью аппарата нечетких когнитивных карт [3, 7–9], а, если быть точнее, то в виде когнитивной карты иерархической структуры, где каждый уровень иерархии будет соответствовать одному из уровней функциональной структуры модели.

Когнитивная модель оценки клиентского опыта

Как уже было отмечено выше, основной для рассматриваемой методики является модель, описывающая взаимосвязь между значением интегрального клиентского опыта и метрик клиентского опыта, сгруппированных по этапам жизненного

цикла клиента. Математической основой данной модели является иерархическая когнитивная карта. Для решения заявленной в исследовании задачи динамического анализа будет использована уже готовая когнитивная модель оценки клиентского опыта, основные принципы построения которой подробно изложены автором в упомянутых работах [1, 3], а также в работах других авторов по данной тематике [9–13]. Ниже в данном разделе приведены основные характеристики модели, значимые для решения обозначенной задачи.

В качестве исходных данных для модели принимается совокупность метрик оператора связи, которые группируются по этапам жизненного цикла, предложенным TM Forum [6]. Основными источниками значений метрик клиентского опыта для данной когнитивной модели являются системы класса B/OSS, система исследования клиентского мнения, система Campaign Management, а также бенчмаркетинговые исследования. Примеры метрик представлены ниже.

Этап жизненного цикла «Interact» (начало взаимодействия, инициализация):

- доля обращений клиентов, решенных через сервисы самообслуживания.

Этап жизненного цикла «Choose» (выбор сервиса и его инсталляция):

- % инсталляций, невыполненных успешно с первого раза;

Этап жизненного цикла «Consume» (использование сервиса):

- количество незавершенных перерывов связи и/или деградации их деградации;

Этап жизненного цикла «Manage» (управление сервисом):

- количество клиентских инцидентов, связанных с работоспособностью услуги;

Этап жизненного цикла «Pay» (оплата сервиса):

- количество запросов на перерасчет;
- субъективная оценка клиентом прозрачности выставленного компанией счета на оплату услуг.

Этап жизненного цикла «Renew» (обновление соглашения об использовании сервиса):

- доля клиентов, обновивших соглашение.

Этап жизненного цикла «Recommend» (отзывы и рекомендации, «сарафанное радио»):

- NPS клиента.

Этап жизненного цикла «Leave» (отток клиента из компании):

- попытки несостоявшегося мотивированного оттока.

Полный список и структура метрик для жизненного цикла B2C клиента можно найти в исходных исследованиях [6].

Далее определяется матрица взаимовлияний факторов друг на друга с помощью опроса экспертов согласно методикам, предложенным автором в предыдущих исследованиях [1]. Функциональный смысл такой матрицы заключается в формализации вектора и силы взаимного влияния метрик клиентского опыта друг на друга и на показатель интегрального клиентского опыта. На рисунке 1 представлен фрагмент матрицы взаимовлияния, смоделированной в среде СППР «ИГЛА» (цветом выделены ненулевые значения).

	Интегральный CX	Интегральный CX (be aware)	Наличие обратной связи на рекламные предложения от клиента	Средняя субъективная оценка качества информирования клиентов об услугах компании и актуальных событиях	Усредненная оценка репутации оператора связи	Мера проникновения и известности бренда в социальных сетях	Интегральный CX (interact)	Средняя субъективная оценка качества клиентского сервиса самообслуживания в личном кабинете
Интегральный CX	0	0	0	0	0	0	0	0
Интегральный CX (be aware)	0.1	0	0	0	0	0	0	0
Наличие обратной связи на рекламные предложения от клиента	0	0.2	0	0	0	0	0	0
Средняя субъективная оценка качества	0	0.4	0	0	0	0	0	0
Усредненная оценка репутации оператора связи	0	0.3	0	0	0	0	0	0
Мера проникновения и известности бренда в социальных сетях	0	0.2	0	0.4	0	0	0	0
Интегральный CX (interact)	0.4	0	0	0	0	0	0	0
Средняя субъективная оценка клиентского сервиса	0	0	0	0	0	0	0.3	0
Средняя субъективная оценка клиентского сервиса обслуживания	0	0	0	0	0	0	0.2	0
Доля обращений клиентов, решенных через сервисы	0	0	0	0	0	0	0.4	0.4
Средняя субъективная оценка клиентом сотрудников компании, с	0	0	0	0	0	0	0.3	0
Интегральный CX (choose)	0.2	0	0	0	0	0	0	0
Количество заявок на подключение не выполненных в	0	0	0	0	0	0	0	0
Количество переносов времени визита специалиста к клиенту по	0	0	0	0	0	0	0	0
% инсталляций, невыполненных успешно с первого раза	0	0	0	0	0	0	0	0
Количество обращений в техническую поддержку на следующий	0	0	0	0	0	0	0	0
Субъективная оценка клиентом сотрудника отдела продаж при	0	0	0	0	0	0	0	0
Субъективная оценка клиентом качества работы инсталлятора	0	0	0	0	0	0	0	0
Субъективная оценка клиентом процесса подключения	0	0	0	0	0	0	0	0
Интегральный CX (consume)	0.6	0	0	0	0	0	0	0
Субъективная оценка клиентом качества услуги интернет	0	0	0	0	0	0	0	0
Среднее соотношение фактической скорости интернет канала к	0	0	0	0	0	0	0	0
Субъективная оценка клиентом качества услуги интерактивное	0	0	0	0	0	0	0	0

Рис. 1. Фрагмент матрицы взаимовлияний, сформированный в ПО СППР «ИГЛА»

Fig. 1. A Fragment of the Matrix of Mutual Influences, Formed in the Software of the DSS "IGLA"

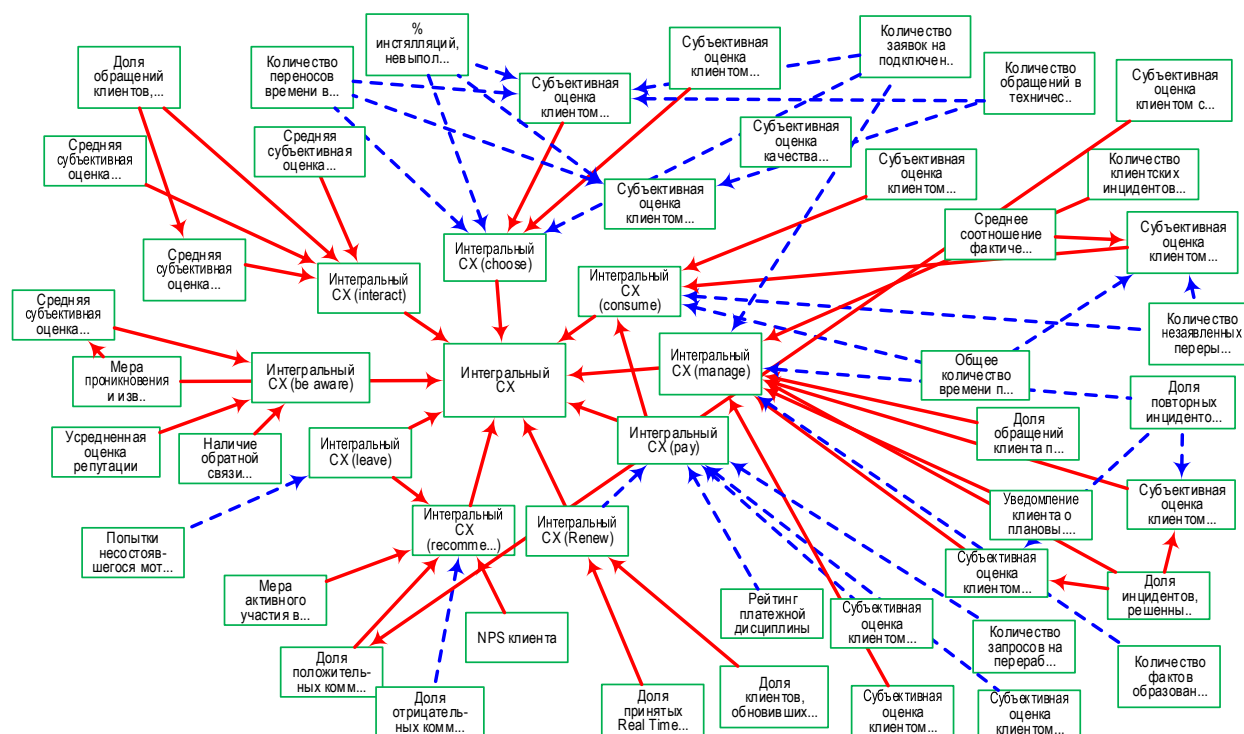


Рис. 2. Фрагмент когнитивной карты для оценки интегрального СХ, сформированная в ПО СППР «ИГЛА»

Fig. 4. A Fragment of a Cognitive Map for Assessing the Integral CX, Formed in the Software of the DSS "IGLA"

На основе метрик и матрицы взаимовлияний формируется когнитивная карта, которая, по сути своей будет иметь иерархическую структуру, согласно описанной в [1]. Первый уровень представляет собой когнитивную карту, где управляющими факторами являются метрики клиентского опыта, а целевыми факторами – значения интегрального показателя CX (*аббр. от англ. Customer eXperience*) для каждого из этапов жизненного цикла клиента. Второй уровень представляет собой когнитивную карту, где управляющими факторами являются значения CX для этапа жизненного цикла клиента, а целевым фактором – значение интегрального CX. Внешний вид когнитивной карты, сформированной в среде СППР «Игла» на основе вышеописанной матрицы, представлен на рисунке 2. Данная когнитивная карта будет характеризоваться параметрами, представленными в таблице 1.

ТАБЛИЦА 1. Характеристики когнитивной карты

TABLE 1. Cognitive Map Parameters

Параметр	Значение	Расчетная формула
Количество факторов (N)	133	–
Количество взаимовлияний между факторами (L)	386	–
Плотность (D)	0,02198678	$D = L/N(N - 1)$
Количество факторов приемников (R)	1	–
Количество факторов передатчиков (T)	74	–
Сложность когнитивной карты (C)	0,01351	$C = R/T$

Таким образом, мы имеем когнитивную карту для оценки интегрального клиентского опыта B2C клиента на протяжении всего его периода взаимоотношений с компанией. За счет системы взаимовлияния управляющих факторов друг на друга данная модель позволяет эмулировать сценарии изменения интегрального клиентского опыта (т.е. целевого фактора), путем подачи возмущения на управляющие факторы, моделирующие метрики клиентского опыта [1, 14].

Динамический анализ причинно-следственной связи между клиентским опытом и показателями эффективности

Рассмотрим алгоритм динамического анализа модели оценки интегрального клиентского опыта в проекции на конкретного клиента. Основной целью анализа, в данном случае, будет являться исследование динамики изменения интегрального клиентского опыта в течение основных этапов жизненного цикла клиента в зависимости от изменения значений управляющих факторов модели (т. е. метрик клиентского опыта) на каждом из этапов. В качестве объекта исследования выберем троих B2C клиентов из структуры клиентской базы отечественного оператора связи.

Процесс динамического анализа поэтапно строится следующим образом.

Этап 1. Инициализируются начальные значения управляющих и целевых факторов модели:

– для управляющих факторов когнитивной модели начальные значения будут определяться текущими значениями метрик клиентского опыта, сформулированными в терминах лингвистической переменной [1, 12, 13]; если метрика не определена для конкретного клиента в начальный момент времени, то берется усредненное значение метрики по данному измерению в контексте клиентской базы;

– для целевых факторов когнитивной модели (т. е. интегральных значений клиентского опыта) примем, что начальные значения будут определены как «Среднее» (терм лингвистической переменной).

Этап 2. Для каждого клиента моделируются сценарии подачи возмущения на управляющие факторы модели. Сценарии моделируются последовательно для каждого из этапов жизненного цикла клиента. Каждый сценарий включает в себя несколько шагов (моделирующих момент времени), на каждом из которых подается возмущение на управляющий фактор (моделируется изменение метрики клиентского опыта).

Этап 3. В рамках каждого из сценариев анализируется динамика изменения интегрального клиентского опыта в разрезе этапа жизненного цикла и совокупный клиентский опыт по всему «пути» клиента.

Для получения прогноза изменения клиентского опыта на разных этапах жизненного цикла клиента используется математический аппарат импульсных процессов, прогнозирующий значения концептов в дискретные моменты времени.

Для нечетких когнитивных карт предлагается следующая модификация модели импульсного процесса:

$$a_i(t+1) = S(a_i(t) + q_i(t+1) + o_i(t+1) + \sum_{j=1}^K T(w_{ij}p_j(t))),$$

где $a_i(t+1)$ – значение концепта v_i в момент времени $t+1$; $a_i(t)$ – значение концепта v_i в момент времени t ; $q_i(t+1)$ – внешнее воздействие (т. е. подача внешнего возмущения) на концепт v_i в момент времени $t+1$; $o_i(t+1)$ – управляющее воздействие (т. е. воздействие связанных факторов) на концепт v_i в момент времени $t+1$; w_{ij} – вес влияния концепта v_j на v_i ; $p_j(t)$ – изменение значения v_j в момент времени t ; T – операция Т-нормы (операция пересечения нечетких множеств); S – операция S-нормы (операция объединения нечетких множеств).

Таким образом, подобный анализ позволяет строить прогноз изменений опыта конкретного клиента в зависимости от влияющих на него факторов.

Рассмотрим пример работы алгоритма для этапа жизненного цикла «Choose» (выбор сервиса и его установка). На этом этапе для каждого из исследуемых клиентов рассматривается сценарий, состоящий из одного шага, на котором подается возмущение на управляющие факторы согласно таблице 2, где: ОВ – очень высокий (клиентский опыт); С – средний; ОН – очень низкий; «–» – нет данных.

ТАБЛИЦА 2. Подаваемое возмущение на управляющие факторы когнитивной модели

TABLE 2. Applied Impulse to the Control Factors of the Cognitive Model

Управляющий фактор (метрика клиентского опыта) для этапа «Choose»	Клиент		
	№ 1	№ 2	№ 3
Количество заявок на подключение не выполненных в запрашиваемый клиентом период	–	–	ОН
Количество переносов времени визита специалиста к клиенту по инициативе компании	ОВ	ОВ	ОН
% инсталляций, невыполненных успешно с первого раза	ОВ	ОН	ОН
Количество обращений в техническую поддержку на следующий день после подключения	ОВ	ОН	ОН
Субъективная оценка клиентом сотрудника отдела продаж при оформлении заявки на подключение	–	ОН	ОВ
Субъективная оценка клиентом качества работы инсталлятора	ОН	ОВ	ОВ
Субъективная оценка клиентом процесса подключения	ОН	С	ОВ

Динамика наблюдаемого фактора «Интегральный клиентский опыт (этап Choose)» достаточно логичны и представлены на рисунке 3.

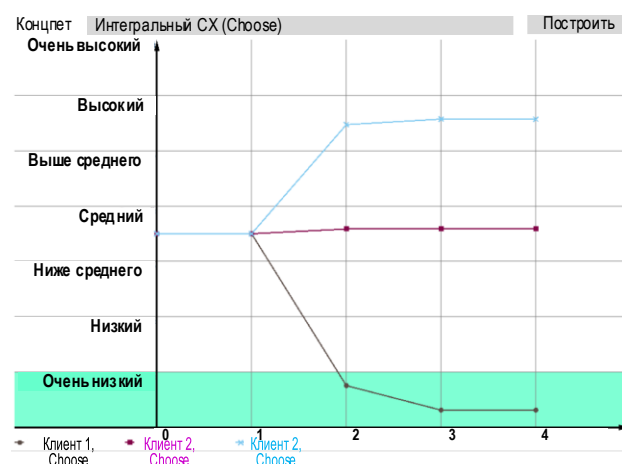


Рис. 3. Динамика интегрального CX для этапа «Choose»

Fig. 3. Dynamics of the Integral CX for the «Choose» Stage

Из представленного графика можно сделать выводы, что опыт на этапе «Choose» у клиента № 1 принял значение «Очень низкий», у клиента № 2 он практически не изменился, а у клиента № 3 стал

«Высокий». Подобные результаты вполне адекватны с учетом тех сценариев возмущения, которые подавались на управляющие факторы для каждого из клиентов. Так, у клиента № 1 имели место явные огрехи в процессе подключения, которые клиент, в свою очередь, вполне логично оценил низкой субъективной оценкой. С другой стороны, пример клиента № 3 показывает, что процесс подключения со стороны компании был отработан идеально, обратная связь от клиента также была крайне положительной, как следствие, клиентский опыт вырос со среднего значения до высокого. У клиента № 2 негативные моменты, связанные с оформлением заявки и переносом времени визита, были компенсированы качественной работой инсталлятора, что, в свою очередь, дало сбалансированное среднее значение клиентского опыта.

Однако наибольший интерес представляет анализ динамики клиентского опыта не для этапа «Choose», а для интегрального CX на всем «жизненном пути» клиента. Динамика интегрального клиентского опыта представлена на рисунке 4.

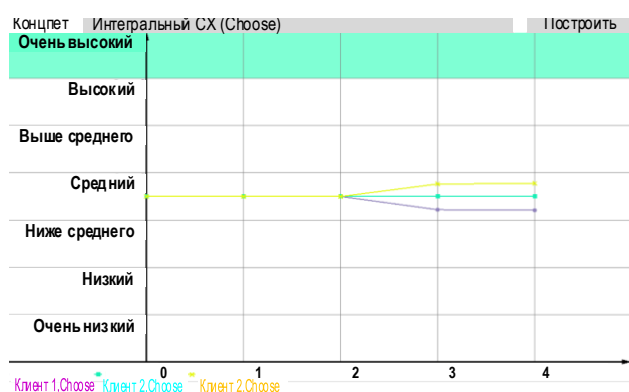


Рис. 4. Динамика интегрального CX

Fig. 4. Integral CX Dynamics

Из данного графика можно сделать вывод, что несмотря на достаточно резкую динамику интегрального клиентского опыта на этапе «Choose» у клиентов № 1 и № 3, его совокупное значение изменилось не сильно. Это обусловлено низкой степенью влияния фактора «Интегральный клиентский

опыт (этап Choose)» на «Интегральный клиентский опыт», что в свою очередь, объясняется предположением экспертов о том, что процесс подключения слабо влияет на интегральный клиентский опыт, т. к., в общем случае, процесс подключения физических лиц — это разовое мероприятие, которое не оказывает сильного влияния на совокупные впечатления клиента при условии устойчивой репутации бренда и низкой стоимости услуг.

Подобным образом проводится и анализируется интегральный клиентский опыт и для остальных этапов жизненного цикла — переменными являются метрики клиентского опыта, т. е., в терминах модели, возмущение, подаваемое на управляющие факторы.

Заключение

Рассмотренная в статье методика динамического анализа когнитивной модели, в общем случае, позволяет формировать множество сценариев изменения клиентского опыта в зависимости от разных комбинаций значений управляющих факторов в определенный момент времени.

Динамический анализ когнитивной модели может использоваться как в контексте операционных процессов, связанных с взаимодействием с клиентом, так и в рамках стратегического и операционного анализа в целях поддержки принятия управленческих решений. В рамках операционных процессов основная ценность модели заключается в возможности рассчитать в момент времени значение интегрального клиентского опыта для конкретного клиента и, на его основе построить персонализированное взаимодействие с ним в точках контакта. Для поддержки принятия управленческих решений динамический анализ модели позволяет моделировать совокупность сценариев управления операционными процессами и выявлять те сценарии, которые позволяют, с одной стороны, максимизировать клиентский опыт, а, с другой стороны — выбрать оптимальную модель влияния на параметры операционных процессов оператора связи.

Список источников

1. Акишин В.А. Когнитивная модель оценки клиентского опыта в структуре инфокоммуникационного ландшафта оператора связи // Проблемы информатики. 2021. № 3(52). С. 34–55. DOI:10.24412/2073-0667-2021-3-34-55
2. Гольдштейн А.Б., Пожарский Н.А., Лихачев Д.А. О когнитивных картах в управлении телекоммуникационным оператором // Информатизация и связь. 2016. № 1. С. 11–15.
3. Akishin V., Goldstein A., Goldstein B. Cognitive Models for Access Network Management // Proceedings of the 17th International Conference (NEW2AN 2017), 10th Conference (ruSMART 2017), Third Workshop NsCC 2017 (St. Petersburg, Russia, 28–30 August 2017). Internet of Things, Smart Spaces, and Next Generation Networks and Systems. Lecture Notes in Computer Science. Vol. 10531. Cham: Springer, 2017. PP. 375–381. DOI:10.1007/978-3-319-67380-6_34
4. GB962 Customer Experience Management Solution Suite // TmForum. URL: <https://www.tmforum.org/resources/suite/gb962-customer-experience-management-solution-suite-r17-5-0> [Accessed 02nd April 2020]
5. GB962 Customer Experience Management: Introduction and Fundamentals R16.0.1 // TmForum. URL: <https://www.tmforum.org/resources/best-practice/gb962-customer-experience-management-introduction-and-fundamentals-r16-0-1> [Accessed 02nd April 2020]

6. GB962A Customer Experience Management Lifecycle Metrics R15.0.1 // TmForum. URL: <https://www.tmforum.org/resources/best-practice/gb962a-customer-experience-management-lifecycle-metrics-r15-0-1> [Accessed 02nd April 2020]
7. Заграновская А.В. Системный анализ на основе нечетких когнитивных карт // Вестник Российского экономического университета имени Г.В. Плеханова. 2018. № 4(100). С. 152–160. DOI:10.21686/2413-2829-2018-4-152-160
8. Маренко В.А., Мальцева М.И. Применение когнитивного моделирования для анализа проблем малого бизнеса // Известия Иркутской государственной экономической академии. 2015. Т. 25. № 6. С. 1014–1024. DOI:10.17150/1993-3541.2015.25(6).1014-1024
9. Ротштейн А.П. Нечеткие когнитивные карты в анализе надежности систем // Надежность. 2019. Т. 19. № 4(71). С. 24–31. DOI:10.21683/1729-2646-2019-19-4-24-31
10. Axelrod R. Structure of Decision. The Cognitive Maps of Political Elites. Princeton University Press, 1976. 422 p.
11. Groumpos P.P. Fuzzy Cognitive Maps: Basic Theories and Their Application to Complex Systems // In: Glykas M. (ed.) Fuzzy Cognitive Maps: Advances in Theory, Methodologies, Tools and Applications. Studies in Fuzziness and Soft Computing. Vol. 247. Berlin, Heidelberg: Springer, 2010. PP. 1–22. DOI:10.1007/978-3-642-03220-2_1
12. Kosko B. Fuzzy Cognitive Maps // International Journal of Man-Machine Studies. 1986. Vol. 24. Iss. 1. PP. 65–75. DOI:10.1016/S0020-7373(86)80040-2
13. Kosko B. Fuzzy systems as universal approximators // IEEE Transactions on Computers. 1994. Vol. 43. Iss. 11. PP. 1329–1333. DOI:10.1109/12.324566
14. Гулаков В.К., Лагерева Д.Г., Подвесовский А.Г. Система поддержки принятия решений на основе когнитивного моделирования «ИГЛА» // Программные продукты и системы. 2007. № 3. С. 50.

References

1. Akishin V.A. Cognitive model for evaluating customer experience in the structure of the infocommunication landscape of a telecom operator. *Problems of Informatics*. 2021;3(52):34–55. (in Russ.) DOI:10.24412/2073-0667-2021-3-34-55
2. Goldstein A.B., Pozharskiy N.A., Likhachev D.A. About the Cognitive Maps in the Management of Telecommunications Operator. *Informization and communication*. 2016;1:11–15. (in Russ.)
3. Akishin V., Goldstein A., Goldstein B. Cognitive Models for Access Network Management. *Proceedings of the 17th International Conference, NEW2AN 2017, 10th Conference, ruSMART 2017, Third Workshop NsCC 2017, 28–30 August 2017, St. Petersburg, Russia. Internet of Things, Smart Spaces, and Next Generation Networks and Systems. Lecture Notes in Computer Science, vol.10531*. Cham: Springer; 2017. p.375–381. DOI:10.1007/978-3-319-67380-6_34
4. TmForum. GB962 Customer Experience Management Solution Suite. URL: <https://www.tmforum.org/resources/suite/gb962-customer-experience-management-solution-suite-r17-5-0> [Accessed 02nd April 2020]
5. TmForum. GB962 Customer Experience Management: Introduction and Fundamentals R16.0.1. URL: <https://www.tmforum.org/resources/best-practice/gb962-customer-experience-management-introduction-and-fundamentals-r16-0-1> [Accessed 02nd April 2020]
6. TmForum. GB962A Customer Experience Management Lifecycle Metrics R15.0.1. URL: <https://www.tmforum.org/resources/best-practice/gb962a-customer-experience-management-lifecycle-metrics-r15-0-1> [Accessed 02nd April 2020]
7. Zagranovskaya A.V. System Analysis on the Basis of Imprecise Cognitive Cards. *Vestnik of the Plekhanov Russian University of Economics*. 2018;4(100):152–160. (in Russ.) DOI:10.21686/2413-2829-2018-4-152-160
8. Marenko V.A., Maltseva V.I. Cognitive Modeling Application for Analyzing Small Businesses Problems. *Bulletin of Baikal State University*. 2015. Vol. 25. Iss. 6. PP. 1014–1024. (in Russ.) DOI:10.17150/1993-3541.2015.25(6).1014-1024
9. Rotshtein A.P. Fuzzy cognitive maps in the dependability analysis of systems. *Dependability*. 2019;19(4):24–31. (in Russ.) DOI:10.21683/1729-2646-2019-19-4-24-31
10. Axelrod R. Structure of Decision. The Cognitive Maps of Political Elites. Princeton University Press; 1976. 422 p.
11. Groumpos P.P. Fuzzy Cognitive Maps: Basic Theories and Their Application to Complex Systems. In: Glykas M. (ed.) Fuzzy Cognitive Maps: Advances in Theory, Methodologies, Tools and Applications. Studies in Fuzziness and Soft Computing, vol.247. Berlin, Heidelberg: Springer; 2010. p.1–22. DOI:10.1007/978-3-642-03220-2_1
12. Kosko B. Fuzzy Cognitive Maps. *International Journal of Man-Machine Studies*. 1986;24(1):65–75. DOI:10.1016/S0020-7373(86)80040-2
13. Kosko B. Fuzzy systems as universal approximators. *IEEE Transactions on Computers*. 1994;43(11):1329–1333. DOI:10.1109/12.324566
14. Gulakov V.K., Lagereva D.G., Podvesovsky A.G. Decision support system based based on cognitive modeling "NEEDLE". *Software & Systems*. 2007;3(50). (in Russ.)

Статья поступила в редакцию 11.10.2022; одобрена после рецензирования 09.12.2022; принята к публикации 12.12.2022.

The article was submitted 11.10.2022; approved after reviewing 09.12.2022; accepted for publication 12.12.2022.

Информация об авторе:

АКИШИН
Владимир Андреевич

аспирант кафедры инфокоммуникационных систем Санкт-Петербургского государственного университета телекоммуникаций им. проф. М.А. Бонч-Бруевича
 <https://orcid.org/0000-0001-9793-2266>

Научная статья

УДК 621.394

DOI:10.31854/1813-324X-2022-8-4-82-88



Flying Fog Mobile Edge Computing Based on UAV-Assisted for IoT Nodes in Smart Agriculture

Abbas Alzaghir, abbasaltamimi89@gmail.com

The Bonch-Bruevich Saint-Petersburg State University of Telecommunications,
St. Petersburg, 193232, Russian Federation

Abstract: *Flying Fog Mobile Edge Computing can play a pivotal part in the field of smart agriculture. Moreover, is an ideal choice for the significant features it enjoys such as its capability of functioning in remote locations, its wide coverage of areas, sufficient bandwidth, as well as its ability of dealing with connectivity issues. Hence, it is essential for smart agriculture provided with IoT devices to utilize offloading data in a real time and execution the satisfactory steps for a certain circumstance by using flying fog mobile edge computing. Flying Fog Mobile Edge Computing is a good choice to treat connectivity issues. In this paper, proposed a cooperation paradigm of UAVs and IoT devices towards smart agriculture for offloading and executing the computation tasks on-behalf IoT nodes by using dynamic programming algorithm and get satisfactory solution for constrained optimization problem and achieving minimize delay to accomplish tasks.*

Keywords: UAVs, IoT, Mobile Edge Computing, IoT nodes.

For citation: Alzaghir A. Flying Fog Mobile Edge Computing Based on UAV-Assisted for IoT Nodes in Smart Agriculture. *Proc. of Telecom. Universities.* 2022;8(4):82–88. (in Russ.) DOI:10.31854/1813-324X-2022-8-4-82-88

Летающие мобильные граничные вычисления на базе БПЛА для узлов Интернета вещей в «умном» сельском хозяйстве

Аббас Али Алзагир, abbasaltamimi89@gmail.com

Санкт-Петербургский государственный университет телекоммуникаций им. М.А. Бонч-Бруевича,
Санкт-Петербург, 193232, Российская Федерация

Аннотация: *Летающие мобильные граничные вычисления могут сыграть ключевую роль в области «умного» (интеллектуального) сельского хозяйства. Кроме того, это идеальный выбор благодаря таким важным характеристикам, как возможность работы в удаленных местах, широкий охват территорий, достаточная пропускная способность, а также способность решать проблемы с подключением. Для «умного» сельского хозяйства, оснащенного IoT-устройствами, важно использовать выгрузку данных в режиме реального времени и выполнять удовлетворительные шаги для определенных обстоятельств с помощью мобильных граничных вычислений. Летающие мобильные граничные вычисления – хороший выбор для решения проблем с подключением. В статье предлагается парадигма сотрудничества БПЛА и «мир» IoT в интересах интеллектуального сельского хозяйства путем выгрузки и выполнения вычислительных задач от имени IoT-узлов за счет использования алгоритма динамического программирования и получения удовлетворительного решения задачи оптимизации с ограничениями, а также минимизации задержки для выполнения задач.*

Ключевые слова: БПЛА, Интернет вещей, мобильные граничные вычисления, IoT-узлы.

Ссылка для цитирования: Алзагир А.А. Летающие мобильные граничные вычисления на базе БПЛА для узлов Интернета вещей в «умном» сельском хозяйстве // Труды учебных заведений связи. 2022. Т. 8. № 4. С. 82–88. DOI:10.31854/1813-324X-2022-8-4-82-88

1. Introduction

Unmanned Aerial Vehicles have been an important part to assist terrestrial networks. Thus, they can contribute considerably in providing extra functional diversity in assisting 5G and next generations of mobile networks. Moreover, for their ease of deployment and observability, it could be used in a different commercial applications and civil purposes such as surveying and mapping, aerial base stations, search and rescue, and development of new user equipment, deployed both for computing, data gathering, surveillance, provide connectivity, traffic management, etc. Moreover, the performance criteria of 5G networks in the context of enhanced reliability, low latency, peak throughput per connection, high speed, and consuming low power makes the UAVs one of the most important options to achieving all issues mentioned above.

A wide range of use cases can be imagined for UAVs which, in general, can be categorized into two important paradigms: the UAV acting as part of wireless communication infrastructure, and the UAV acting as a mobile terminal. Furthermore, terrestrial base stations BSs have been recently assisted by UAVs, hence, their capacity has been extended in terms of resource allocation and coverage. Also, they assist WSN (wireless sensor networks), IoT (Internet of things), and support Smart cities [1]. Forming flexible aerial platforms, UAVs can be easily employed in the sky [2]. In addition, using 5G networks, seamless connectivity can be well supported and multiple QoS requirements can be guaranteed for many devices, with a large amount of data being handled, which are generated by physical environments [3]. Thus, wireless communication systems of 5G and beyond can boost the support of platforms of aerial communication access. With such capacities, UAVs are considered an integral part of the future generation of mobile networks. They can work jointly as a single system [4]. UAVs have also been used for other purposes in smart agriculture provided by IoT devices like computing, aerial sensing, monitoring, data collection, tracking, and communication.

The current paper proposes a new computing paradigm which is flying fog edge computing based on UAV-MEC assisted IoT devices in smart agriculture. Where, IoT are small limited resources devices that generate data from the surrounding environment. The IoT devices don't have ability to do computing and processing the data because of they have limited resources [5]. In conventional techniques, the computing is implemented by transfer data to a central base station with server provided via multi-hops and relays, leading to delays and errors [6]. For such issues, flying fog computing based on UAV-MEC play a vital role to accomplish the computation tasks on-behalf IoT devices by offloading data from IoT nodes to nearby flying UAV [7, 17]. As well, the effective cooperation between UAVs and IoT

devices to processing and offloading data can be leveraged in real-time. Thus, the flying fog computing based on UAV-MEC can reduce the execution time delay of the IoT devices, by offloading data to be processing (IoT device to nearby UAV, instead of IoT device to a far-away base station). This extends battery life [8]. Furthermore, UAVs can be used in various positions; they can carry flexible loads, measure and provide analytics about anything anywhere and at any time. The significant aspects that cooperation of UAVs and IoT have are represented by the better connectivity and delivery of high QoS as well as lower prices. The UAV-based MEC is equipment onboard devices such as memory, digital cameras, sensors, communication technologies, and actuators [18].

2. Related works

This part highlights the most relevant works that examined cooperation UAV and IoT devices in many applications. The authors in the study [9] survey the applications and techniques of drones and IoT collaboration, which have been recently proposed in order to augment the smartness of cities. The authors highlight in a comprehensive manner, the recent and current research on drone and IoT collaboration to improve the real-time application.

In the [10] the researchers introduced UAV-enabled intelligent transportation for a smart city. They investigated the potential challenges and applications for UAV enabled intelligent transportation for next generation smart cities.

Furthermore, the author of [11] addressed drone architecture as a method of delivering IoT services through a drone. The authors investigated employing RFID-equipped drones (Radio Frequency Identification), together with cameras and sensors for data collection.

The authors of [12] described the data gathering from IoT devices by using swarm of UAVs for the transmission power to be minimized from IoT devices. It was shown that each UAV delivers services on the ground to IoT cluster devices by considering the mobility of IoT devices in smart cities.

The hierarchical structure based on the collaboration between associated wireless sensors and UAVs in [13] presented crop monitoring in (PA) or precision agriculture. The authors demonstrated that the collaboration in such specific applications is an efficient solution for control, collecting data, and analysis by integrating UAVs with IoT and ground sensors. The effective management of network load and latency through optimized routes of UAV and in-situ data processing has significant benefits not only in online data collection but also relaying the data to a central monitoring point. The Authors in [14] used edge computing paradigm for smart agriculture to gathering data, exploiting tasks, and the prevalent issue of internet access.

3. System model and scenario

The proposed system model consists of a set of IoT nodes distributed in the smart agriculture that generate data and need to be processing. Also, the system has two flying UAVs one of them is UAV-MEC equipped with mobile computing server, as well as the remote base station provided by edge computing server as in the figure 1. The data will be processing either at nearby IoT nodes by flying fog edge computing server UAV-MEC or remotely at central edge cloud computing server. For first scenario, the flying fog mobile edge computing system, a UAV as MEC has been used, where the data will be offloaded from IoT nodes to nearby UAV-MEC which equipped with a computation resources, it has ability to store, processing and analyze data [19, 20]. The second scenario is remotely computing system, where the UAV as relay has been used to transfer data from IoT nodes to central edge cloud computing server via a wireless channel as shown in figure 1.

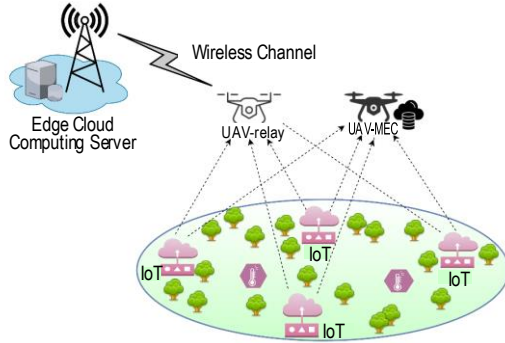


Fig. 1. System Model

The IoT nodes generates N independent tasks of computation that need to be processed. To accomplish the task, the data are offloaded and processed either at UAV-MEC when a binary computation offloading decision α_i is '1' or remotely at central edge cloud server by transfer tasks via UAV-relay when a binary computation offloading decision α_i is '0':

$$\alpha_i = \begin{cases} 1 & \text{at UAV - MEC} \\ 0 & \text{at edge cloud server} \end{cases}.$$

The following equation calculates the maximum rate of uplink data where the data of computation task are transmitted over the wireless channel [15]:

$$D_{\text{IoT,UAV}} = w * \log_2 \left(1 + \frac{P_{\text{IoT,UAV}} G_{\text{IoT,UAV}}}{\sigma w} \right), \quad (1)$$

where, w represents the channel bandwidth; $G_{\text{IoT,UAV}}$ is the channel gain between IoT node and UAV and edge cloud server; $P_{\text{IoT,UAV}}$ is the UAV transmission power and IoT device, and σ is the density of noise power.

3.1. Computation model

This subsection presents the computation offloading model. First, the IoT nodes has N independent tasks of computation requiring completion. A tuple

$\{S_i, C_i, T_i^{\text{constraint}}\}$ represents the task required for each computation task i , where S_i is the size of data required to be transmitted, C_i is the total number of CPU cycles and $T_i^{\text{constraint}}$ is the deadline required for task i to be completed.

Flying fog computing

In flying fog computing case, where the computation task i is offloaded and processed at UAV-MEC. The IoT nodes looks for UAV-MEC to check availability of resources to perform the task or not.

The transmission delay of computation task i from IoT node to UAV-MEC can be expressed as:

$$T_{\text{IoT-UAV}}^{\text{trans}} = \frac{S_i}{D_{\text{IoT}}}, \quad (2)$$

and the processing delay of computation task i in the UAV-MEC can be formulated by the following equation:

$$T_{\text{UAV-MEC}}^{\text{process}} = \frac{C_i}{F_{\text{UAV}}}, \quad (3)$$

where F_{UAV} is the computational capability of UAV-MEC, from (2) and (3) the total processing delay at UAV-MEC can be calculated as:

$$T_{\text{UAV-MEC}}^{\text{total}} = T_{\text{IoT-UAV}}^{\text{trans}} + T_{\text{UAV-MEC}}^{\text{process}}, \quad (4)$$

$$T_{\text{UAV-MEC}}^{\text{total}} = \frac{S_i}{D_{\text{IoT}}} + \frac{C_i}{F_{\text{UAV}}}. \quad (5)$$

Edge-cloud server computing

In edge-cloud server computing case, where the computation task i of IoT nodes will be transmitted to edge cloud server via UAV-relay and will be processed there. The transmission delay from UAV-relay to edge cloud server of computation task i of IoT node can be expressed as:

$$T_{\text{UAV-server}}^{\text{trans}} = \frac{S_i}{D_{\text{UAV}}}. \quad (6)$$

The processing delay of computation task i of IoT node at edge cloud server can be expressed as:

$$T_{\text{server}}^{\text{process}} = \frac{C_i}{F_{\text{server}}}, \quad (7)$$

where, F_{server} is the computational capability of edge cloud server.

Last, the total computation for transmission and processing delay at edge cloud server can be calculated by summation (2), (6) and (7):

$$T_{\text{server}}^{\text{total}} = T_{\text{IoT-UAV}}^{\text{trans}} + T_{\text{UAV-server}}^{\text{trans}} + T_{\text{server}}^{\text{process}}, \quad (8)$$

$$T_{\text{server}}^{\text{total}} = \frac{S_i}{D_{\text{IoT}}} + \frac{S_i}{D_{\text{UAV}}} + \frac{C_i}{F_{\text{server}}}. \quad (9)$$

The total overhead delay for processing the computation task i can be expressed as:

$$T_i^{\text{total}} = \alpha_i T_{\text{UAV-MEC}}^{\text{total}} + (1 - \alpha_i) T_{\text{server}}^{\text{total}}. \quad (10)$$

3.2. Problem statement

This section examines the achieving efficient delay computation offloading based on flying fog computing system for smart agriculture.

The issue of computation offloading is formulated as the following constrained optimization problem:

$$\begin{aligned} \min \quad & \sum_{i=1}^N T_i^{\text{total}}, \\ \text{s.t.} \quad & T_i^{\text{total}} \leq T_i^{\text{constraint}} \quad C1 \\ & \alpha_i \in \{0,1\} \quad C2 \end{aligned} \quad (11)$$

The aim of this study is minimizing the weighted delaying sum by distributing the task offloading. The constraints C1 represents time consumption upper bounds. Constraint C2 is the guarantee that the variables of offloading decisions are binary values.

4. Computation offloading algorithm

The computation flying fog computing offloading algorithm in this paper based on “Dynamic Programming with Hamming Distance Termination (DPH) algorithm” [16]. The algorithm provides inclusive process to find the decisions of optimal computation offloading of flying fog computing system. Initially, The IoT nodes offloads the task i to nearby UAV-MEC when $\alpha_i = 1$ or to the edge-cloud server when $\alpha_i = 0$. Dynamic programming is the basis of the proposed algorithm is based on by using $N \times N$ table (where N is the number of tasks that need to be processed). The table is used to store a bit stream to ensure which task will be processed nearby at UAV-MEC and which tasks will be executed remotely at edge-cloud server. In the table, the random bit streams that are generated are filled as ones (1s) in the following horizontal cell. The zeros (0s) are filled in the following vertical cell. The first cell is empty all the time. When the first bit is 1, then the starting cell is (1, 2). When the first bit is 0, then the starting cell is (2, 1). To illustrate the process of filling in the table the random bit stream generated, let us propose that $N = 8$, the first random α_i bit stream is 00110100 (red bits), and the second random bit stream is 10101101 (black bits). Then (2, 1) is the first stream starting cell where the first bit was 0. On the other hand, (1, 2) is the second stream starting cell as long as the first bit is 1. By following this rule to fill the tables, the resulting stream as shown in the table 1.

TABLE.1 Random Bit Stream

	1						
0	0	1					
0	1	1/0	1	1			
		0	1	0	1		
			0				
			0				

From the table, we calculate the delay of each task by each cell has 0s for flying fog computing case and each cell has 1s for edge-cloud server computing case. The computation offloading algorithm proposed in this paper is shown below.

The Computation Flying Fog Offloading Algorithm Based on Dynamic Programming Tables

1. Initialize Time matrixes and set the Completion deadline ($T_i^{\text{constraint}}$) and Transmission Rate
2. generate a task (randomly)
3. Loop iteration
4. generate a random bit stream
5. calculate delay for tasks of IoT nodes (at UAV-MEC, at edge-cloud server)
6. check the first bit to specify the starting cell in the first table
8. loop i to $N-1$
9. if bit(i) == 1 in the table (UAV-MEC)
10. regenerate random bit (0 or 1)
11. end if
12. Put each bit of the bit stream in the correct position in table
13. if this specific cell in tables is visited before compare the new Total delay of this cell with the previous one
14. if the new Total delay of the cell is less than the previous one
15. Replace the total delay of this cell with the new calculated amounts.
16. Calculate the delay of the remaining bits of the new bit stream
17. else
18. Keep the previous total delay in the cell.
29. Calculate the delay of the remaining cells of the new stream based on the existing amount of this cell
20. end if
21. end if
22. end Loop
23. if Number of bits in tables = N & $T_{\text{total}} < T_i^{\text{constraint}}$ & hamming distance criterion is met
24. return T_{total}
25. end if
26. end Loop

5. Simulation setup and results

The simulation of our work was implemented by Matlab environment. The parameters that applied in this work it shown in the table 2.

TABLE 2. Simulation Parameters

Parameter	Value
Number of tasks N	15
Data size S_i	10–30 MB
CPU cycles C_i	1900 Cycle/s
Time Constraint $T_i^{\text{constraint}}$	0,002 s
Transmission data rate $D_{\text{IoT}}, D_{\text{UAV}}$	3–9 Mbps
Computation capacity of UAV-MEC (F_{UAV})	500 MHz
Computation capacity of edge-cloud server (F_{server})	1000 GHz

The number of tasks is set as $N = 15$ and 5 as the number of IoT nodes. The computational capabilities of UAV-MEC and edge-cloud server are 500 MHz and 1000 GHz, respectively. Hence, data size augmented randomly from 10 to 30 Megabyte. The CPU cycles needed to perform the task i is 1900 cycle/s. According

to the distances, the rates of transmission data also changed randomly 3 to 9 Mbps, which means that shorter distances mean bigger rate of transmission.

Figure 2 the delay versus transmission data rate, as shown in the figure, the delay decreases whenever transmission data rate increase when IoT nodes offloads all task to UAV-MEC or to edge-cloud server. As well as, in the Figure 3 the delay versus computational capability in case flying fog computing and edge-cloud server computing. The figure shows that the total delay decreased when increasing the computational capability when IoT nodes offloads the tasks to UAV-MEC or to edge-cloud server.

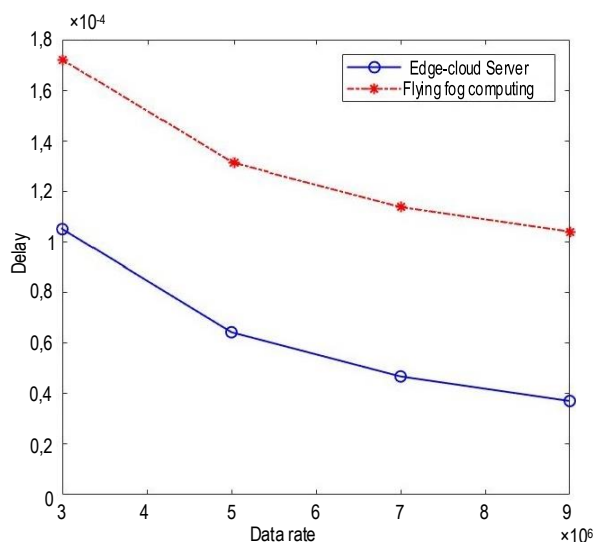


Fig. 2. Delay VS Data Rate

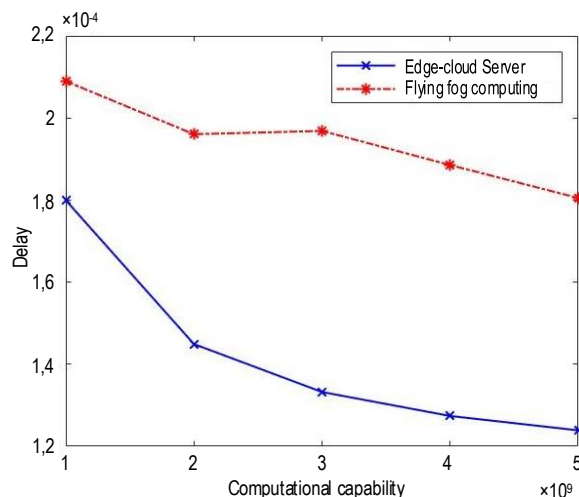


Fig. 3. Delay VS Computational Capability

In the figures 4 and 5, the delay in both figures increased linearly with increase the data size and number of tasks that generated from IoT nodes. As shown in the figure, the total delay is maximized when the tasks are offloaded and executed at UAV-MEC or remotely at edge-cloud server. The delay in case of flying fog computing much higher than the delay in case of edge-cloud server because of the computation capacity of edge-

cloud server much higher than the computation capacity of UAV-MEC.

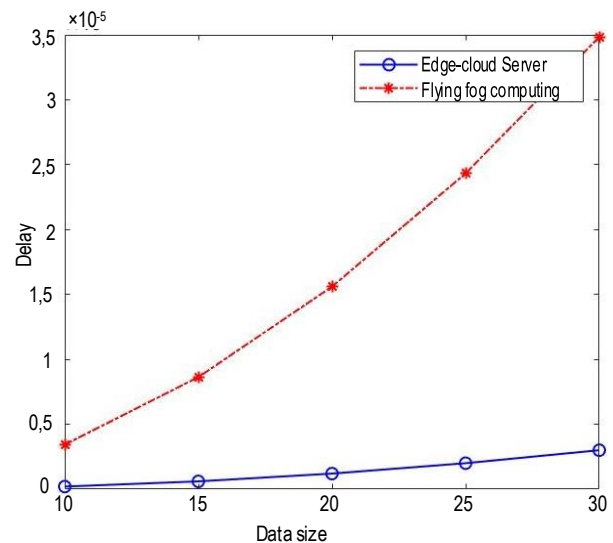


Fig. 4. Delay VS Data Size

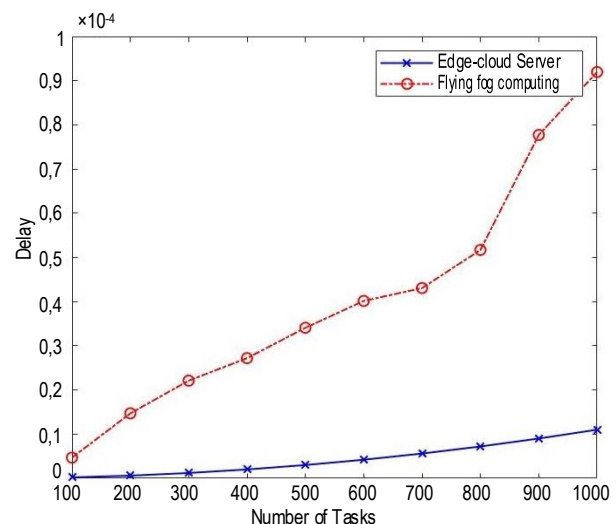


Fig. 5. Delay VS Number of Tasks

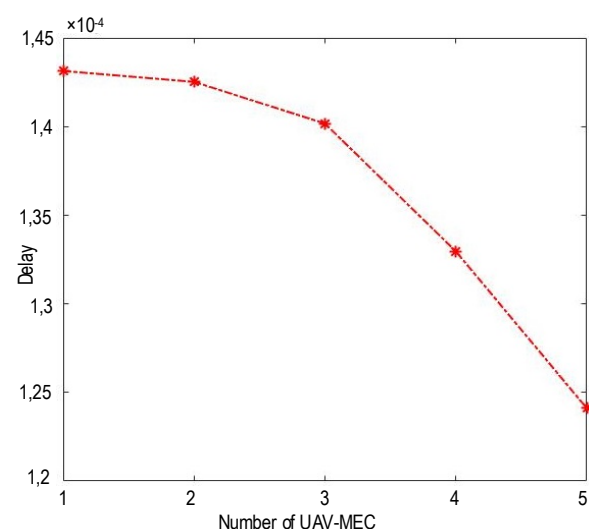


Fig. 6. Delay VS Number of UAV-MEC

Accordingly, to reduce the delay of computation task need to increase either the computational capacity of UAV-MEC or increase the number of UAV-MEC as shown in the figure 6.

Conclusion

In this paper, presented a computation offloading model based on flying fog mobile edge computing to assisting IoT devices in smart agriculture by using UAV mounted with computation resources, as well as remote edge cloud server. The processing and the services will be provided to the IoT devices either by nearby UAV-MEC or by remote edge server. The evolving of edge computing brings computing to the edge of

the network near data sources. The UAV and edge computing providing a promising solution for efficient intelligent IoT applications. We have formulated a delay-efficient computation offloading problem. Then we are proposed algorithm to solve the formulated problem, it was "Dynamic Programming with Hamming Distance Termination (DPH) algorithm" which showed good results to solve the proposed problem and realize a computation offloading tasks. The objective of work is to minimize the total delay to processing the data of IoT devices. In conclude, the results showed that the greater data rate, and greater the computational capability in both UAV-MEC and remote edge cloud server, the less delay to accomplish the tasks.

References

1. Naqvi S.A.R., Hassan S.A., Pervaiz, Ni Q. Drone-Aided Communication as a Key Enabler for 5G and Resilient Public Safety Networks. *IEEE Communications Magazine*. 2018;56(1):36–42. DOI:10.1109/MCOM.2017.1700451
2. Zhang M., Su C., Liu Y., Hu M., Zhu Y. Unmanned Aerial Vehicle Route Planning in the Presence of a threat Environment Based on a Virtual Globe Platform. *ISPRS International Journal of Geo-Information*. 2016;5(10):184. DOI:10.3390/ijgi5100184
3. Mahmud I., Cho Y.-Z. Adaptive Hello Interval in FANET Routing Protocols for Green UAVs. *IEEE Access*. 2019;7:63004–63015. DOI:10.1109/ACCESS.2019.2917075
4. Cao X., Yang P., Alzenad M., Xi X., Wu D., Yanikomeroglu H. Airborne Communication Networks: A Survey. *IEEE Journal on Selected Areas in Communications*. 2018;36(9):1907–1926. DOI:10.1109/JSAC.2018.2864423
5. Mozaffari M., Saad W., Bennis M., Debbah M. Mobile Unmanned Aerial Vehicles (UAVs) for Energy-Efficient Internet of Things Communications. *IEEE Transactions on Wireless Communications*. 2017;16(11):7574–7589. DOI:10.1109/TWC.2017.2751045
6. Alsamhi S.H., Ma O., Ansari M.S., Almalki F.A. Survey on Collaborative Smart Drones and Internet of Things for Improving Smartness of Smart Cities. *IEEE Access*. 2019;7:128125–128152. DOI:10.1109/ACCESS.2019.2934998
7. Alsamhi S.H., Ma O., Ansari M.S., Meng Q. Greening Internet of Things for Smart Everythings with a Green-Environment Life: A Survey and Future Prospects. 2018. DOI:10.48550/arXiv.1805.00844
8. Alsamhi S.H., Ma O., Ansari M.S., Gupta S.K. Collaboration of Drone and Internet of Public Safety Things in Smart Cities: An Overview of QoS and Network Performance Optimization. *Drones*. 2019;3(1):13. DOI:10.3390/drones3010013
9. Alsamhi S.H., Ma O., Ansari M.S., Almalki F.A. Survey on Collaborative Smart Drones and Internet of Things for Improving Smartness of Smart Cities. *IEEE Access*. 2019;7:128125–128152. DOI:10.1109/ACCESS.2019.2934998
10. Menouar H., Guvenc I., Akkaya K., Uluagac A. S., Kadri A., Tuncer A. UAV-Enabled Intelligent Transportation Systems for the Smart City: Applications and Challenges. *IEEE Communications Magazine*. 2017;55(3):22–28. DOI:10.1109/MCOM.2017.1600238CM
11. Motlagh N.H., Taleb T., Arouk O. Low-Altitude Unmanned Aerial Vehicles-Based Internet of Things Services: Comprehensive Survey and Future Perspectives. *IEEE Internet Things Journal*. 2016;3(6):899–922. DOI:10.1109/JIOT.2016.2612119
12. Mohammad M., Saad W., Bennis M., Debbah M. Mobile Internet of Things: Can UAVs Provide an Energy-Efficient Mobile Architecture? *Proceedings of the Global Communications Conference, GLOBECOM, 04–08 December 2016, Washington, USA*. IEEE; 2016. DOI:10.1109/GLOCOM.2016.7841993
13. Chen X., Shi Q., Yang L., Xu J. ThriftyEdge: Resource-Efficient Edge Computing for Intelligent IoT Applications. *IEEE Network*. 2018;32(1):61–65. DOI:10.1109/MNET.2018.1700145
14. Li X., Ma Z., Zheng J., Liu Y., Zhu L., Zhou N. An Effective Edge-Assisted Data Collection Approach for Critical Events in the SDWSN-Based Agricultural Internet of Things. *Electronics*. 2020;9(6):907. DOI:10.3390/electronics9060907
15. Alzaghir A., Koucheryavy A. Multi Task Multi-UAV Computation Offloading Enabled Mobile Edge Computing Systems. *Proceedings of the 24th International Conference on Distributed Computer and Communication Networks, DCCN, 20–24 September 2021, Moscow, Russia. Communications in Computer and Information Science, vol.1552*. Cham: Springer; 2021. DOI:10.1007/978-3-030-97110-6_1
16. Shahzad H., Szymanski T.H. A dynamic programming offloading algorithm for mobile cloud computing. *Proceedings of the Canadian Conference on Electrical and Computer Engineering, CCECE, 15–18 May 2016, Vancouver, Canada*. IEEE; 2016. DOI:10.1109/CCECE.2016.7726790
17. Koucheryavy A.E., Vladyko A.G., Kirichek R.V. Flying Ubiquitous Sensor Networks – A New Application of Internet of Things. *Proceedings of the IV International Conference on Infotelecommunications in Science and Education, 03–04 March 2015, St. Petersburg, Russia*. St. Petersburg: The Bonch-Bruевич Saint-Petersburg State University of Telecommunications Publ.; 2015. p.17–22. (in Russ.)
18. Vyrelkin A., Koucheryavy A. Using of Unmanned Aerial Vehicles for Solving the Problems of the Smart City. *Telecom IT*. 2017;5(1): 105–113. (in Russ.)
19. Alzaghir A.A., Koucheryavy A.E. Offloading Traffic When Integrating UAVs and Edge Computing Systems. *SPbNTORES: Proceedings of the Annual Scientific and Technical Conference*. 2022;1(77):115–116. (in Russ.)
20. Filimonova M.I., Alzaghir A.A., Muthanna A.S.A. Development of Methods of UAV Application to Ensure Stability of Communication Networks 2030. *SPbNTORES: Proceedings of the Annual Scientific and Technical Conference*. 2020;1(75):164–165. (in Russ.)

Список источников

1. Naqvi S.A.R., Hassan S.A., Pervaiz H., Ni Q. Drone-Aided Communication as a Key Enabler for 5G and Resilient Public Safety Networks // IEEE Communications Magazine. 2018. Vol. 56. Iss. 1. PP. 36–42. DOI:10.1109/MCOM.2017.1700451
2. Zhang M., Su C., Liu Y., Hu M., Zhu Y. Unmanned Aerial Vehicle Route Planning in the Presence of a threat Environment Based on a Virtual Globe Platform // ISPRS International Journal of Geo-Information. 2016. Vol. 5. Iss. 10. P. 184. DOI:10.3390/ijgi5100184
3. Mahmud I., Cho Y.-Z. Adaptive Hello Interval in FANET Routing Protocols for Green UAVs // IEEE Access. 2019. Vol. 7. PP. 63004–63015. DOI:10.1109/ACCESS.2019.2917075
4. Cao X., Yang P., Alzenad M., Xi X., Wu D., Yanikomeroglu H. Airborne Communication Networks: A Survey // IEEE Journal on Selected Areas in Communications. 2018. Vol. 36. Iss. 9. PP. 1907–1926. DOI:10.1109/JSAC.2018.2864423
5. Mozaffari M., Saad W., Bennis M., Debbah M. Mobile Unmanned Aerial Vehicles (UAVs) for Energy-Efficient Internet of Things Communications // IEEE Transactions on Wireless Communications. 2017. Vol. 16. Iss. 11. PP. 7574–7589. DOI:10.1109/TWC.2017.2751045
6. Alsamhi S.H., Ma O., Ansari M.S., Almalki F.A. Survey on Collaborative Smart Drones and Internet of Things for Improving Smartness of Smart Cities // IEEE Access. 2019. Vol. 7. PP. 128125–128152. DOI:10.1109/ACCESS.2019.2934998
7. Alsamhi S.H., Ma O., Ansari M.S., Meng Q. Greening Internet of Things for Smart Everything with a Green-Environment Life: A Survey and Future Prospects. 2018. DOI:10.48550/arXiv.1805.00844
8. Alsamhi S.H., Ma O., Ansari M.S., Gupta S.K. Collaboration of Drone and Internet of Public Safety Things in Smart Cities: An Overview of QoS and Network Performance Optimization // Drones. 2019. Vol. 3. Iss. 1. P. 13. DOI:10.3390/drones3010013
9. Alsamhi S.H., Ma O., Ansari M.S., Almalki F.A. Survey on Collaborative Smart Drones and Internet of Things for Improving Smartness of Smart Cities // IEEE Access. 2019. Vol. 7. PP. 128125–128152. DOI:10.1109/ACCESS.2019.2934998
10. Menouar H., Guvenc I., Akkaya K., Uluagac A. S., Kadri A., Tuncer A. UAV-Enabled Intelligent Transportation Systems for the Smart City: Applications and Challenges // IEEE Communications Magazine. 2017. Vol. 55. Iss. 3. PP. 22–28. DOI:10.1109/MCOM.2017.1600238CM
11. Motlagh N.H., Taleb T., Arouk O. Low-Altitude Unmanned Aerial Vehicles-Based Internet of Things Services: Comprehensive Survey and Future Perspectives // IEEE Internet Things Journal. 2016. Vol. 3. Iss. 6. PP. 899–922. DOI:10.1109/JIOT.2016.2612119
12. Mohammad M., Saad W., Bennis M., Debbah M. Mobile Internet of Things: Can UAVs Provide an Energy-Efficient Mobile Architecture? // Proceedings of the Global Communications Conference (GLOBECOM, Washington, USA, 04–08 December 2016). IEEE, 2016. DOI:10.1109/GLOCOM.2016.7841993
13. Chen X., Shi Q., Yang L., Xu J. ThriftyEdge: Resource-Efficient Edge Computing for Intelligent IoT Applications // IEEE Network. 2018. Vol. 32. Iss. 1. PP. 61–65. DOI:10.1109/MNET.2018.1700145
14. Li X., Ma Z., Zheng J., Liu Y., Zhu L., Zhou N. An Effective Edge-Assisted Data Collection Approach for Critical Events in the SDWSN-Based Agricultural Internet of Things // Electronics. 2020. Vol. 9. Iss. 6. P. 907. DOI:10.3390/electronics9060907
15. Alzaghir A., Koucheryavy A. Multi Task Multi-UAV Computation Offloading Enabled Mobile Edge Computing Systems // Proceedings of the 24th International Conference on Distributed Computer and Communication Networks (DCCN, Moscow, Russia, 20–24 September 2021). Communications in Computer and Information Science. Vol. 1552. Cham: Springer, 2021. DOI:10.1007/978-3-030-97110-6_1
16. Shahzad H., Szymanski T.H. A dynamic programming offloading algorithm for mobile cloud computing // Proceedings of the Canadian Conference on Electrical and Computer Engineering (CCECE, Vancouver, Canada, 15–18 May 2016). IEEE, 2016. DOI:10.1109/CCECE.2016.7726790
17. Кучерявый А.Е., Владыко А.Г., Киричек Р.В. Летящие сенсорные сети-новое приложение интернета вещей // IV Международная научно-техническая и научно-методическая конференция «Актуальные проблемы инфотелекоммуникаций в науке и образовании» (Санкт-Петербург, Россия, 03–04 марта 2015). Сборник научных статей. СПб.: СПбГУТ, 2015. С. 17–22.
18. Вырелкин А.Д., Кучерявый А.Е. Использование беспилотных летательных аппаратов для решения задач «умного города» // Информационные технологии и телекоммуникации. 2017. Т. 5. № 1. С. 105–113.
19. Алзагир А.А., Кучерявый А.Е. Разгрузка трафика при интеграции БПЛА и граничных вычислительных систем // СПбНТОРЭС: труды ежегодной НТК. 2022. № 1(77). С. 115–116.
20. Филимонова М.И., Алзагир А.А., Мутханна А.С.А. Разработка методов применения БПЛА для обеспечения устойчивости сетей связи 2030 // СПбНТОРЭС: труды ежегодной НТК. 2020. № 1(75). С. 164–165.

Статья поступила в редакцию 23.11.2022; одобрена после рецензирования 12.12.2022; принята к публикации 13.12.2022.

The article was submitted 23.11.2022; approved after reviewing 12.12.2022; accepted for publication 13.12.2022.

Информация об авторе:

**АЛЗАГИР
Аббас Али**

аспирант кафедры сети связи и передачи данных Санкт-Петербургского государственного университета телекоммуникаций им. проф. М.А. Бонч-Бруевича
 <https://orcid.org/0000-0003-2937-9934>

Научная статья

УДК 004.27+004.056

DOI:10.31854/1813-324X-2022-8-4-89-99



Методы машинного обучения для прогнозирования трафика в многоуровневой облачной архитектуре для сервисов автономных транспортных средств

Малик Аль-Свейти, aldonasmar@gmail.com

Санкт-Петербургский государственный университет телекоммуникаций им. М.А. Бонч-Бруевича,
Санкт-Петербург, 193232, Российская Федерация

Аннотация: Автономные транспортные средства (AV, аббр. от англ. Autonomous Vehicle) являются одним из наиболее важных новых вариантов использования и перспективной технологией для сетей пятого поколения (5G) и следующего поколения в многочисленных приложениях. В настоящее время использование AV экспоненциально растет во всем мире, благодаря быстрому росту осведомленности и применению методов искусственного интеллекта в различных областях. Прогнозирование потоков данных необходимо для AV, чтобы улучшить передачу данных и уменьшить задержки за счет более эффективного использования соответствующих возможностей, мониторинга, управления и контроля дорожной системы. В данной работе предлагается подход глубокого обучения с двунаправленной моделью с долгой краткосрочной памятью (BI-LSTM, аббр. от англ. Bidirectional Long-Short-Term Memory) для прогнозирования сетевого трафика AV с многоуровневыми сервисами облачных вычислений. С точки зрения точности прогнозирования проводится сравнение между BI-LSTM и однонаправленной моделью с долгой краткосрочной памятью (LSTM) в зависимости от количества используемых пакетов. Точность предсказания рассчитывается с помощью среднеквадратичной ошибки, средней абсолютной процентной ошибки, коэффициента детерминации (R^2) и времени обработки. Результаты показывают, что точность прогнозирования с помощью BI-LSTM превосходит модель LSTM. Кроме того, точность прогнозирования с использованием размера обучающей партии (BatchSize) равной 8, превосходит конкурентов и обеспечивает высокую производительность.

Ключевые слова: беспилотные автомобили, 5G, MEC, ML, DL, прогнозирование, BI-LSTM, LSTM

Ссылка для цитирования: Аль-Свейти М. Методы машинного обучения для прогнозирования трафика в многоуровневой облачной архитектуре для сервисов автономных транспортных средств // Труды учебных заведений связи. 2022. Т. 8. № 4. С. 89–99. DOI:10.31854/1813-324X-2022-8-4-89-99

Deep Learning Approaches for Traffic Prediction Forecasting in Multi-Level Cloud Architecture for Autonomous Vehicle Services

Malik Alsweity, aldonasmar@gmail.com

The Bonch-Bruevich Saint-Petersburg State University of Telecommunications,
St. Petersburg, 193232, Russian Federation

Abstract: Autonomous vehicle (AV) is one of the most new use cases and a technology for fifth-generation (5G) and next-generation mobile networks in numerous applications., the use of AVs has exponentially worldwide due to the rapidly growing awareness and use of artificial intelligence (AI) methods in various fields. Predicting data flows is essential for AVs to improve data transmission and decrease delays through more efficient use of appropriate

capabilities, monitoring, management, and control of the traffic system. This paper proposes a deep learning approach (DL) with the bidirectional long-short-term memory model (BI-LSTM) for predicting the traffic rates of AVs with multi-cloud services. In terms of prediction accuracy, a comparison is conducted between the BI-LSTM and the unidirectional LSTM based on the number of batch sizes used. The prediction accuracy is computed using the root mean square error (RMSE), mean absolute percentage error (MAPE), coefficient of determination (R^2), and processing time. The results show that the prediction accuracy with BI-LSTM outperforms the LSTM model. Besides, the prediction accuracy using 8 batch sizes outperforms the competitors and offers outstanding performance.

Keywords: autonomous vehicles, 5G, MEC, ML, DL, prediction, BI-LSTM, LSTM

For citation: Alsweity M. Deep Learning Approaches for Traffic Prediction Forecasting in Multi-Level Cloud Architecture for Autonomous Vehicle Services. *Proc. of Telecom. Universities*. 2022;8(4):89–99. (in Russ.) DOI:10.31854/1813-324X-2022-8-4-89-99

ВВЕДЕНИЕ

Многоуровневая сетевая структура отличается от любой другой структуры, поскольку она охватывает, контролирует, управляет локальными облачными структурами и предлагает лучшие возможности, чем поставщики облачных услуг. Многоуровневая архитектура обеспечивает стабильную и повторяемую архитектуру на нескольких платформах: она является основной в производстве, а также ядром нынешнего и будущего публичного облака. С ростом использования Интернета вещей (IoT, аббр. от англ. Internet of Things) в различных сферах жизни, включая обмен данными в реальном времени между пользователями и машинами, приобрел актуальность тактильный интернет, который позволил системе IoT мгновенно и быстро взаимодействовать в промышленных и коммерческом секторах.

Ожидается, что технологии беспроводной связи следующего поколения, включая сети 5G и выше, станут важным фактором успеха беспилотных автомобилей в ближайшие годы. Они позволят внедрить новые услуги и сценарии применения в будущем интеллектуальном транспорте, благодаря возможности быстрого и надежного обмена данными между различными субъектами. Развитие коммуникационных технологий для интеллектуальных транспортных систем в сочетании с передовой обработкой данных и искусственным интеллектом (AI, аббр. от англ. Artificial Intelligence) означает, что такие важные функции как обеспечение крупномасштабных сетей, выбор технологий для гетерогенного беспроводного доступа, а также интеллектуальные и безопасные интегрированные услуги, пользуются большим спросом [1].

Полностью функциональная и эффективная сеть 5G невозможна без AI. Сочетание машинного обучения (ML аббр. от англ. Machine learning) и AI на границе сети может быть достигнуто путем распределения сетей 5G. Данное сочетание обеспечивает синхронное подключение нескольких устройств IoT и генерирует большое количество данных, которые могут быть обработаны с помощью ML и AI. Это позволяет таким сетям быть

предиктивными и проактивными, что необходимо для эффективности сети пятого поколения. Добавив ML к технологии 5G, интеллектуальные каналы могут принимать собственные решения. Мобильные устройства могут создавать гибкие, динамические коллекции в соответствии со считанными данными, что повышает эффективность, латентность и надежность сетевых приложений.

Как только ML и AI будут объединены с 5G и периферийными вычислениями для множественного доступа (MEC, аббр. от англ. Multi-Access Edge Computing), мобильные операторы смогут обеспечить [2, 3]:

- значительные вычислительные возможности за счет распределенной структуры ML и AI на границе сети;
- управление трафиком в сетях доступа на основе приложений;
- динамическую нарезку сети (слайсинг, от англ. slice), которая охватывает различные сценарии с различными условиями качества обслуживания (QoS, аббр. от англ. Quality of Service) [4].

Беспилотные автомобили с поддержкой многоуровневых облачных вычислений растут во всем мире по экспоненте, поскольку репутация методов искусственного интеллекта и их использование в многочисленных приложениях резко возросли. Прогнозирование транспортных потоков необходимо для того, чтобы беспилотные автомобили определяли маршрут движения и принимали адаптивные решения относительно окружающих их объектов. Связь между транспортными средствами (V2V, аббр. от англ. Vehicle-to-Vehicle) позволяет автомобилям общаться друг с другом, передавая данные о скорости и местоположении. Когда система транспортных средств обменивается данными с придорожной инфраструктурой (V2I, аббр. от англ. Vehicle-to-Infrastructure), придорожное устройство (RSU, аббр. от англ. Roadside Unit) берет на себя управление движением транспортных средств и отправляет широковещательное сообщение всем ближайшим автомобилям [5, 6].

Существуют специфические проблемы, связанные с маршрутизацией в автомобильных сетях

(VANET) – топология сети, различная плотность трафика в разное время и быстрые изменения прибывающих и убывающих транспортных средств и пр. Все эти проблемы требуют системного решения на базе современных технических решений, в качестве которого предлагается построение некой системы для сервисов AV с многоуровневой облачной архитектурой поддержки вычислений с использованием методов искусственного интеллекта.

Предлагаемая архитектура системы, показанная на рисунке 1, состоит из четырех уровней. Уровень 1 – это физическое оборудование, включающее в себя бортовые устройства (OBU, аббр. от англ. On-Board Unit), которые могут быть подключены к распределенным RSU. RSU может представлять собой интеллектуальный мультисервисный узел доступа, используемый вместо небольших сетевых узлов при расширении традиционных сетей и создании новых сетей с большим количеством удаленных объектов.

Уровень 2 содержит гетерогенные, облачные, граничные серверы, расположенные вдоль границы радиосети (RAN, аббр. от англ. Radio Access Network). Предлагаемая система состоит из двух серверов MEC: миниоблака и микрооблачного граничного сервера. Каждый RSU связан с мобильными базовыми станциями и граничным сервером микрооблака. Граничный сервер микрооблака работает с ограниченными вычислительными и энергетическими возможностями. Каждый набор серверов микрооблака связан с пограничным сервером миниоблака с мощными вычислительными и энергетическими ресурсами.

Уровень 3 – это программно-определяемая сеть (SDN, аббр. от англ. Software-Defined Network), распределенная по основной сети. Этот уровень состоит из двух основных подуровней: управления и уровня данных. На уровне данных находятся распределенные виртуальные коммутаторы OpenFlow, которые обслуживают протокол OpenFlow.

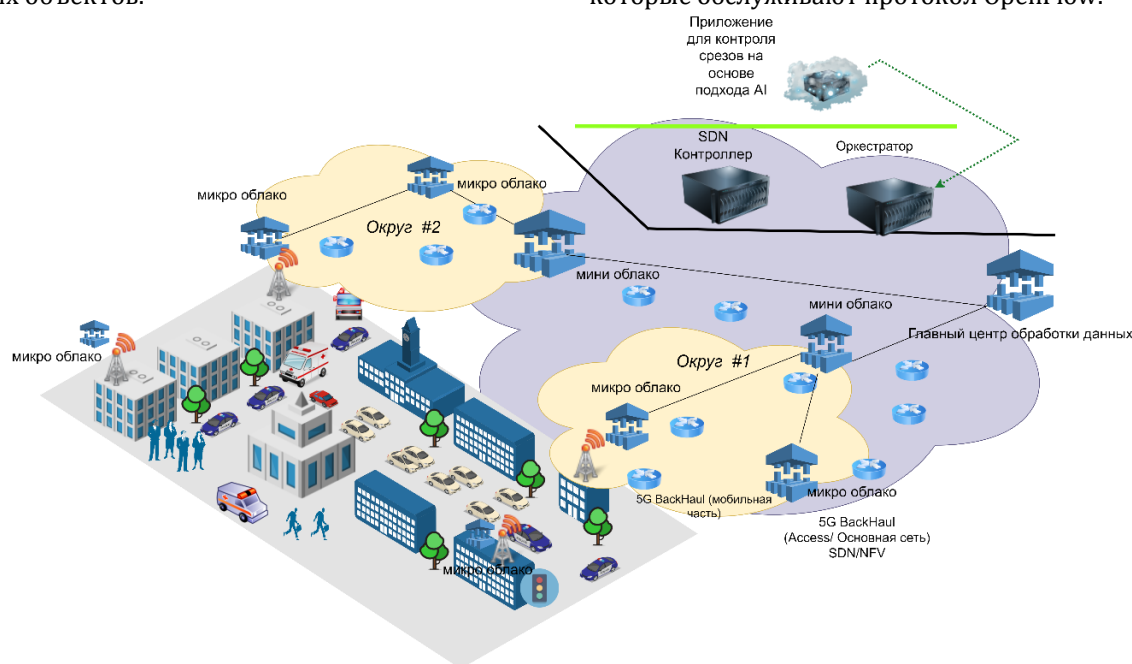


Рис. 1. Предлагаемая многоуровневая облачная система

Fig. 1. The proposed Multi-Level Cloud System

Уровень управления (Уровень 4) включает распределенные SDN для управления и контроля всей сети. Интерфейс прикладных программ (API, аббр. от англ. Application Programming Interface) управляет SDN и основными сетевыми интерфейсами к Уровню 1 и серверу приложений. Предлагаемая система имеет два прямых интерфейса на Уровне 1. Первичным интерфейсом является транспортное средство, а последующим – так называемая, «внутренняя инфраструктура» транспортного средства. Это может быть достигнуто через соответствующую сеть IEEE 802.11, различные стандарты связи для беспроводной локальной сети связи (WLAN,

аббр. от англ. Wireless Local Area Network) на различных частотах.

На Уровне 2 распределенные граничные серверы связаны через быструю беспроводную сеть. Каждый RSU связан с сервером MEC для обеспечения вычислительной мощности на границе сети доступа. Это снижает трафик на ведущую сеть, уменьшая ее перегрузку или потерю пакетов.

Концепции глубокого обучения (DL, аббр. от англ. Deep Learning) привлекают внимание многих исследователей благодаря своей способности решать проблемы распознавания, понимания естественного языка, сокращения размерности, иден-

тификации объектов, моделирования движения, прогнозирования трафика и т.д. DL использует концепции многослойных нейронных сетей для вывода глубинных свойств данных от самого низкого до самого высокого уровня. Они находят в данных большое количество структур, которые позволяют их представить и сделать логические выводы. Разработка беспилотного автомобиля, который может сделать транспортные сети гораздо более экономичными и снизить риск для жизни людей, также является предметом изучения разработчиков и исследователей интеллектуальных транспортных систем (ITS, *аббр. от англ. Intelligent transportation system*). Концепция DL также имеет такое существенное преимущество, как экономия времени, что особенно важно для обеспечения безопасного автоматизированного вождения – информация от систем помощи водителю, автономных транспортных средств и систем распознавания дорожных знаков [1, 7] должна поступать своевременно, без критической во величине задержки.

Прогнозирование сетевого трафика является важным инструментом для беспроводных сетей 5G и других сетей, позволяющим управлять перегрузкой и ресурсами сети, а также обеспечивать безопасность, надежность и устойчивость (связность) выбранных сетей. Использование статистических временных рядов или подходов машинного обучения позволяет прогнозировать будущие потоки сетевого трафика на основе предыдущих данных. Эффективное прогнозирование может улучшить QoS и снизить эксплуатационные расходы для поставщиков сетевых услуг. Существующие источники показывают, что DL-модели более эффективно подходят для моделирования сетевого трафика и более точно предсказывают будущий трафик, чем традиционные модели [2, 3, 8].

Анализ существующих работ

В последнее время многие исследователи сосредоточились на прогнозировании трафика беспроводных сетей с использованием методов DL и технологии 5G. Данная статья посвящена прогнозированию трафика в автономных транспортных средствах с многоуровневыми облачными вычислениями с использованием DL-подхода на основе BI-LSTM (*аббр. от англ. Bidirectional Long-Short-Term Memoгу – двунаправленная модель с долгой краткосрочной памятью*) и LSTM (*однонаправленная модель*). Ниже представлены основные работы, имеющие отношение к предметной области.

В работе [9] рассматривается прогнозирование сетевого трафика с использованием глубоких нейронных сетей (DNN, *аббр. от англ. Deep Neural Network*). Исследуется то, как DNN могут заранее предсказать приблизительную скорость сетевого взаимодействия. В работе [10] было выполнено

прогнозирование задержки IoT с помощью многопараметрического метода DNN. В [11, 12] изучалось долгосрочное и краткосрочное прогнозирование трафика беспроводной сети с помощью LSTM с поддержкой DL. В [13] авторами представлены решения на основе DL для сетей 5G и интернета транспортных средств (IoV, *аббр. от англ. Internet of Vehicles*). В статье [14] рассматриваются последние исследования беспроводных сетей следующего поколения и роль методов машинного обучения (ML, *аббр. от англ. Machine Learning*) в этих будущих беспроводных системах. Прогнозирование трафика по временным рядам с использованием DL и LSTM-сети для граничных вычислений с поддержкой IoT выполнено в работе [15].

В работе [16] представлены исследования проблемы прогнозирования трафика IoT с помощью ML, DL, статистических методов прогнозирования на основе временных рядов, таких как LSTM, ARIMA, VARMA и нейронных сетей прямого распространения (FFNNs, *аббр. от англ. Feed Forward Neural Networks*). В статье [17] был представлен обширный обзор современных ML-подходов к прогнозированию сотового трафика в сетях 5G. В работе [17] проведены исследования прогнозирования маршрута транспортного средства на основе ML с использованием V2V-взаимодействия и бортовых датчиков. Представлен метод прогнозирования маршрута с использованием алгоритма случайного леса и архитектуры кодер-декодер LSTM.

Проанализированные релевантные работы позволили сделать некоторые предварительные выводы относительно способа решения задачи прогнозирования трафика в беспроводной коммуникационной среде AV с многоуровневой облачной архитектурой поддержки вычислений с использованием методов искусственного интеллекта. Представляется, что гипотетически перспективным является DL-подход на основе моделей рекуррентных нейронных сетей типа LSTM и их возможных модификаций, адаптированных под предметную область.

Рекуррентные нейронные сети для решения задач последовательного

А. Сеть долгой краткосрочной памяти (LSTM)

Одной из самых популярных и часто используемых модельных структур в искусственном интеллекте является LSTM. Сеть LSTM – это тип рекуррентной нейронной сети (RNN, *аббр. от англ. Recurrent Neural Network*), наиболее подходящих для долгосрочного хранения данных и обычно используемых в области DL. Поскольку большие объемы данных могут повлиять на производительность модели, она является естественным выбором для построения, обучения и развертывания сети. Преимущество LSTM в том, что она помогает обес-

печить меньшее влияние на независимые связи. Кроме того, сеть должна быть обучена определять, какой фрагмент информации подходит для сети, и иметь точное представление о том, что нужно хранить. В случае DL, LSTM применяется многократно.

Стандартная структура ячеек LSTM показана на рисунке 2. Ячейка в LSTM имеет три основных узла, называемых гейтами (gate), управляющих ее состоянием: входной (input gate), забывания (forget gate) и выходной (output gate), а фактическая ячейка обратной связи – это скрытое состояние.

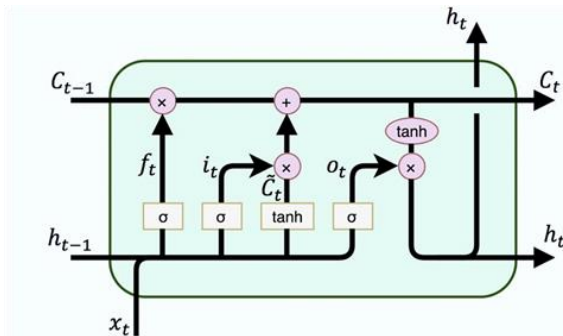


Рис. 2. Структура сети LSTM

Fig. 2. Structure of LSTM Network

Гейты LSTM представляют собой сигмоидальную передаточную функцию (1):

$$\sigma(x) = \frac{1}{1 + e^{-x}}. \quad (1)$$

Следует оценить гейт забывания, как процентный вклад входа; входной гейт выбирает текущую информацию для хранения в ячейке памяти. Текущий вектор значений-кандидатов может быть использован для состояния слоя активации гиперболического тангенса (tanh-слой – один из типов слоев, используемых в нейронных сетях, который включает свои собственные весовые матрицы). Входной гейт подключается к tanh-слою для получения изменения состояния. Выход функции активации tanh соответствует значению между -1 и 1 для определения его значимости.

Оценка использует функцию $\tanh(x)$ следующим образом:

$$\tanh(x) = \frac{e^x - e^{-x}}{e^x + e^{-x}}. \quad (2)$$

Другие связи увеличивают связность модели. Предположим, что x_t и h_t – это векторы входного и скрытого состояния по времени t . В этом случае W_i и W_h представляют собой матрицы весовых коэффициентов, которые применяются к входному пути и обратной связи, соответственно, а b – вектор смещения.

Учитывая следующий вход x_t для скрытого состояния f с предыдущего шага h_{t-1} и текущее состояние ячейки C_{t-1} , вычисляются зависимости для

входного гейта i_t , ворот забывания f_t и выходных ворот o_t в LSTM:

$$i_t = \sigma(w_i x_t + g_i h_{t-1} + b_i), \quad (3)$$

$$f_t = \sigma(w_f x_t + g_f h_{t-1} + b_f), \quad (4)$$

$$o_t = \sigma(w_o x_t + g_o h_{t-1} + b_o), \quad (5)$$

где i_t, f_t, o_t – функции весовых матриц $w_i, g_i, w_f, g_f, w_o, g_o$ и векторов смещения b_i, b_f, b_o .

Компактные формы для уравнений состояния клетки-кандидата, состояния ячейки-кандидата и вектора скрытого состояния (выходного вектора) следующие:

$$C'_t = \tanh(w_c x_t + g_c h_{t-1} + b_c), \quad (6)$$

$$C_t = f_t \odot C_{t-1} + i_t \odot C'_t, \quad (7)$$

$$h_t = o_t \odot \tanh(C'_t), \quad (8)$$

Состояние ячейки-кандидата $\tilde{C}_t$ определяются как функция весовых матриц w_c и g_c ; оператор $\odot$ обозначает произведение Hadamard (произведение по элементам).

В. Двухнаправленная LSTM (BI-LSTM)

Двухнаправленные LSTM основаны на блоке LSTM, где два LSTM подаются на входной сигнал. Одна подается на входной ряд (путь прямого распространения). На втором этапе обратная форма входного ряда подается на модель LSTM (путь обратного распространения). Сеть LSTM анализирует только влияние прошлой серии на текущую и игнорирует более позднюю информацию, поэтому оптимальная производительность не достигается. В отличие от этого BI-LSTM связывает выход блока LSTM двухнаправленно. Она улавливает двухнаправленные зависимости сигналов, что повышает общую производительность модели. BI-LSTM – это последовательная вычислительная модель, состоящая из двух LSTM. Каждая нейронная сеть имеет ряд информации в обратном пути (от приходящей к предыдущей) и прямом пути (от последней к приходящей). В двухнаправленной сети входные данные поступают в двух направлениях, что отличает BI-LSTM от обычной LSTM. В обычной LSTM входной поток может идти в одном направлении: либо назад, либо вперед. В двухнаправленной LSTM можно заставить входные данные поступать в обоих направлениях, чтобы получить информацию из будущего и прошлого.

BI-LSTM эффективно увеличивают количество информации, доступной сети, улучшая содержание, доступное алгоритму. Прямое и обратное направления BI-LSTM одновременно передаются на выходной модуль. Таким образом, могут быть получены прошлые и предстоящие данные, как показано на рисунке 3. В каждый момент времени t вход подается на прямой и обратный путь сети LSTM.

Выход BI-LSTM может быть представлен следующим образом:

$$\vec{h}_t = H(W_1 x_t + W_2 \vec{h}_{t-1} + \vec{b}), \quad (9)$$

$$\vec{h}_t = H(W_3 x_t + W_5 \vec{h}_{t-1} + \vec{b}), \quad (10)$$

$$y_t = W_4 \vec{h}_t + W_6 \vec{h}_t + b_y, \quad (11)$$

где $\vec{h}_t$, $\vec{h}_t$, и y_t – векторы для прямого, обратного и выходного слоев; W – весовые коэффициенты; $\vec{b}$, $\vec{b}$ и b_y – соответствующие векторы смещения.

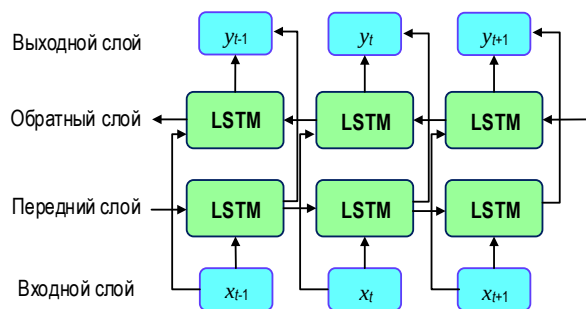


Рис. 3 Структура нейронной сети Bi-LSTM

Fig. 3. Structure of Bi-LSTM Neural Network

На рисунке 3 можно видеть поток информации в обратном и прямом слоях. BI-LSTM обычно используется там, где требуется последовательность задач. Этот тип сети может использоваться в классификации текстов, распознавании речи и прогнозистических моделях.

Постановка задачи и модель системы

Для прогнозирования сетевого трафика использовалось множество методов машинного обучения, таких как Random Forest [18], ARIMA [16, 19], VARMA [16], LSTM [2, 11, 12, 15], NARX [3, 8, 20, 21] и др. В данной статье предложены двунаправленная BI-LSTM и однонаправленная LSTM с DNN для прогнозирования трафика в автономном транспортном средстве на основе многоуровневых облачных вычислений.

Для проведения исследования было выполнено построение DL на основе блоков LSTM и BI-LSTM для прогнозирования трафика. Для получения обучающего набора данных была создана система AV с помощью симулятора AnyLogic. После сбора, исследования и обработки набора данных они использовались в качестве входных данных для DL и для метода прогнозирования. Затем набор данных применялся к сети в двух подмножествах: в столбцах входных данных (I) и выводных (O), – а затем разбивался на подмножества для обучения и тестирования. Нормирование входных данных должно было находиться в интервале $[-1, 1]$, что соответствует фактическим максимальным или минимальным значениям.

Далее выполнялись этапы обучения, тестирования и внедрения. Следует отметить, что в данном

исследовании не использовался проверочный набор для сети и не проводилась оптимизация статических гиперпараметров сети, таких как размер слоя LSTM. Модель DL была обучена в среде VANET с использованием различных размеров порций для BI-LSTM и LSTM. Цель этапа состояла в том, чтобы найти оптимальный размер обучающей партии, который обеспечит наилучшую точность прогнозирования.

А. Среда VANET

Пусть трафик представляет собой пуассоновский поток, а экспоненциальное распределение описывает время обслуживания. Модель очереди в целом совместима с методом $M/M/1/k$ с ограниченным буфером.

Тогда вероятность того, что входящая информация не попадет в систему (вероятность потери) определяется выражением:

$$p = \frac{1 - \rho}{1 - \rho^{n+2}} \rho^{n+1}. \quad (12)$$

В этом уравнении $\rho = a/\mu$, где a – интенсивность входящих сообщений; μ – интенсивность входящего трафика; в этом случае производительность сервера равна ti .

Следующее уравнение позволяет рассчитать средний размер очереди при $i = 1$:

$$\bar{L} = \frac{\rho(1 - (n + 1)\rho^n + k\rho^{n+1})}{(1 - \rho)(1 - \rho^{n+1})}. \quad (13)$$

Среднее время отклика первого слоя представлено следующим образом:

$$T = (\bar{L} + 1)\bar{t}. \quad (14)$$

Сравнивая конструкцию с ограниченным и неограниченным размером очереди, вычисляется задержка системы $M/M/1$:

$$\bar{T}_m = \frac{\bar{t}}{1 - \rho}. \quad (15)$$

Для метода $M/M/1$ нагрузка на сервер достаточна для обеспечения трафика; для метода $M/M/1/k$ нагрузка на сервер может быть вычислена следующим образом:

$$u_i = 1 - P_0, \quad (16)$$

$$P_0 = \begin{cases} \frac{1}{n+1} & \rho_i = 1 \\ \frac{1 - \rho_i}{1 - \rho_i^{n+1}} & \rho_i \neq 1 \end{cases}, \quad (17)$$

где P_0 – вероятность того, что сервер не работает в это время.

Предлагается модель реализации для МЕС с учетом вышеприведенного предположения о модели очереди. Чтобы увеличить использование метода

МЕС (микро- или миниоблака), следует выбрать режим повышенного использования облака; однако это приведет к ухудшению QoS. Предлагается использовать несколько уровней, включая облака, предназначенные для обслуживания избыточного трафика, поступающего с соседних уровней. Такой метод работает по следующей схеме: коммуникации с регионом VANET, ограниченным регионом EDC, поступают в облако первого уровня, описываемое системой очередей $M/M/1/k$ (первый уровень). Предполагается, что производительность облака μ_1 определяется временем обслуживания t_1 . И выбираем значение t на основе времени доставки T_0 и требований к нагрузке сервера.

В. Имитационная модель

Как показано на рисунке 4, структура моделируемой сети представляет собой некую реализацию метода очередей.

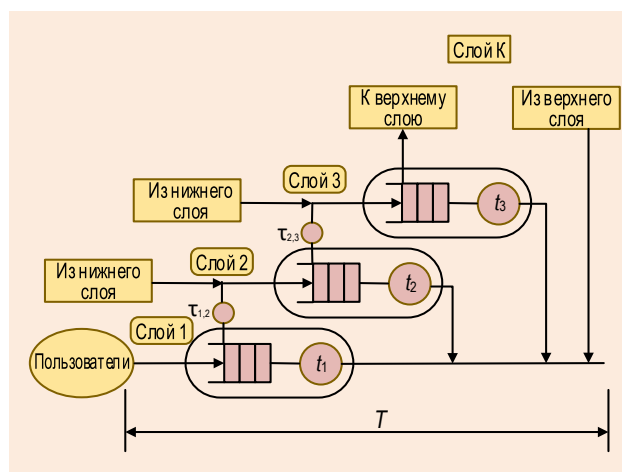


Рис. 4. Структура сети
Fig. 4. Network Structure

Каждый слой модели состоит из одного сервера и одной очереди, и каждая очередь имеет два выхода и только один вход. Вход очереди принимает входящую информацию от этого слоя. Выходом является верхняя часть очереди, подключенная к серверу. Если некоторые запросы не были удовлетворены на данном уровне (потерянные рекомендации), они выходят из очереди и продолжают поступать на следующий уровень через этот выход. Существуют разные причины, по которым запросы не были обслужены от одной среды к другой.

Для среды VANET использовалась следующая структура модели: каждый слой описывает стационарную ячейку базовой станции и потерянные запросы из-за чрезмерного трафика в первом случае; во втором случае потери вызваны слишком большой задержкой, превышающей T_m .

Обычно в этих двух случаях можно использовать несколько приоритетных запросов. Тем не

менее, предполагалось, что все пакеты (сообщения) в среде VANET однородны, и из-за этого использовались неприоритетные очереди.

Результаты моделирования

В этой статье осуществляется прогнозирование трафика на основе DL-подхода с использованием BI-LSTM и LSTM сетей для AV с многоуровневыми облачными вычислениями. Точность прогнозирования измерялась с помощью RMSE, MAPE, R^2 и времени обработки, с использованием функции потерь MSE и скорости обучения 0,1. Было проведено сравнение между BI-LSTM и однонаправленной LSTM с использованием RMSE, MAPE, R^2 и времени обработки при различных размерах для среды VANET. Наборы данных для обучения были получены из многоуровневых облачных вычислений с поддержкой AV. Данная работа была выполнена с использованием MATLAB, так как набор данных был собран и обработан, он был разделен на 70 и 30 % для обучения, а также 30 % для тестирования.

Для расчета точности прогнозирования применялись математические формы для RMSE, MAPE и R^2 , как описано в уравнениях (9) и (10):

$$RMSE = \sqrt{\frac{1}{N} \sum_{i=1}^n (y_i - \hat{y}_i)^2}, \quad (28)$$

$$MAPE = \frac{1}{N} \sum_{i=1}^n \left| \frac{y_i - \hat{y}_i}{x_t} \right|, \quad (29)$$

$$R^2 = 1 - \frac{SS_{Regression}}{SS_{Total}} = 1 - \frac{\sum_i (y_i - \hat{y}_i)}{\sum_i (y_i - \bar{y}_i)}, \quad (30)$$

где N – общее число наблюдений; y_i – фактическое значение; $\hat{y}_i$ – предсказанное значение; $\bar{y}_i$ – среднее значение всех значений; SS_{Total} – сумма общих квадратичных ошибок; $SS_{Regression}$ – сумма квадратичных ошибок регрессии.

В таблице 1 показана точность предсказания скорости трафика в случае использования среды VANET при трех различных размерах обучающей партии BatchSizes с точки зрения использования двух различных BI-LSTM и LSTM-моделей с учетом функции потерь MSE в качестве меры производительности и скорости обучения 0,1. Чтобы исследовать модель прогнозирования, которая обеспечивает парадигмальную точность и максимальное среднее улучшение, масштабировалась точность прогнозирования с помощью среднеквадратичной ошибки (RMSE, аббр. от англ. Root Mean Square Error), средней абсолютной процентной ошибки (MAPE, аббр. от англ. Mean Absolute Percentage Error) и коэффициента детерминации R^2 .

ТАБЛИЦА 1. Точность прогнозирования трафика в среде VANET
TABLE 1. The Prediction Accuracy for the Traffic Rate in the VANET Environment

Batch Sizes	BI-LSTM / LSTM			
	RMSE	MAPE%	R^2	Время обработки
8	0,0241 / 0,0547	2,9902 / 5,1858	0,9959 / 0,9862	44,5000 / 27,7969
16	0,0350 / 0,0954	4,3937 / 10,3052	0,9958 / 0,9732	39,8750 / 28,6563
64	0,0943 / 0,1379	10,8848 / 15,3204	0,9721 / 0,9436	25,1094 / 36,1719

Как видно из результатов в таблице 1, при использовании BatchSizes = 8 точность предсказания превосходит конкурентов и имеет наилучшие показатели для BI-LSTM и LSTM сетей.

Соответственно, максимальное среднее улучшение в обоих случаях составляет 7.9 и 10.135 %. Однако это занимает больше всего времени обработки для BI-LSTM и быстрее всего для LSTM. Точность прогнозирования при BatchSizes = 16 примерно такая же, как и при BatchSizes = 8. В этом случае максимальное среднее улучшение составляет 6.5 и 5.12 % соответственно для BI-LSTM и LSTM. Однако, точность прогнозирования при использовании BatchSizes = 64 достаточно низкая по сравнению с другими, хотя имеет самое быстрое

время обработки для BI-LSTM, но самое длительное для LSTM. Кроме того, коэффициент детерминации R^2 примерно одинаков в обоих случаях и близок к 1, что указывает на хорошее соответствие. С другой стороны, точность предсказания с помощью BI-LSTM выше, чем у LSTM во всех случаях, а максимальное среднее улучшение BI-LSTM по сравнению с LSTM во всех случаях: 2.2, 5.9 и 4.4 %, соответственно.

На рисунках 5–7 показаны результаты прогнозирования для различных размеров партии Batch Size в BI-LSTM и LSTM-моделях: кривые (слева) представляет собой вероятности ошибки предсказания скорости трафика, а гистограммы (справа) – вероятности потери с течением времени (в секундах).

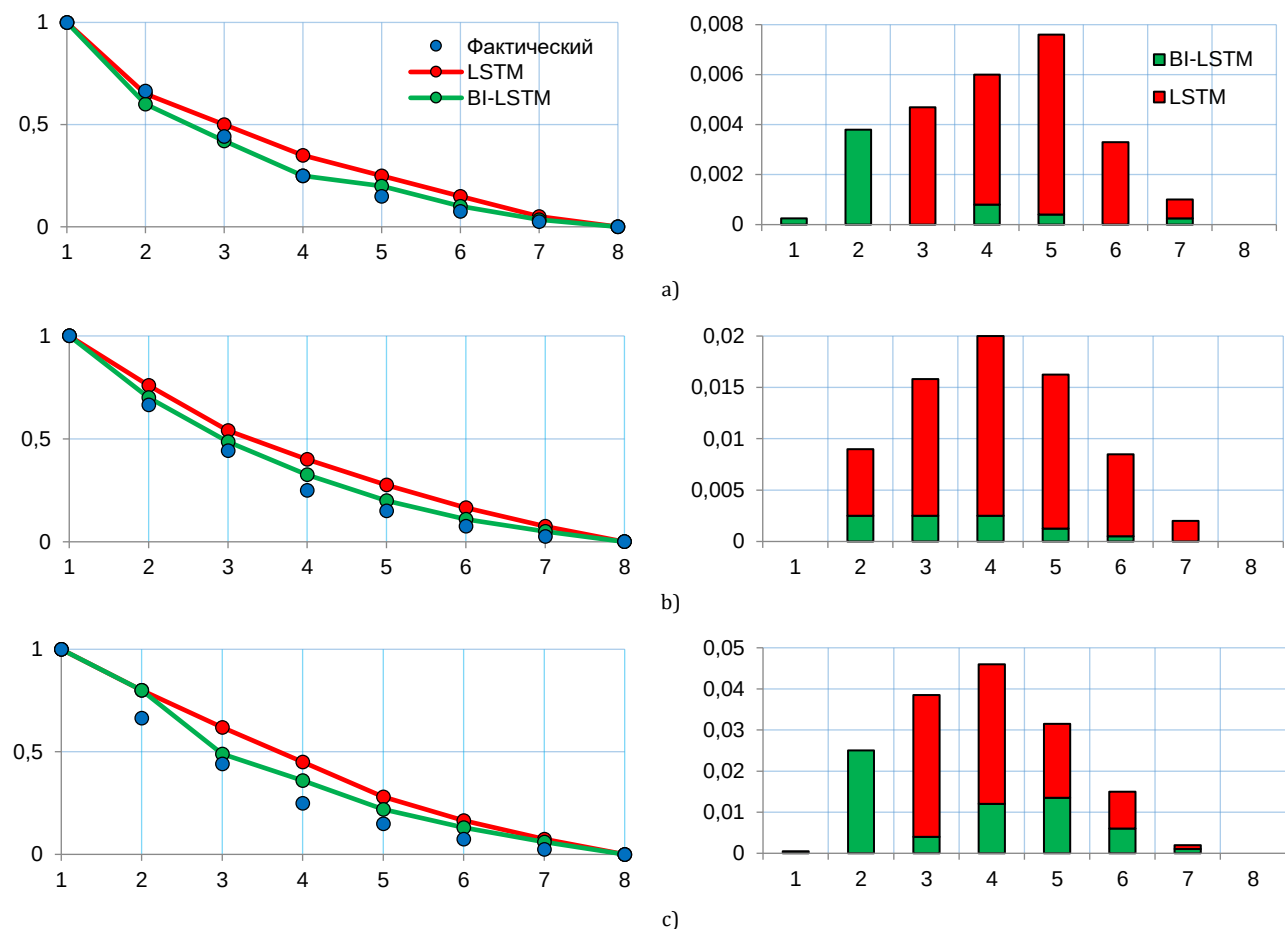


Рис. 5. Прогнозирование выходных паттернов в случае использования BatchSize, равной: а) 8, б) 16 и в) 64

Fig. 5. Prediction of Output Patterns in Case of Using a) 8, b) 16 and c) 64 Batch Size

Модели прогнозирования BI-LSTM и LSTM для случаев, когда используются BatchSizes = 8, 16 и 64, как показывают кривые слева, дают примерно одинаковый результат: вероятности ошибки предсказания скорости трафика постепенно уменьшаются со временем, что достаточно похоже на реально наблюдаемый процесс (на графиках – «Фактический»). Гистограммы справа показывают, что модель на основе BI-LSTM имеет наименьшие потери со временем во всех случаях по сравнению с моделью на основе LSTM, а наибольшие потери составляют 5, 4 и 4 сек. при использовании BatchSizes = 8, 16 и 64, соответственно.

Заключение

В данной статье предлагаются методы DL для прогнозирования трафика в автономных транспортных средствах с многоуровневыми облачными вычислениями. DL был обучен на примере среды VANET, используя BI-LSTM и LSTM сети для различных размеров партии, чтобы исследовать модель прогнозирования, которая обеспечивает парадигмальную точность, а также максимальное среднее улучшение. Точность прогнозирования рассчитана с использованием среднеквадратичной ошибки, средней абсолютной процентной ошибки, коэффициента детерминации R^2 и времени обработки.

Результаты моделирования точности прогнозирования показывают, что BI-LSTM превосходит LSTM во всех случаях. Для BatchSize = 64 точность прогнозирования низкая по сравнению с другими, а при BatchSize = 8 – превосходит конкурентов. Коэффициент детерминации R^2 примерно одинаков в обоих случаях и близок к 1, что означает, что сеть хорошо обучена. При использовании среды VANET время обработки при BatchSize = 64 самое короткое, а при BatchSize = 8 – самое длительное в сравнении с другими.

Полученные результаты исследования, без потери общности, позволяют масштабировать прогнозные модели для систем облачных и туманных вычислений в системе VANETs [21], которые обеспечивают значительные вычислительные возможности за счет DL на границах сети для различного количества облаков, в том числе, в условиях мигрирующего тумана.

Кроме этого, использования данного подхода позволяют перейти к решению оптимизационных задач при взаимодействиях граничных устройств VANETs [22] с учетом ограничений полученных прогнозных моделей.

Указанные вопросы определяют будущее направления исследований по данной работе.

Список источников

1. Abdellah A.R., Alshahrani A., Muthanna A., Koucheryavy A. Performance Estimation in V2X Networks Using Deep Learning-Based M-Estimator Loss Functions in the Presence of Outliers // *Symmetry*. 2021. Vol. 13. Iss. 11. P. 2207. DOI:10.3390/sym13112207.
2. Chochliouros I.P., Spiliopoulou A.S., Lazaridis P., Dardamanis A., Zaharis Z., Kostopoulos A. Dynamic Network Slicing: Challenges and Opportunities // *Proceedings of the International Conference on Artificial Intelligence Applications and Innovations (AIAI 2020, Neos Marmaras, Greece, 5–7 June 2020)*. IFIP WG 12.5 International Workshops. IFIP Advances in Information and Communication Technology. Vol. 585. Cham: Springer, 2020. DOI:10.1007/978-3-030-49190-1_5
3. Miglani A., Kumar N. Deep learning models for traffic flow prediction in autonomous vehicles: A review, solutions, and challenges // *Vehicular Communications*. 2019. Vol. 20. P. 100184. DOI:10.1016/j.vehcom.2019.100184
4. Gillani M., Niaz H.A., Farooq M.U., Ullah A. Data collection protocols for VANETs: a survey // *Complex & Intelligent Systems*. 2022. Vol. 8. Iss. 3. PP. 2593–2622. DOI:10.1007/s40747-021-00629-x
5. Grigorescu S., Trasnea B., Cocias T., Macesanu G. A survey of deep learning techniques for autonomous driving // *Journal of Field Robotics*. 2020. Vol. 37. Iss. 3. PP. 362–386. DOI:10.1002/rob.21918
6. Pfülb B., Hardegen C., Gepperth A., Rieger S. A Study of Deep Learning for Network Traffic Data Forecasting // *Proceedings of the 28th International Conference on Artificial Neural Networks and Machine Learning (ICANN 2019, Munich, Germany, 17–19 September 2019)*. Lecture Notes in Computer Science. Vol. 11730. Cham: Springer, 2019. PP. 497–512. DOI:10.1007/978-3-030-30490-4_40
7. Ateeq M., Ishmanov F., Afzal M.K., Naeem M. Predicting Delay in IoT Using Deep Learning: A Multiparametric Approach // *IEEE Access*. 2019. Vol. 7. PP. 62022–62032. DOI:10.1109/ACCESS.2019.2915958
8. Abdellah A.R., Koucheryavy A. Deep Learning with Long Short-Term Memory for IoT Traffic Prediction // *Proceedings of the 20th International Conference on Next Generation Networks and Systems, NEW2AN 2020, and 13th Conference on Internet of Things, Smart Spaces, ruSMART 2020 (St. Petersburg, Russia, 26–28 August 2020)*. Lecture Notes in Computer Science. Vol. 12525. Cham: Springer, 2020. PP. 267–280. DOI:10.1007/978-3-030-65726-0_24
9. Almutairi M.S. Deep Learning-Based Solutions for 5G Network and 5G-Enabled Internet of Vehicles: Advances, Meta-Data Analysis, and Future Direction // *Mathematical Problems in Engineering*. 2022. Vol. 2022. P. 6855435. DOI:10.1155/2022/6855435
10. Kaur J., Khan M.A., Iftikhar M., Imran M., Haq Q.E.U. Machine Learning Techniques for 5G and Beyond // *IEEE Access*. 2021. Vol. 9. PP. 23472–23488. DOI:10.1109/ACCESS.2021.3051557
11. Abdellah A.R., Volkov A., Muthanna A., Gallyamov D., Koucheryavy A. Deep Learning for IoT Traffic Prediction Based on Edge Computing // *Proceedings of the 23rd International Conference on Distributed Computer and Communication Networks: Control, Computation, Communications (DCCN 2020, Moscow, Russia, 14–18 September 2020)*. Com-

munications in Computer and Information Science. Vol. 1337. PP. 18–29. Cham: Springer, 2020. DOI:10.1007/978-3-030-66242-4_2

12. Khedkar S.P., Canessane R.A., Najafi M.L. Prediction of Traffic Generated by IoT Devices Using Statistical Learning Time Series Algorithms // *Wireless Communications and Mobile Computing*. 2021. Vol. 2021. P. 5366222. DOI:10.1155/2021/5366222

13. Selvamanju E., Shalini V.B. Machine Learning Based Mobile Data Traffic Prediction in 5G Cellular Networks // *Proceedings of the 5th International Conference on Electronics, Communication and Aerospace Technology (ICECA, Coimbatore, India, 02–04 December 2021)*. IEEE, 2021. PP. 1318–1324. DOI:10.1109/ICECA52323.2021.9675887

14. Choi D., Yim J., Baek M., Lee S. Machine Learning-Based Vehicle Trajectory Prediction Using V2V Communications and On-Board Sensors // *Electronics*. 2021. Vol. 10. Iss. 4. P. 420. DOI:10.3390/electronics10040420

15. Rasouli A., Tsotsos J.K. Autonomous Vehicles That Interact With Pedestrians: A Survey of Theory and Practice // *IEEE Transactions on Intelligent Transportation Systems*. 2020. Vol. 21. Iss. 3. PP. 900–918. DOI:10.1109/TITS.2019.2901817

16. 19.Badicu A., Suci G., Balanescu M., Dobrea M., Birdici A., Orza O., Pasat A. PMs concentration forecasting using ARIMA algorithm // *Proceedings of the 91-st Vehicular Technology Conference (VTC2020-Spring, Antwerp, Belgium, 25–28 May 2020)*. IEEE, 2020. DOI:10.1109/VTC2020-Spring48590.2020.9129390

17. Shang Q., Tan D., Gao S., Feng L. A Hybrid Method for Traffic Incident Duration Prediction Using BOA-Optimized Random Forest Combined with Neighborhood Components Analysis // *Journal of Advanced Transportation*. 2019. Vol. 2019. P. 4202735. DOI:10.1155/2019/4202735

18. Кучерявый А.Е. Сети связи с ультрамалыми задержками // *Труды научно-исследовательского института радио*. 2019. № 1. С. 69–74.

19. Мутханна А.С. Интеллектуальная распределенная архитектура сети связи для поддержки беспилотных автомобилей // *Электросвязь*. 2020. № 7. С. 29–34. DOI:10.34832/ELSV.2020.8.7.004

20. Владыко А.Г., Мутханна А.С., Кучерявый А.Е. Метод выгрузки трафика в V2X/5G сетях на основе системы граничных вычислений // *Электросвязь*. 2020. № 8. С. 24–30. DOI:10.34832/ELSV.2020.9.8.004

21. Shrestha R., Bajracharya R., Nam S.Y. Challenges of Future VANET and Cloud-Based Approaches // *Wireless Communications and Mobile Computing*. 2018. Vol. 2018. P. 5603518. DOI:10.1155/2018/5603518

22. Плотников П.В., Владыко А.Г. Минимизация задержек при взаимодействии граничных устройств с использованием кластеризации в сетях VANETs // *Труды учебных заведений связи*. 2022. Т. 8. № 2. С. 6–13. DOI:10.31854/1813-324X-2022-8-2-6-13

References

1. Abdellah A.R., Alshahrani A., Muthanna A., Koucheryavy A. Performance Estimation in V2X Networks Using Deep Learning-Based M-Estimator Loss Functions in the Presence of Outliers. *Symmetry*. 2021;13(11);2207. DOI:10.3390/sym13112207

2. Chochliouros I.P., Spiliopoulou A.S., Lazaridis P., Dardamanis A., Zaharis Z., Kostopoulos A. Dynamic Network Slicing: Challenges and Opportunities. *Proceedings of the International Conference on Artificial Intelligence Applications and Innovations, AIAI 2020, 5–7 June 2020, Neos Marmaras, Greece. IFIP WG 12.5 International Workshops. IFIP Advances in Information and Communication Technology*, vol.585. Cham: Springer; 2020. DOI:10.1007/978-3-030-49190-1_5

3. Miglani A., Kumar N. Deep learning models for traffic flow prediction in autonomous vehicles: A review, solutions, and challenges. *Vehicular Communications*. 2019;20:100184. DOI:10.1016/j.vehcom.2019.100184

4. Gillani M., Niaz H.A., Farooq M.U., Ullah A. Data collection protocols for VANETs: a survey. *Complex & Intelligent Systems*. 2022;8(3):2593–2622. DOI:10.1007/s40747-021-00629-x

5. Grigorescu S., Trasnea B., Cocias T., Macesanu G. A survey of deep learning techniques for autonomous driving. *Journal of Field Robotics*. 2020;37(3):362–386. DOI:10.1002/rob.21918

6. Pfülb B., Hardegen C., Gepperth A., Rieger S. A Study of Deep Learning for Network Traffic Data Forecasting. *Proceedings of the 28th International Conference on Artificial Neural Networks and Machine Learning, ICANN 2019, 17–19 September 2019, Munich, Germany. Lecture Notes in Computer Science*, vol.11730. Cham: Springer; 2019. p.497–512. DOI:10.1007/978-3-030-30490-4_40

7. Ateeq M., Ishmanov F., Afzal M.K., Naeem M. Predicting Delay in IoT Using Deep Learning: A Multiparametric Approach. *IEEE Access*. 2019;7:62022–62032. DOI:10.1109/ACCESS.2019.2915958

8. Abdellah A.R., Koucheryavy A. Deep Learning with Long Short-Term Memory for IoT Traffic Prediction. *Proceedings of the 20th International Conference on Next Generation Networks and Systems, NEW2AN 2020, and 13th Conference on Internet of Things, Smart Spaces, ruSMART 2020, 26–28 August 2020, St. Petersburg, Russia. Lecture Notes in Computer Science*, vol.12525. Cham: Springer; 2020. p.267–280. DOI:10.1007/978-3-030-65726-0_24

9. Almutairi M.S. Deep Learning-Based Solutions for 5G Network and 5G-Enabled Internet of Vehicles: Advances, Meta-Data Analysis, and Future Direction. *Mathematical Problems in Engineering*. 2022;2022:6855435. DOI:10.1155/2022/6855435

10. Kaur J., Khan M.A., Iftikhar M., Imran M., Haq Q.E.U. Machine Learning Techniques for 5G and Beyond. *IEEE Access*. 2021;9:23472–23488. DOI:10.1109/ACCESS.2021.3051557

11. Abdellah A.R., Volkov A., Muthanna A., Gallyamov D., Koucheryavy A. Deep Learning for IoT Traffic Prediction Based on Edge Computing. *Proceedings of the 23rd International Conference on Distributed Computer and Communication Networks: Control, Computation, Communications, DCCN 2020, 14–18 September 2020, Moscow, Russia. Communications in Computer and Information Science*, vol.1337. p.18–29. Cham: Springer, 2020. DOI:10.1007/978-3-030-66242-4_2

12. Khedkar S.P., Canessane R.A., Najafi M.L. Prediction of Traffic Generated by IoT Devices Using Statistical Learning Time Series Algorithms. *Wireless Communications and Mobile Computing*. 2021;2021:5366222. DOI:10.1155/2021/5366222

13. Selvamamju E., Shalini V.B. Machine Learning Based Mobile Data Traffic Prediction in 5G Cellular Networks. *Proceedings of the 5th International Conference on Electronics, Communication and Aerospace Technology, ICECA, 02–04 December 2021, Coimbatore, India*. IEEE; 2021. p.1318–1324. DOI:10.1109/ICECA52323.2021.9675887
14. Choi D., Yim J., Baek M., Lee S. Machine Learning-Based Vehicle Trajectory Prediction Using V2V Communications and On-Board Sensors. *Electronics*. 2021;10(4):420. DOI:10.3390/electronics10040420
15. Rasouli A., Tsotsos J.K. Autonomous Vehicles That Interact With Pedestrians: A Survey of Theory and Practice. *IEEE Transactions on Intelligent Transportation Systems*. 2020;21(3):900–918. DOI:10.1109/TITS.2019.2901817
16. Badicu A., Suciu G., Balanescu M., Dobrea M., Birdici A., Orza O., Pasat A. PMs concentration forecasting using ARIMA algorithm. *Proceedings of the 91-st Vehicular Technology Conference, VTC2020-Spring, 25–28 May 2020, Antwerp, Belgium*. IEEE; 2020. DOI:10.1109/VTC2020-Spring48590.2020.9129390
17. Shang Q., Tan D., Gao S., Feng L. A Hybrid Method for Traffic Incident Duration Prediction Using BOA-Optimized Random Forest Combined with Neighborhood Components Analysis. *Journal of Advanced Transportation*. 2019;2019:4202735. DOI:10.1155/2019/4202735
18. Kucheryavy A. Network Delay Communications Networks. *Trudy NIIR*. 2019;1:69–74. (in Russ.)
19. Muthanna A.S. Distributed Intelligent Communication Network Architecture for Unmanned Vehicles. *Electrosvyaz*. 2020;7:29–34. (in Russ.) DOI: 10.34 832/ELSV.2020.8.7.004
20. Vladyko A.G., Muthanna A.S., Koucheryavy A.Eu. Traffic Offloading Method for V2X/5G Networks Based on the Edge Computing System. *Electrosvyaz*. 2020;8:24–30. (in Russ.) DOI: 10.34 832/ELSV.2020.9.8.004
22. Shrestha R., Bajracharya R., Nam S.Y. Challenges of Future VANET and Cloud-Based Approaches. *Wireless Communications and Mobile Computing*. 2018;2018:5603518. DOI:10.1155/2018/5603518
23. Plotnikov P., Vladyko A. Minimizing Delays in the Interaction of Edge Devices Using Clustering in VANETs. *Proceedings of Telecommunication Universities*. 2022;8(2):6–13. (in Russ.) DOI:10.31854/1813-324X-2022-8-2-6-13

Статья поступила в редакцию 24.11.2022; одобрена после рецензирования 20.12.2022; принята к публикации 21.12.2022.

The article was submitted 24.11.2022; approved after reviewing 20.12.2022; accepted for publication 21.12.2022.

Информация об авторе:

**АЛЬ-СВЕЙТИ
Малик**

аспирант кафедры сети связи и передачи данных Санкт-Петербургского государственного университета телекоммуникаций им. проф. М.А. Бонч-Бруевича
 <https://orcid.org/0000-0002-6267-4727>

Научная статья

УДК 621.396

DOI:10.31854/1813-324X-2022-8-4-100-108



Исследование корреляционных свойств сигналообразующих последовательностей в целях оптимизации характеристик канала случайного доступа 5G NR

Иван Андреевич Бабанов, ivan.babanov@gmail.com

Санкт-Петербургский государственный университет телекоммуникаций им. М.А. Бонч-Бруевича,
Санкт-Петербург, 193232, Российская Федерация

Аннотация: В статье исследованы корреляционные свойства сигналообразующих последовательностей, которые могут быть положены в основу методики оптимизации канала случайного доступа. Идея основана на выборе корней для построения преамбул случайного доступа, вероятность детектирования которых выше, чем выбранных классическим способом корней. Приводятся результаты имитационного моделирования на всем множестве преамбул длиной 839 отсчетов. Показано, что с ростом количества одновременно передаваемых преамбул возрастает разброс возможных значений коэффициента корреляции, что прямо влияет на успешность детектирования. Сделан вывод о возможности оптимизации характеристик канала случайного доступа, как с точки зрения конфигурации его ресурсов, так и рационального выбора корней сигналообразующих преамбул.

Ключевые слова: 5G NR, LTE, параметры радиоканала, преамбула случайного доступа

Ссылка для цитирования: Бабанов И.А. Исследование корреляционных свойств сигналообразующих последовательностей в целях оптимизации характеристик канала случайного доступа 5G NR // Труды учебных заведений связи. 2022. Т. 8. № 4. С. 100–108. DOI:10.31854/1813-324X-2022-8-4-100-108

Correlation Properties Investigation of Signaling Sequences to Optimize the 5G NR Random Access Channel Characteristics

Ivan Babanov, ivan.babanov@gmail.com

The Bonch-Bruevich Saint-Petersburg State University of Telecommunications,
St. Petersburg, 193232, Russian Federation

Abstract: The article describes a random access channel optimization technique based on the choice of roots for constructing random access preambles, the detection probability of which is higher than the roots selected in the classical way according. The results of simulation modeling are presented for the entire set of preambles 839 samples long. It is shown that with an increase in the number of simultaneously transmitted preambles, the spread of possible values of the correlation coefficient increases, which directly affects the success of detection. The conclusion is made about the possibility of optimizing the characteristics of the random access channel, both in terms of the configuration of the random access channel resources and based on the rational choice of the roots of the signal-forming preambles.

Keywords: 5G NR, LTE, radio signal parameters, mobile network

For citation: Babanov I. Correlation Properties Investigation of Signaling Sequences to Optimize the 5G NR Random Access Channel Characteristics. *Proc. of Telecom. Universities*. 2022;8(4):100–108. (in Russ.) DOI:10.31854/1813-324X-2022-8-4-100-108

1. Введение

Современный стандарт мобильной связи 5G NR [1] является эволюционным развитием предыдущего стандарта сетей 4-го поколения LTE [1] и во многом переиспользует структуру физических радиоканалов, имеющуюся в LTE и более ранних технологиях. Новый стандарт призван улучшить сети 4-го поколения в части пропускной способности и гибкости настройки радиоканалов. Развитие осуществляется по трем направлениям: широкополосная мобильная связь MBW (*аббр. от англ. Mobile Broadband*), сверхнадежная межмашинная связь с низкими задержками URLLC (*аббр. от англ. Ultra-Reliable Low Latency Communications*) и массивный межмашинный обмен mMTC (*аббр. от англ. Massive Machine-Type Communications*) [1].

Планируется, что с точки зрения MBW стандарт позволит обеспечить скорости до 1 Gb и выше. Направление URLLC должно открыть возможности по управлению техническими системами, критическими к задержке, которая должна составлять ≤ 1 мс. Третье направление – mMTC, ориентировано на возможность работы огромного количества беспроводных устройств Интернета вещей.

Проблема оптимизации параметров канала случайного доступа встает все острее с каждым последующим поколением систем мобильной связи. В первую очередь это вызвано постоянно ожесточающимися временными характеристиками новых сервисов. Если стандарт 3G предполагал в основном только широкополосный доступ для базовых приложений, то в стандарте 4-го поколения уже специфицирована дополнительная функциональность под названием «быстрое планирование TTI» (*аббр. от англ. Short TTI Scheduling*) [2]. Данный метод предполагает уменьшение времени получения ответа от сети до 2 мс по сравнению с базовым значением ~ 20 мс в «классическом» варианте развертывания LTE. В стандарте 5-го поколения сверхбыстрые коммуникации уже являются обязательной частью системы, что актуализирует задачи уменьшения задержек.

Целью исследования является оптимизация настройки параметров физического канала случайного доступа (PRACH, *аббр. от англ. Physical Random Access Channel*). Предлагаемая методика позволит улучшить характеристики производительности канала PRACH, что, в свою очередь, должно благоприятно отразиться на показателях качества обслуживания (*от англ. Quality Of Service*) всей системы. Основным показателем качества в данном канале является время установления соединения с сетью и, как следствие этого, время, потраченное пользователем на доступ к сервису сети.

Данный показатель не является критичным в случае использования широкополосного доступа, но с внедрением новых сервисов, таких как ультранадежная передача со сверхнизкими задержками, данный показатель становится критичным. Также в случае внедрения массового межмашинного обмена показатель времени доступа к сервису также становится важным параметром, но уже с точки зрения переповторов процедуры, с учетом ограниченного энергетического ресурса мобильной станции. Так как принципы организации канала случайного доступа не изменились при переходе от LTE к 5G NR, то предложенная методика является применимой для обеих технологий.

PRACH-канал предназначен для передачи первого сообщения между UE (*аббр. от англ. User Equipment*) и eNB/gNB; в дальнейшем будем использовать термины базовая станция (БС) и мобильная станция (МС). Как указывалось выше, принцип взаимодействия между МС и БС по PRACH-каналу при переходе к 5G NR не изменился и заключается в отсылке специального сигнала, называемого преамбулой случайного доступа. PRACH-канал является однонаправленным и предназначен исключительно для передачи преамбулы от МС к БС.

Несмотря на то, что организация канала случайного доступа для систем 5G NR не изменилась по сравнению со стандартом LTE, в стандарте 5G NR возможности конфигурации канала были сильно расширены. Если для LTE предполагались только 2 варианта длины ZC-последовательностей в 837 и 139 символов, то для стандарта 5G NR введены дополнительные наборы длин последовательностей в 1151 и 571 символ. Также изменилось количество возможных форматов преамбулы. В LTE было определено 4 формата для FDD (*аббр. от англ. Feature Driven Development*, методология разработки программного обеспечения, принимающего за основу функциональность) и один формат для TDD (*аббр. от англ. Test-Driven Development*, техника разработки через тестирование). В стандарте они называются конфигурации 0-3 и конфигурация 4, соответственно. Для FDD преамбула могла занимать от одного до трех сабфреймов. В новом стандарте 5G NR сохранены конфигурации, использовавшиеся в FDD LTE. Вместо конфигурации 4 для преамбул на основе ZC-последовательности длиной 139 символов определено 9 возможных конфигураций преамбулы названных, соответственно, A1-A3, B1-B4 и C0, C2. Такие же конфигурации используются для ZC-последовательностей длиной 1151 и 571 элемент. Таким образом, количество возможных конфигураций преамбулы увеличилось с 5 до 31.

Конфигурация, используемая в PRACH-канале, заранее известна МС путем считывания системной информации, осуществляемой после сканирования эфира. Таким образом, набор преамбул становится известен как МС, так и БС. Поэтому при приеме радиосигнала PRACH-канала БС пытается в принятом сигнале обнаружить одну или несколько сконфигурированных преамбул. С точки зрения организации обмена сообщениями передаваемую преамбулу обычно называют RA (аббр. от англ. Random Access), а ответом на нее является сообщение RAR (аббр. от англ. Random Access Response), передаваемое по каналу PDCCH. В случае успешного обнаружения RA БС может определить удаленность МС и корректно выставить упреждение по времени и передать RAR по нисходящему каналу. Один из возможных сценариев случайного доступа приведен на рисунке 1.

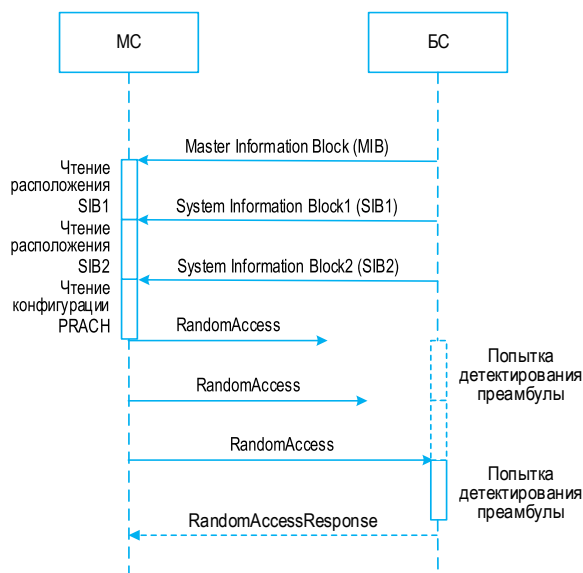


Рис. 1. Процедура случайного доступа

Fig. 1. Random Access Procedure

Как видно из рисунка 1, детектирование преамбулы происходит постоянно, но его успешность зависит от многих факторов. В первую очередь это мощность, с которой МС отправляет преамбулу. Начальное значение мощности и шаг ее увеличения передается в системной информации и известен МС до начала процедуры случайного доступа. Кроме этих двух параметров, определяется количество попыток, которые должна сделать МС, а также время ожидания между неуспешными попытками.

2. Генерация и детектирование преамбул

Для выполнения процедур случайного доступа и процедур переключения между БС мобильная станция должна сгенерировать 64 преамбулы [3]. Процедура генерации преамбулы циклична и выполняется в соответствии с параметрами, передаваемыми в системном информационном блоке БС (SIB, аббр. от англ. System Information Block).

RA сообщение, передаваемое по PRACH-каналу, состоит из одной или нескольких ZC-последовательностей в зависимости от используемой конфигурации канала случайного доступа. В начало сообщения добавляется циклический префикс (от англ. Cyclic Prefix) и завершается сообщение так называемым защитным интервалом (от англ. Guard Period).

Генерация ZC-последовательности осуществляется по формуле:

$$x_u(i) = e^{-j\frac{2\pi u i(i+1)}{L_{RA}}}, i = 0, 1, \dots, L_{RA}-1, \quad (1)$$

где L_{RA} – это длина ZC-последовательности; специфицированные длины последовательностей для стандартов LTE и 5G NR приведены в [3].

Для построения всех 64-х преамбул используется циклический сдвиг (ЦС) исходной ZC-последовательности. Величина сдвига – это один из параметров конфигурации канала RACH и зависит от размера обслуживаемого сектора: чем больше радиус сектора, тем значение ЦС между преамбулами, образованными от одного корня, должно быть больше. Это связано с тем, что во временной области при декодировании сигнала временная задержка при приеме представляет из себя как раз ЦС исходного сигнала. Таким образом, чтобы БС могла отличить преамбулу $P(N)$ от физически далеко расположенной МС от преамбулы $P(N+1)$ от МС, расположенной ближе, необходимо выбирать значение параметра ZeroCorrelationZoneConfig с ЦС больше, чем максимально возможное, привнесенное временной задержкой от максимально удаленной МС. Значения сдвига приведены в [3].

Таким образом, количество преамбул N , которое можно построить из образованной от одного корня ZC-последовательности, можно определить как:

$$N = \frac{L_{RA}}{N_{CS}}. \quad (2)$$

В случае, $N < 64$, и из одной ZC-последовательности нельзя построить все необходимые 64 преамбулы, то для построения недостающих преамбул используется ZC-последовательность, образованная от следующего корня, который выбирается в соответствии с таблицами 5.7.2–4, 6.3.3.1–3 [3, 4]. Кроме того, для успешного построения всех 64-х последовательностей в стандартах LTE и 5G NR определена величина ZeroCorrelationZoneConfig, которая также приведена в соответствующих таблицах в [3, 4] и определяет величину ЦС между соседними преамбулами, образованными от одного корня.

Для детектирования преамбулы на стороне БС выполняется операция по построению всех 64-х сконфигурированных преамбул. Стандартом 3GPP определен только передатчик, а конечная реализация приемника остается на усмотрение производи-

теля. Как правило, основным способом определения наличия заданной преамбулы в принятом сигнале является вычисление корреляции между принятым сигналом и искомой последовательностью.

Для вычисления коэффициента корреляции можно воспользоваться формулой Пирсона:

$$r_{XY} = \frac{\sum (X_i - \bar{X})(Y_i - \bar{Y})}{\sqrt{\sum (X_i - \bar{X})^2 \sum (Y_i - \bar{Y})^2}}. \quad (3)$$

При детектировании преамбулы следует учитывать, что на стороне БС заранее не известно удаление МС, а также возможный ЦС, вызванный временной задержкой при приеме сигнала.

Таким образом, количество преамбул, для которых надо вычислить корреляцию, можно определить по формуле:

$$N_{corr} = N_{RA}(N_{CS} - 1). \quad (4)$$

Вид корреляционной функции при детектировании преамбулы с используемым ЦС 4 приведен на рисунке 2.

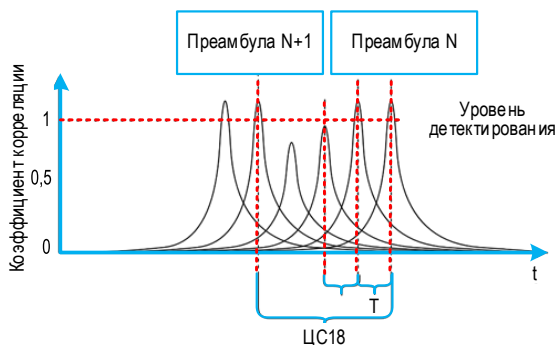


Рис. 2. Детектирование преамбулы с учетом временного сдвига

Fig. 2. Preamble Detection with Time Shift

Канал случайного доступа в системах мобильной связи спроектирован с возможностью одновременного выполнения процедуры несколькими устройствами. Данная возможность обеспечивается свойством CAZAC (аббр. от англ. Constant Amplitude Zero Autocorrelation) ZC-последовательностей. На рисунке 3 приведен вид ZC-последовательности на комплексной плоскости. Для примера используется последовательность длиной в 151 элемент.

Пусть существуют R_i передаваемых преамбул для $i \in [0, 1...63]$ и такой же набор преамбул D_j на стороне БС, которые она будет пытаться обнаружить в принятом сигнале. Тогда свойство CAZAC обеспечивает истинность формулы:

$$\sum_{i=0}^{63} \sum_{j=0}^{63} r(R_i, D_j) = 1 \quad \text{только для } j = i, \quad (5)$$

где R – одна из 64-х преамбул, передаваемая МС; D – одна из 64-х преамбул, которую БС пытается детек-

тировать; при этом наборы R и D состоят из одинаковых преамбул, а преамбула R_{i+1} получена путем ЦС преамбулы R_i .

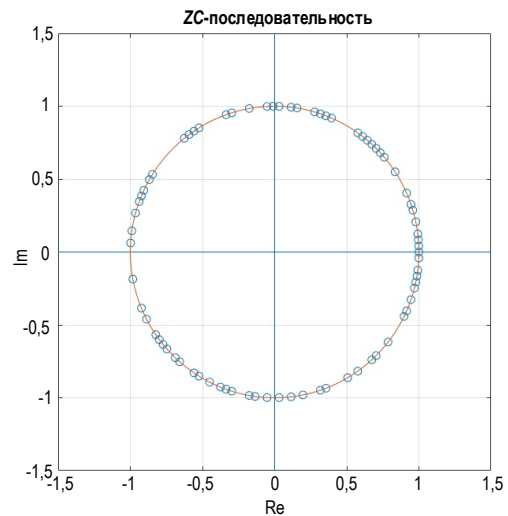


Рис. 3. Пример ZC-последовательности на комплексной плоскости

Fig. 3. ZC-Sequence Example on Complex Plane

То есть, при передаче одной ZC-последовательности $r(R_i, D_i) = 1$, а $r(R_i, D_{i-1}) = 0$, и аналогично для всех других i .

3. Пути оптимизации PRACH-канала

В научной литературе неоднократно рассматривались пути оптимизации и улучшения характеристики канала случайного доступа. Вот некоторые из них.

Во-первых, случайный доступ с ранним обнаружением коллизий. В [5] предлагается схема раннего обнаружения коллизий на первом шаге процедуры случайного доступа. Рекомендуется к использованию специальные преамбулы, которые состоят из тагированной особым образом ZC-последовательности с применением различных корневых чисел, соответственно. Предложенная схема позволяет быстрее, по сравнению с классической схемой процедуры случайного доступа, определять наличие коллизии и разрешать ее.

Во-вторых, увеличение пропускной способности канала случайного доступа. В [6] приводится детальное изучение возможностей приоритизации через разделение множества преамбул на неперекрывающиеся классы. Иначе говоря, предлагается, чтобы МС с различными потребностями с точки зрения временных характеристик использовали разные множества преамбул, благодаря чему БС сможет приоритизировать обслуживание наиболее важных устройств и тем самым улучшить характеристики канала случайного доступа для них.

В-третьих, уменьшение задержки в канале случайного доступа. В [7] описан метод самоорганизации со стороны БС в зависимости от нагрузки на

сеть. Предполагается, что БС сможет изменять настройки канала случайного доступа и при необходимости выделять под него больше ресурсов и уменьшать их количество в случае малой нагрузки на канал.

В-четвертых, исследование детектирования перегрузки канала случайного доступа приведено в [8]. Предложены методики детектирования для сценариев использования в рамках развертывания M2M сервисов.

В-пятых, методы организации гибридной процедуры случайного доступа приведены в [9, 10], где делается предположение, что в сценариях M2M организованный классически канал случайного доступа может быть перегружен. Предлагается гибридная процедура случайного доступа и приводятся обоснования, почему ее использование решает данную проблему.

В-шестых, использование канала случайного доступа для передачи информации на раннем этапе подключения. В [11] предлагается использовать канал случайного доступа для передачи информации вместе с преамбулой. Такие сценарии в основном ориентированы на M2M-сегмент устройств и подразумевают, что им нет необходимости выполнять полную процедуру подключения к сети, если объем данных невелик и может быть передан в рамках процедуры случайного доступа. Приводятся примеры, что это позволяет существенно снизить нагрузку на сеть, особенно в сценариях развертывания сетей 5-го поколения.

Также в [12] было проведено сравнительное исследование корреляционных свойств ZC-последовательностей и показана неоднородность взаимной корреляции преамбул, образованных от разных корней.

ТАБЛИЦА 1. Значения коэффициентов корреляции и ΔКК в зависимости от используемых корневых последовательностей

TABLE 1: Values of Correlation Coefficients and its Delta Depending on the Used Sequence Roots

ЦС	КК-1	ΔКК-1	КК-4	ΔКК-4	КК-16	ΔКК-16	КК-32	ΔКК-32	КК-56	ΔКК-56
15	1	0	0,4991	0	0,2478	0	0,1735	0	0,1700	0,0903
18	1	0	0,4991	0	0,2478	0	0,1735	0	0,1749	0,0910
22	1	0	0,4991	0	0,2478	0	0,1735	0	0,1644	0,0606
26	1	0	0,4991	0	0,2478	0	0,1735	0	0,1661	0,0452
32	1	0	0,4991	0	0,2478	0	0,2150	0,0872	0,1773	0,0794
38	1	0	0,4991	0	0,2478	0	0,2194	0,0787	0,1752	0,0677
46	1	0	0,4991	0	0,2478	0	0,2119	0,0288	0,1679	0,0636
59	1	0	0,4991	0	0,2822	0,0695	0,2145	0,0707	0,1792	0,0540
76	1	0	0,4991	0	0,2828	0,0563	0,2161	0,0559	0,1778	0,0846
93	1	0	0,4991	0	0,2835	0,0201	0,2251	0,0788	0,1787	0,0889
119	1	0	0,4991	0	0,2923	0,0694	0,2178	0,0784	0,1782	0,0832
167	1	0	0,4991	0	0,2918	0,0549	0,2182	0,0798	0,1739	0,0881
279	1	0	0,5211	0,0349	0,2898	0,0625	0,2200	0,0838	0,1706	0,1026
19	1	0	0,5164	0	0,2913	0,0427	0,2153	0,0729	0,1664	0,0899

В реальной сети часто возможна ситуация, когда несколько мобильных устройств отсылают преамбулу одновременно. Такое возможно, к примеру, на выходе из туннеля, когда абонентские терминалы почти одновременно обнаруживают наличие сети и пытаются выполнить подключение. В сценариях внедрения МТС подобная ситуация может сложиться, когда большое количество беспроводных датчиков, работая синхронно, будут так же осуществлять попытки передачи данных в одно время.

В таком случае совершенно логичным выглядит требование константной корреляции для любой из 837 конфигураций корневой последовательности для любой из 64-х построенных преамбул. Очевидно, что в случае передачи лишь одной преамбулы, на значение коэффициента корреляции (КК) будет влиять лишь уровень шума в радиоканале, а в случае идеального радиоканала и отсутствия шума этот коэффициент составит 1.

4. Исследование корреляционных свойств базовых последовательностей преамбул случайного доступа

Для исследования постоянства КК был проведен имитационный эксперимент в MATLAB с суммированием нескольких преамбул и его вычисления для каждой из них. Таким образом эмулировалась одновременная передача преамбулы несколькими абонентскими терминалами. Результаты приведены в таблице 1. Из таблицы видно, что, как и ожидалось, КК для единичной передачи составляет 1. В случае увеличения количества передаваемых одновременно преамбул КК уменьшается, но для передачи четырех преамбул он остается практически постоянным.

В дальнейшем с ростом числа передаваемых одновременно преамбул КК становится не статичным, о чем говорит ненулевое значение дельты, представленное в соответствующем столбце. Под дельтой подразумевается разность между наибольшим и наименьшим значением КК, вычисленного для заданного количества одновременно передаваемых преамбул и величины ЦС. В таблице 1 приведены значения КК для каждого из возможных ЦС и для 4-х вариантов количества одновременно передаваемых преамбул. Также для каждой из конфигураций указано значение дельты коэффициента корреляции ($\Delta\text{КК}$). В этом случае $\Delta\text{КК}-N$ означает, что в столбце приведена разница между наименьшим и наибольшим значениями КК для N -одновременно передаваемых преамбул.

Следует отметить, что ожидаемое требование постоянной корреляции оказывается на практике недостижимо из-за свойств каналообразующей последовательности. Как видно из приведенных данных, существуют множества значений величины ЦС, в рамках которых значение КК константно, но эти области не покрывают ни множество возможных ЦС, ни одновременно передаваемых преамбул, даже с учетом их количества в реальной сети менее 64.

В данном расчете использовалось допущение, что ЦС, вносимый расстоянием между МС и БС, является постоянным. На практике такие случаи возможны, что схематично приведены на рисунке 4. Вариант, представленный на рисунке 4а, возможен в случае, например, выходящего из тоннеля поезда. Распределенное расположение (см. рисунок 4б) может наблюдаться, при конфигурации транспортного пути в виде железнодорожной или автомобильной магистрали.

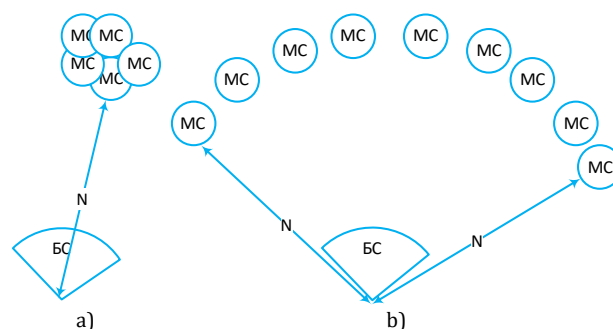


Рис. 4. Варианты расположения МС на равном удалении: а) сгруппированное; б) распределенное

Fig. 4. Variants of UE Arrangement on the Same Distance: a) Grouped; b) Distributed

В ходе эксперимента величина добавочного ЦС была взята равной 0 в силу неопределенности параметров выбора величины этого сдвига для разных значений параметра ZeroCorrelationZoneConfig. Однако на практике такие случаи не сильно распространены, и более правильным было бы ввести в расчет изменяемую величину ЦС, вызванного временной задержкой из-за расстояния между МС и БС. Величина такого добавленного ЦС не должна превышать величину, определенную выбранной конфигурацией канала случайного доступа. Характер распределения величины добавочного ЦС был выбран как равномерное случайное распределение. Полученные данные приведены в таблице 2. Цветом указаны ячейки с нехарактерными значениями, что вызвано случайным выбором при моделировании величины ЦС, эмулирующего удаление МС от БС по расстоянию.

Значения $\Delta\text{КК}$ приведены на диаграмме (рисунок 5), где видно, что $\Delta\text{КК}$ увеличивается с ростом количества одновременно передаваемых преамбул.

ТАБЛИЦА 2. Значения коэффициентов корреляции и $\Delta\text{КК}$ в зависимости от используемых корневых последовательностей с учетом возможного циклического сдвига

TABLE 2. Values of Correlation Coefficients and Its Delta Depending on the Used Sequence Roots and Considering Possible Cyclic Shift

ЦС	КК-4	$\Delta\text{КК}-4$	КК-16	$\Delta\text{КК}-16$	КК-32	$\Delta\text{КК}-32$	КК-56	$\Delta\text{КК}-56$
15	0,4991	0	0,2478	0	0,1735	0	0,1924	0,1442
18	0,4991	0	0,2478	0	0,2555	0,1748	0,1969	0,1730
22	0,4991	0	0,2478	0	0,2555	0,1748	0,1584	0,0937
26	0,4991	0	0,2478	0	0,1735	0	0,1555	0,0847
32	0,4991	0	0,2478	0	0,2113	0,0940	0,1627	0,1025
38	0,4991	0	0,2478	0	0,2022	0,0845	0,1615	0,1072
46	0,4991	0	0,2478	0	0,2006	0,0817	0,1649	0,1102
59	0,4991	0	0,2760	0,0713	0,2064	0,0916	0,2109	0,2156
76	0,4991	0	0,2775	0,0751	0,2063	0,0955	0,1662	0,1185
93	0,4991	0	0,2749	0,0689	0,2082	0,1035	0,1619	0,1130
119	0,4991	0	0,2779	0,0746	0,2072	0,1054	0,1696	0,1297
167	0,4991	0	0,2825	0,0766	0,2118	0,1092	0,1680	0,1258
279	0,5207	0,0346	0,2808	0,0835	0,2124	0,1129	0,1675	0,1252
419	0,5243	0,0172	0,2849	0,0902	0,2070	0,1039	0,1728	0,1322

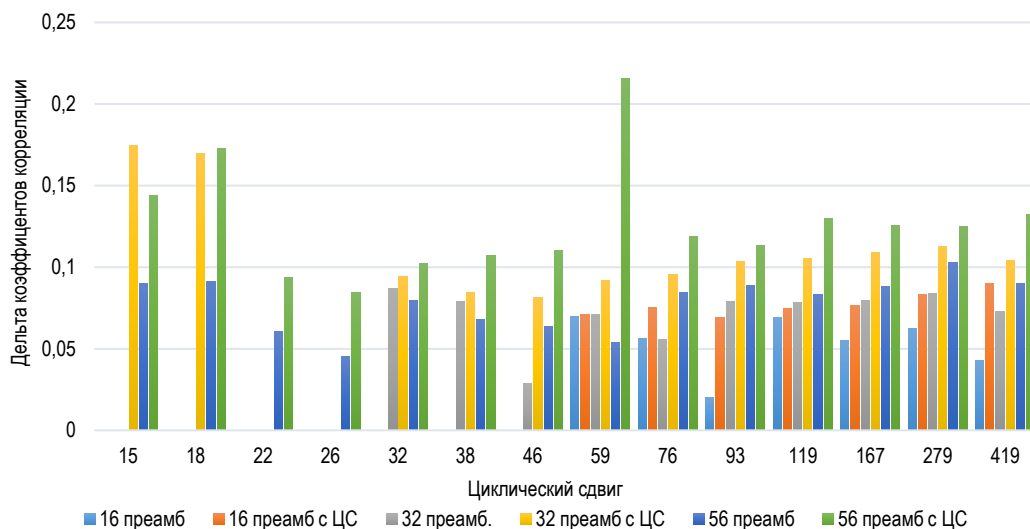


Рис. 5. Дельта минимального и максимального коэффициентов корреляции

Fig. 5. Delta Value of the Minimal and the Maximal Correlation Coefficients

График на рисунке 5 показывает разницу между максимальным и минимальным значением КК. Следует обратить внимание на большое значение Δ КК для ЦС-59 в случае передачи 56-ти преамбул. Этот выброс имеет во многом случайное значение, потому что, как было указано выше, величина добавочного ЦС в эксперименте выбиралась случайным образом, что послужило причиной этой аномалии.

На рисунке 6 приведены данные аналогичного эксперимента. Можно видеть, что большое значение Δ КК получено при ЦС-93 (на рисунки – CS-93). Однако более важным является то, что с увеличением

количества одновременно передаваемых преамбул минимальный КК стремится к 0. Это говорит о том, что есть преамбулы, которые будет очень сложно детектировать. Потенциально это вызовет повтор процедуры случайного доступа и, соответственно, увеличение времени доступа МС к сети.

Подобные повторы процедуры предусмотрены стандартом и сами по себе не несут никакого негативного влияния на сеть за исключением повышенной нагрузки на канал случайного доступа, однако в сценариях с ультранизкой задержкой это недопустимо.

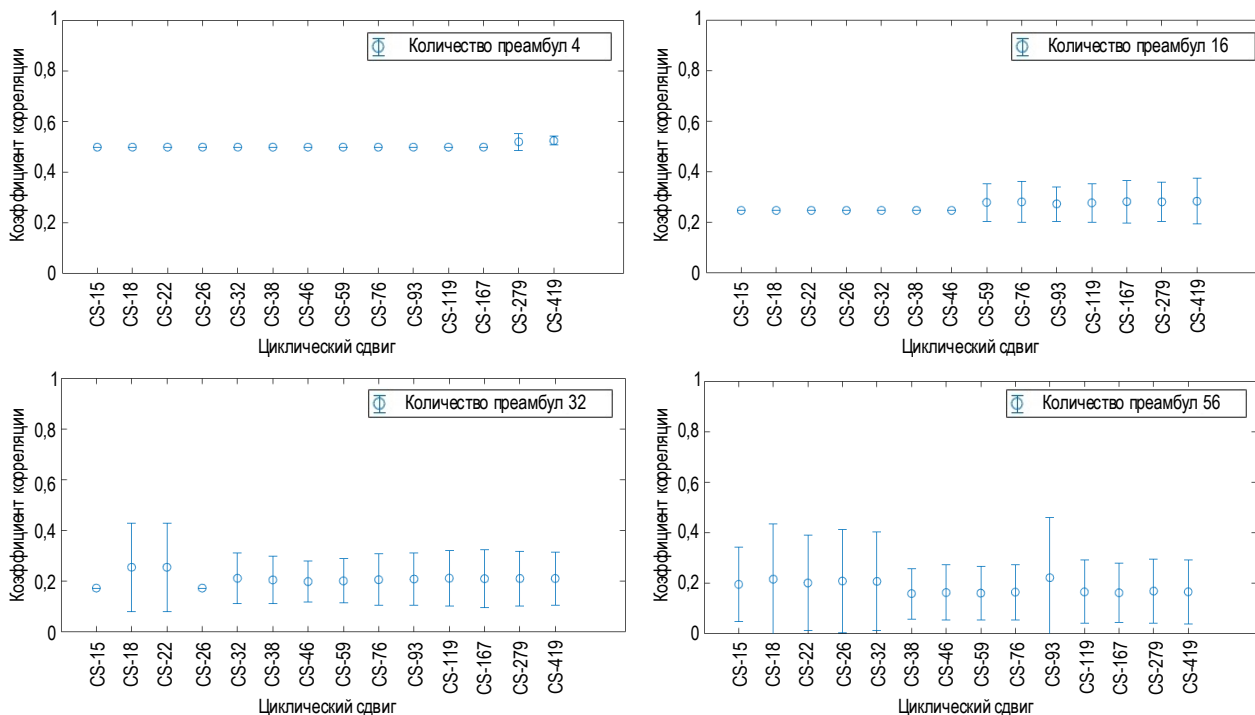


Рис. 6. Зависимость величины дельты от количества одновременно передаваемых преамбул

Fig. 6. Dependency of Delta Value from Number of Preambles Transmitted Simultaneously

Отметим, что рост значений ДКК нелинейный. Области ненулевых значений ДКК – это области, показывающие наличие значений ЦС и начальных значения корней, при которых может зависеть успешность детектирования преамбулы от выбора конкретных корней каналообразующих последовательностей. На основании этого можно сформулировать требования к рациональному выбору корней ZC -последовательности. Представляется логичным, что в процедуре случайного доступа лучше использовать корни, образующие последовательности с наибольшей корреляцией. Выбор и апробация таких корней предполагается в качестве дальнейшего развития исследования. Таким образом, можно сделать вывод, что оптимизация производительности канала случайного доступа возможна уже на уровне выбора конфигурации.

5. Заключение

В данной работе показано, что, несмотря на довольно большое количество исследований в области канала случайного доступа, по-прежнему остаются возможности для оптимизации. Несмотря на использованное в стандартах LTE и 5G NR упорядочивание преамбулообразующих корней, добиться постоянного коэффициента взаимной корреляции не удалось в силу свойств самих ZC -последовательностей. И хотя практика показывает, что имеющаяся неоднородность во взаимной корреляции не является критичной для существующих сервисов, необходимо рассматривать возможность оптимизации характеристик канала случайного доступа, основанную на рациональном выборе корней сигналаобразующей последовательности. Следует учитывать, что растущие требования к системам

мобильной связи в виде массового межмашинного обмена и ультранадежной передачи с низкой задержкой предъявляют повышенные требования в том числе и к процедурам случайного доступа. Допущения, которые были приемлемыми в решениях широкополосного доступа, могут оказаться неприемлемыми в рамках новых сервисов.

Также следует учитывать, что в сценариях внедрения новых сервисов недостатки в работе канала случайного доступа, приводящие к переповторам процедуры, будут влиять не только на временные характеристики системы, но и на возможности автономной работы устройств, сильно ограниченных по питанию. Примером могут служить сценарии МТС при использовании большого количества автономных датчиков и аналогичных им устройств. Потому направление исследований и разработки методов оптимизации канала случайного доступа должны быть продолжены с учетом внедрения сценариев новых сервисов.

В дальнейшем предполагается проведение натурного эксперимента на основе существующих детекторов канала случайного доступа.

В первую очередь в качестве объектов исследования планируется рассмотреть существующие открытые реализации стека LTE/5G NR. Среди них – решения от Software Radio Systems и Open Air Alliance. Оба эти решения позволяют работать обеими технологиями 4-го и 5-го поколений. В то же время исследования коммерческих базовых станций видится малореальным как с точки зрения доступности оборудования и организации тестовой зоны, так и с точки зрения возможных правовых коллизий с их производителями.

Список источников

1. Kottkamp M., Pandey A., Roessler A., Stuhlfauth R., Raddino D. 5G New Radio: Fundamentals, Procedures, Testing Aspects. Rohde & Schwarz, 2019. 450 p.
2. 3GPP (2017-06). Work item on Ultra Reliable Low Latency Communication for LTE (Revision of RP-170796).
3. ETSI TS 136 211 V16.2.0 (2020-09). LTE. Evolved Universal Terrestrial Radio Access (E-UTRA). Physical channels and modulation. 3GPP TS 36.211 version 16.2.0 Release 16. Technical Specification.
4. ETSI TS 138 211 V16.2.0 (2020-07). 5G. NR. Physical channels and modulation. 3GPP TS 38.211 version 16.2.0 Release 16. Technical Specification.
5. Jang H.S., Kim S.M., Park H.-S., Sung D.K. An Early Preamble Collision Detection Scheme Based on Tagged Preambles for Cellular M2M Random Access // IEEE Transactions on Vehicular Technology. 2016. Vol. 66. Iss. 7. PP. 5974–5984. DOI:10.1109/TVT.2016.2646739
6. Vilgelm M., Gürsu H.M., Kellerer W., Reisslein M. LATMAPA: Load-Adaptive Throughput-MAXimizing Preamble Allocation for Prioritization in 5G Random Access // IEEE Access. 2017. Vol. 5. PP. 1103–1116. DOI:10.1109/ACCESS.2017.2651170
7. Lo A., Law Y.W., Jacobsson M., Kucharzak M. Enhanced LTE-Advanced Random-Access Mechanism for Massive Machine-to-Machine (M2M) Communications // 27th World Wireless Research Forum (WWRF) Meeting (WWRF27- WG4-08, Atlantic City, USA, October 2011).
8. Laya A., Alonso L., Alonso-Zarate J. Efficient Contention Resolution in Highly Dense LTE Networks for Machine Type Communications // Proceedings of the Global Communications Conference (GLOBECOM, San Diego, USA, 06–10 December 2015). IEEE, 2015. DOI:10.1109/GLOCOM.2015.7417669
9. Condoluci M., Dohler M., Araniti G., Molinaro A., Sachs J. Enhanced Radio Access and Data Transmission Procedures Facilitating Industry-Compliant Machine-Type Communications over LTE-Based 5G Networks // IEEE Wireless Communications. 2016. Vol. 23. Iss. 1. PP. 56–63. DOI:10.1109/MWC.2016.7422406

10. Hasan M., Hossain E., Niyato D. Random access for machine-to-machine communication in LTE-advanced networks: Issues and approaches // *IEEE Communications Magazine*. 2013. Vol. 51. Iss. 6. PP. 86–93. DOI:10.1109/MCOM.2013.6525600
11. Wiriaatmadja D.T., Choi K.W. Hybrid Random Access and Data Transmission Protocol for Machine-to-Machine Communications in Cellular Networks // *IEEE Transactions on Wireless Communications*. 2014. Vol. 14. Iss. 1. PP. 33–46. DOI:10.1109/TWC.2014.2328491
12. Lavrukhin V., Lazarev V., Ryjkov A. Correlation Properties Comparative Analysis of Pseudorandom Binary Sequences and LTE Standard ZC Sequences // *Proceedings of the 16th International Conference on Internet of Things, Smart Spaces, ruSMART 2016, and Next Generation Networks and Systems, NEW2AN 2016* (St. Petersburg, Russia, 26–28 September 2016). *Lecture Notes in Computer Science (LNCS, Vol. 9870)*. Computer Communication Networks and Telecommunications (LNCCN). Cham: Springer, 2016. PP. 414–425. DOI:10.1007/978-3-319-46301-8_35

References

1. Kottkamp M., Pandey A., Roessler A., Stuhlfauth R., Raddino D. *5G New Radio: Fundamentals, Procedures, Testing Aspects*. Rohde & Schwarz; 2019. 450 p.
2. 3GPP (2017-06). *Work item on Ultra Reliable Low Latency Communication for LTE* (Revision of RP-170796).
3. ETSI TS 136 211 V16.2.0 (2020-09). *LTE. Evolved Universal Terrestrial Radio Access (E-UTRA). Physical channels and modulation*. 3GPP TS 36.211 version 16.2.0 Release 16. Technical Specification.
4. ETSI TS 138 211 V16.2.0 (2020-07). *5G. NR. Physical channels and modulation*. 3GPP TS 38.211 version 16.2.0 Release 16. Technical Specification.
5. Jang H.S., Kim S.M., Park H.-S., Sung D.K. An Early Preamble Collision Detection Scheme Based on Tagged Preambles for Cellular M2M Random Access. *IEEE Transactions on Vehicular Technology*. 2016;66970:5974–5984. DOI:10.1109/TVT.2016.2646739
6. Vilgelm M., Gürsu H.M., Kellerer W., Reisslein M. LATMAPA: Load-Adaptive Throughput-Maximizing Preamble Allocation for Prioritization in 5G Random Access. *IEEE Access*. 2017;5:1103–1116. DOI:10.1109/ACCESS.2017.2651170
7. Lo A., Law Y.W., Jacobsson M., Kucharzak M. Enhanced LTE-Advanced Random-Access Mechanism for Massive Machine-to-Machine (M2M) Communications. *27th World Wireless Research Forum (WWRF) Meeting (WWRF27- WG4-08, October 2011)*, Atlantic City, USA.
8. Laya A., Alonso L., Alonso-Zarate J. Efficient Contention Resolution in Highly Dense LTE Networks for Machine Type Communications. *Proceedings of the Global Communications Conference, GLOBECOM, 06–10 December 2015, San Diego, USA*. IEEE; 2015. DOI:10.1109/GLOCOM.2015.7417669
9. Condoluci M., Dohler M., Araniti G., Molinaro A., Sachs J. Enhanced Radio Access and Data Transmission Procedures Facilitating Industry-Compliant Machine-Type Communications over LTE-Based 5G Networks. *IEEE Wireless Communications*. 2016;23(1):56–63. DOI:10.1109/MWC.2016.7422406
10. Hasan M., Hossain E., Niyato D. Random access for machine-to-machine communication in LTE-advanced networks: Issues and approaches. *IEEE Communications Magazine*. 2013;51(6):86–93. DOI:10.1109/MCOM.2013.6525600
11. Wiriaatmadja D.T., Choi K.W. Hybrid Random Access and Data Transmission Protocol for Machine-to-Machine Communications in Cellular Networks. *IEEE Transactions on Wireless Communications*. 2014;14(1):33–46. DOI:10.1109/TWC.2014.2328491
12. Lavrukhin V., Lazarev V., Ryjkov A. Correlation Properties Comparative Analysis of Pseudorandom Binary Sequences and LTE Standard ZC Sequences. *Proceedings of the 16th International Conference on Internet of Things, Smart Spaces, ruSMART 2016, and Next Generation Networks and Systems, NEW2AN 2016, 26–28 September 2016, St. Petersburg, Russia. Lecture Notes in Computer Science (LNCS, vol.9870)*. Computer Communication Networks and Telecommunications (LNCCN). Cham: Springer; 2016. p.414–425. DOI:10.1007/978-3-319-46301-8_35

Статья поступила в редакцию 11.10.2022; одобрена после рецензирования 31.10.2022; принята к публикации 01.11.2022.

The article was submitted 11.10.2022; approved after reviewing 31.10.2022; accepted for publication 01.11.2022.

Информация об авторе:

БАБАНОВ
Иван Андреевич

аспирант кафедры радиосвязи и вещания Санкт-Петербургского государственного университета телекоммуникаций им. проф. М.А. Бонч-Бруевича

 <https://orcid.org/0000-0002-8782-5819>

Научная статья

УДК 004.7

DOI:10.31854/1813-324X-2022-8-4-109-118



Способ и алгоритм определения типа трафика в зашифрованном канале связи

Сергей Маратович Ишкуватов, sysroot0@gmail.com

Национальный исследовательский университет ИТМО,
Санкт-Петербург, 197101, Российская Федерация

Аннотация: В статье предложен способ определения состава протоколов, применяемых в IPsec-канале связи, на основе закономерностей хронологии следования и длин пакетов с зашифрованной нагрузкой. Рассмотрены характерные информативные признаки протоколов. Приведен алгоритм, позволяющий получить значения длин ESP-пакетов, содержащих произвольные пользовательские данные, для распространенных режимов работы IPsec-туннеля.

Ключевые слова: шифрование, пассивный наблюдатель, Virtual Private Network, IPsec-туннель

Ссылка для цитирования: Ишкуватов С.М. Способ и алгоритм определения типа трафика в зашифрованном канале связи // Труды учебных заведений связи. 2022. Т. 8. № 4. С. 109–118. DOI:10.31854/1813-324X-2022-8-4-109-118

Method and Algorithm for Determining the Type of Traffic in an Encrypted Communication Channel

Sergei Ishkuvatov, sysroot0@gmail.com

ITMO University,
St. Petersburg, 197101, Russian Federation

Abstract: The article proposes a method for determining the composition of protocols used in IPsec communication channel, based on the regularities of the chronology and the lengths of encrypted load packets. The characteristic informative features of the protocols are considered. An algorithm is given to obtain the length values of ESP packets containing arbitrary user data for common modes of IPsec tunnel operation.

Keywords: encryption, passive observer, Virtual Private Network, IPsec tunnel

For citation: Ishkuvatov S. Method and Algorithm for Determining the Type of Traffic in an Encrypted Communication Channel. *Proc. of Telecom. Universities*. 2022;8(4):109–118. (in Russ.) DOI:10.31854/1813-324X-2022-8-4-109-118

Введение

Распространение каналов Virtual Private Network (VPN), способных скрывать от пассивного наблюдателя передаваемые данные, и, как следствие – возможность обхода сетевых блокировок и политик корпоративных сетей, делает актуальным задачу определения видов протоколов, используемых внутри зашифрованных каналов связи (ШКС). Ряд научных работ демонстрирует возможность определения передаваемых видов протоколов в VPN-

канале с помощью нейронных сетей, анализирующих объемные и интервальные зависимости передаваемых сторонами порций данных [1–4]. Они рассматривают методы классификации исследуемых видов трафика для разных протоколов обеспечения защиты данных (OpenVPN, IPsec, TLS), но только в контексте выявления в них одного вида трафика. Нейронные сети, анализирующие трафик, в качестве входных признаков используют ограниченный набор доступных параметров: время регистрации

или длительность интервалов между пакетами, их длину и, иногда – направление передачи. При этом применяется корреляция между этими параметрами вложенного протокола и протокола обеспечения защиты данных.

В общем случае ШКС может содержать один вид трафика или их различные комбинации. В первом случае размеры и интервалы пакетов определяются исключительно свойствами этого трафика; во втором – общий трафик будет содержать признаки каждого из них, что увеличивает вероятность ложного распознавания или не распознавания используемых протоколов. Вместе с тем, следует отметить наличие устойчивых закономерностей между наблюдаемыми внешними характеристиками шифрованного трафика и передаваемыми внутри него данными. Особую ценность этим закономерностям придает то, что они могут быть выявлены и проанализированы с использованием низкзатратных вычислительных процедур, что открывает возможность *разработки методов и средств определения видов протоколов внутри ШКС*. Кроме того, при анализе передаваемых данных важно определять и в последствии учитывать параметры конфигурации канала, которые будут одинаково сказываться на характеристиках всех передаваемых в этом канале протоколов.

Задача исследования

Таким образом, задачей исследования является *разработка и проверка продуктивности алгоритма определения видов протоколов, используемых внутри ШКС* на основании закономерностей между наблюдаемыми внешними характеристиками шифрованного трафика и передаваемыми внутри него данными. Ее решение предполагает *выявление этих закономерностей и формализацию правил, позволяющих определить используемые сетевые протоколы в IPsec-трафике без применения нейронных сетей*.

Предлагаемый алгоритм должен обеспечивать работоспособность и при наличии нескольких видов трафика в ШКС. Алгоритм должен быть применим с произвольного момента времени и не должен иметь необходимости учитывать данные, передаваемые только в определенных фазах соединения (например, данных протокола Internet Key Exchange при установлении соединения).

Описание условий и режимов функционирования исследуемого ШКС

Модель ШКС

В работе используется типовая модель ШКС, которая применяется для передачи данных через сеть Интернет таким способом, чтобы передаваемая информация была защищена от чтения и модификации узлами сети по пути следования пакетов.

Стандартными этапами информационного обмена в ШКС являются:

- 1) установление соединения;
- 2) согласование применения алгоритмов шифрования, проверки целостности и аутентификации сторон;
- 3) упаковка передаваемых данных в пакеты, обеспечивающие шифрование и контроль целостности.

Так как ШКС всегда добавляет к передаваемым данным служебные заголовки, это уменьшает значение MTU (*аббр. от англ. Maximum Transmission Unit*) шифрованного канала, которое влечет необходимость фрагментировать крупные пакеты и уменьшать максимальные допустимые размеры сегментов (например, в протоколе TCP) для сокращения фрагментации.

В контексте решаемой задачи IPsec [5] состоит из протоколов, обеспечивающих следующий функционал: Encrypted Secure Payload (ESP) [6] – шифрование передаваемой информации; Authentication Header (AH) – целостность и аутентификацию источника; Internet Security Association and Key Management Protocol (ISAKMP) – первичную настройку соединения, взаимную аутентификацию и обмен ключами.

Определены 2 режима функционирования:

- транспортный (шифруются только данные IP-пакета, но сохраняется исходный IP-заголовок);
- туннельный (весь исходный IP-пакет, включая информацию об отправителе и получателе, содержится в шифрованной нагрузке нового пакета; часто используется совместно с L2TP).

Тогда в зависимости от используемых конфигураций типовая структура данных, наблюдаемых в ШКС, представлена на рисунке 1.

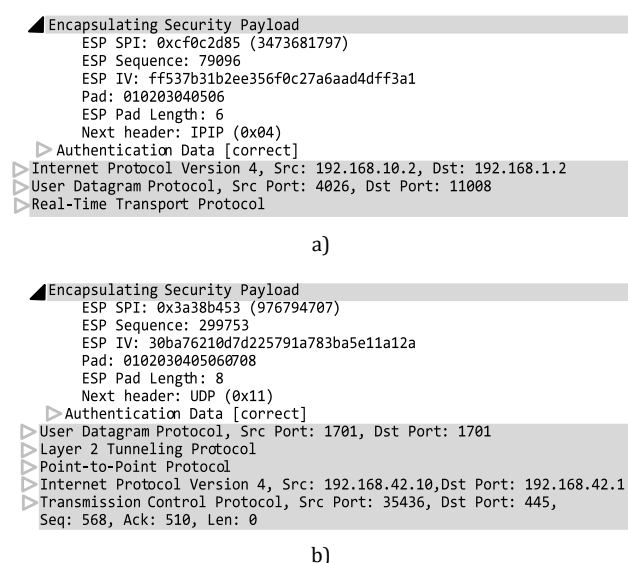


Рис. 1. Стеки протоколов внутри ESP-пакетов: только IP-заголовок (а), стек с L2TP (б)

Fig. 1. Protocol Stacks Inside ESP packets: IP Header Only (a), Stack with L2TP (b)

Таким образом, пользовательская нагрузка в каждом ESP-пакете будет содержать составляющую постоянной длины, зависящую от режима функционирования туннеля (рисунок 2; условные обозначения по таблице 1).

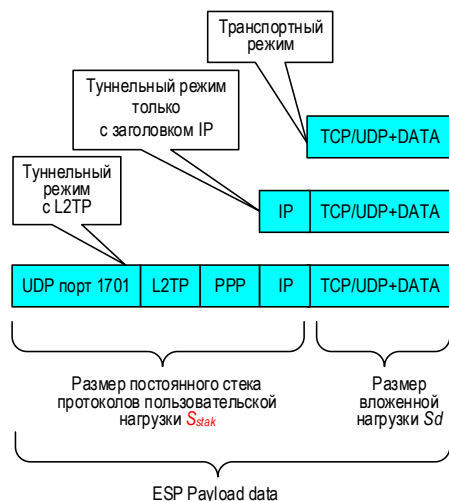


Рис. 2. Структура ESP-пакета

Fig. 2. ESP Packet Structure

Кроме того, на протяжении всего времени существования каждого конкретного туннеля предполагается неизменность размеров полей Initialization Vector, Authentication Data и алгоритма шифрования для всех ESP-пакетов (рисунок 3; на белом фоне – не шифруемые данные).

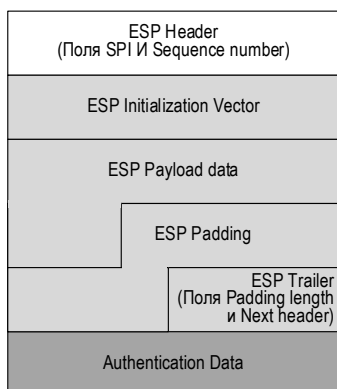


Рис. 3. Схема расположения служебных полей в ESP-пакете

Fig. 3. Layout of Service Fields in the ESP Packet

Определение и характеристики анализируемых данных

Пассивному наблюдателю ШКС, не имеющему ключей шифрования, для анализа доступны только следующие параметры: общие длины ESP-пакетов, значения 32-битового идентификатора туннеля (SPI) и порядковые номера (Sequence number) для пакетов каждого из направлений (см. рисунок 3). Скрытые шифрованием поля, исключая пользовательскую нагрузку, имеют небольшой набор возможных длин, определяемых параметрами канала. Сумма длин всех полей и пользовательской нагрузки равна длине ESP-пакета.

В таблице 1 приводятся возможные размеры служебных заголовков для разных режимов работы IPsec. Если обозначить размер постоянного стека протоколов пользовательской нагрузки S_{stak} (вложенной в ESP), то это позволит объединить записи формул для транспортного или туннельного режима, приведенные в работе [7].

Стандартными средствами мониторинга трафика обеспечивается получение только размера каждого ESP-пакета в сессии (S_{ESP}). На основании собранных длин пакетов становится возможным определить используемый в сессии размер блока алгоритма шифрования. Устанавливать конкретный использующийся алгоритм шифрования нет необходимости, т. к. в дальнейшем для расчетов используется только размер блока Bl . Результирующая длина ESP-пакета за вычетом константы всегда кратна Bl (16 или 32, а для режима AEAD – 4 байтам). Несмотря на то, что в некоторых случаях размер поля AuT_{ESP} может быть определен активным воздействием на ШКС (например, утилитами типа *ike-scan* [8]), прямому наблюдению средствами мониторинга он не доступен и может оцениваться только статистически.

Определение закономерностей функционирования ШКС

Эмпирическим путем выявлен ряд зависимостей между типом трафика в канале связи и распределением длин ESP-пакетов, осуществляющих их передачу. На основании этого выдвигается гипотеза о наличии закономерности между длиной ESP-пакета и пользовательского вложения. Кроме того, апостериорно определены закономерности между номенклатурой протоколов, одновременно присутствующих в ШКС. Это позволяет делать априорные предположения о наличии «сопутствующих» протоколов при обнаружении одного из них. Например, при обнаружении сессии RTP-протокола следует предполагать наличие протоколов сигнализации и установления соединения SIP, MGCP или H.323, а также протокола управления передачей в реальном времени RTP.

Примером описываемой закономерности является зависимость размера шифрованной нагрузки ESP-пакета от размера, передаваемого в нем пакета нагрузки, определяемая организацией структуры самого протокола. Размер накладных расходов служебных заголовков ESP-пакета (ESP Overhead) зависит от выбранного метода шифрования и размера поля Padding, который, в свою очередь, определяется остатком от деления размера вложенных данных на размер блока шифрования. В сети Интернет доступны калькуляторы длин IPsec-пакетов для произвольных вариаций стеков вложенных в IPsec протоколов [9, 10], которые позволяют вычислить размеры служебных заголовков в зависимости от используемого типа шифрования.

ТАБЛИЦА 1. Обозначение, назначение и размеры полей протокола IPsec [7]

TABLE 1. Designation, Purpose and Sizes of IPsec Protocol Fields [7]

Обозначение	Описание	Длина
H_{ESP}	Поле ESP Header	8 байт
Bl	Размер блока алгоритма шифрования	– 16 байт (aes128, blowfish128, cast128) – 8 байт (des, 3des) – 4 байта (AEAD)
IV_{ESP}	Поле ESP Initialization Vector	Равен Bl , но в режиме работы AEAD 16 байт
Tr_{ESP}	ESP Trailer	2 байта
AuT_{ESP}	Authentication Data	– 12 байт (96 bit HMAC включая: md5, sha1, aesxcbc, aescmac, sha256_96) – 16 байт (128 bit HMAC включая: md5_128, aes128gmac, aes192gmac, aes256gmac) – 20 байт (160 bit HMAC, sha1_160) – 24 байта (192 bit HMAC) – 32 байта (256 bit HMAC)
Pad_{ESP}	ESP Padding	Определяется остатком от деления общего размера всего стека протоколов, нагрузки вложенного пакета и Tr_{ESP} на Bl Длина поля от 0 до $(Bl - 1)$ байт
Sd	Размер вложенной нагрузки без постоянного стека протоколов	Длина пользовательской нагрузки, начиная с заголовков транспортных протоколов
S_{stak}	Размер постоянного стека протоколов пользовательской нагрузки.	Суммарный размер всех заголовков пользовательской нагрузки до начала транспортного уровня: – 0 байт при транспортном режиме; – 20 байт для туннельного режима в случае вложения только заголовка IP Header. Более 20 байт для туннельного режима в случае присутствия заголовков помимо заголовка IP Header
S_{ESP}	Полный размер порции данных ESP, содержащей все служебные заголовки и полезную вложенную нагрузку, не включает вышестоящие протоколы	

Другой полезной особенностью протокола IPsec в контексте определения вида передаваемого трафика может быть сохранение значения приоритета вложенного трафика в поле Type of Service (ToS). В большинстве случаев значение поля копируется из пакета вложения в заголовок ESP-пакета для сохранения возможности приоритизации чувствительного к задержкам трафика [11]. Таким образом, шифрованный трафик в большом количестве случаев будет иметь DSCP, (аббр. от англ. Differentiated Services Code Point), подобный исходному, что может являться дополнительным признаком при определении некоторых типов нагрузки.

Статистические закономерности вложенного трафика будут проявляться и в транспортирующем его трафике IPsec. Разбив сигнал на небольшие интервалы времени Δt , можно построить распределение длин всех пакетов, встретившихся в этом интервале времени. При визуализации серии пакетов одинаковой длины будут создавать в таком распределении линии для соседних интервалов или одиночные точки, повторяющиеся с определенной периодичностью.

В части случаев несколько линий появляются только совместно, например, при передаче данных равными порциями большого размера. В этом случае линию создаст максимальный размер пакета и остаток порции. Абсолютные значения длин, передаваемых по сети IPsec-пакетов, будут отличаться в зависимости от стека протоколов внутри канала, поэтому при исследовании следует рассматривать относительные значения длин и возможные диапазоны значений исходных не упакованных данных.

Длины ESP-пакетов для всех режимов с аутентификацией (ATH) можно вычислить как:

$$S_{ESP} = H_{ESP} + Tr_{ESP} + IV_{ESP} + AuT_{ESP} + Sd + S_{stak} + Pad_{ESP}, \quad (1)$$

где Pad_{ESP} – размер поля ESP Padding, определяемый остатком от деления (mod) суммы размеров вложенной пользовательской нагрузки полностью ($Sd + S_{stak}$) и константной длины Tr_{ESP} (см. выражение 2) на размер блока выбранного алгоритма шифрования (Bl).

Таким образом, сумма $Sd + S_{stak} + Tr_{ESP} + Pad_{ESP}$ всегда кратна Bl .

$$Pad_{ESP} = \begin{cases} 0, & \text{если } ((Sd + S_{stak} + Tr_{ESP}) \bmod Bl) = 0 \\ Bl - ((Sd + S_{stak} + Tr_{ESP}) \bmod Bl), & \text{в остальных случаях.} \end{cases} \quad (2)$$

Выражение ниже устанавливает зависимость между длиной пользовательских данных и параметрами ШКС; оно может быть использовано для вычисления границ размеров вложенного пакета пользовательской нагрузки, а также для получения длины исходных пользовательских данных при известных S_{ESP} , Bl , AuT_{ESP} и S_{stak} :

$$S_d = S_{ESP} - H_{ESP} - Tr_{ESP} - IV_{ESP} - AuT_{ESP} - S_{stak} - Pad_{ESP}.$$

Алгоритм определения видов протоколов, используемых внутри ШКС

Обобщенный алгоритм определения видов протоколов, используемых внутри ШКС, предполагает выполнение следующих операций.

1) Подготовить список отличительных признаков протоколов, содержащих характерные распределения длин пакетов, начиная с заголовков транспортного уровня включительно (TCP, UDP), хронологические и интервальные закономерности (см. Обсуждение результатов).

2) Определить значение размера блока алгоритма шифрования Bl (см. таблицу 1): вычисляется как минимальная разница между любыми двумя зарегистрированными значениями длин S_{ESP} .

3) Определить возможные значения AuT_{ESP} , величина должна безостаточно делиться на Bl , т. е. для любой встречаемой длины S_{ESP} должно выполняться равенство $(S_{ESP} - H_{ESP} + IV_{ESP} + AuT_{ESP}) \bmod Bl = 0$.

4) Для каждого распределения длин из подготовленного списка признаков по формуле (1) вычислить поправку до размера ESP-пакета, для возможных значений Bl , AuT_{ESP} и S_{stak} .

5) Искать совпадения признаков, полученных на предыдущем этапе в передаваемом трафике. При нахождении четкого совпадения сохранение параметров Bl , AuT_{ESP} и S_{stak} и в дальнейшем использование только их в этом конкретном IPsec-тоннеле.

6) При обнаружении стабильно передаваемых и легко прогнозируемых протоколов (таких как потоковое аудио или видео) следует вычестить из суммарного распределения значения, вносимые этими протоколами, для облегчения поиска других протоколов.

Эксперимент

Для проверки продуктивности предлагаемого алгоритма проведен эксперимент по моделированию работы IPsec-тоннеля на базе решения StrongSwan, в котором поочередно передавались протоколы:

- Samba и FTP в момент загрузки файлов;
- VoIP, содержащий пакеты установления соединения SIP и речевые пакеты RTP G.729, G.711, G.723.1;
- RDP (аббр. от англ. Remote Desktop Protocol);
- BitTorrent в различных режимах.

Все пакеты шифрованного трафика записывались в PCAP-файл утилитой tcpdump. Протоколировались SPI ESP-пакетов каждого направления, время регистрации и длина пакета нагрузки. Для фрагментированных IP-пакетов записывалась итоговая длина и время регистрации первого. Это позволило находить хронологические закономерности, распределение длин ESP-пакетов. Командой «ip xfrm state» сохранялись сессионные ключи, которые использовались для проверки корректности работы алгоритма. Для записей с *большой дисперсией длин пакетов* параметр размера блока алгоритма шифрования Bl определяется минимальной разницей между любыми двумя зарегистрированными значениями длин S_{ESP} . В некоторых случаях Bl может быть определен как максимальный результат безостаточного деления каждой встречаемой длины пакета S_{ESP} за вычетом $H_{ESP} + IV_{ESP} + AuT_{ESP}$ на 16,8 и 4.

Для автоматического обнаружения видов протоколов внутри ШКС реализованы программные модули-детекторы, базирующиеся на выделенных закономерностях распределения длин пакетов. На вход детекторов помимо сигнала последовательно подавались возможные значения параметров Bl , AuT_{ESP} и S_{stak} .

Результаты, полученные обработчиком на подготовленном датасете для каждого типа детектируемого трафика, сведены в таблицу 2, где: A – количество срабатываний детекторов с правильно подобранной конфигурацией; B – с любой вариацией ошибочного определения конфигурацией или вложенного стека.

ТАБЛИЦА 2. Результаты обработки файлов записей

Table 2. Results of Processing Record Files

Тип трафика	Количество файлов записей	Количество срабатываний детекторов			
		если трафик присутствует в записи		отсутствующих в записи типов трафика	
		A	B	A	B
RTP G.711	100	100	0	0	0
RTP G.723.1	100	100	0	0	0
RTP G.729	100	100	0	0	0
RDP	100	66	476	0	0
FTP	100	85	106	0	0
BitTorrent	50	46	303	0	105

Количество корректных результатов детектирования протоколов с правильно подобранными параметрами Bl , AuT_{ESP} и S_{stak} содержатся в графе «с правильно подобранной конфигурацией». Отдельной графой приведено количество корректного детектирования этого протокола с любыми некорректными значениями из Bl , AuT_{ESP} и S_{stak} . Такое сравнение позволяет выбрать наиболее подходящие протоколы обработчики для первоначального определения значений параметров Bl , AuT_{ESP} и S_{stak} . Эти па-

параметры смогут использоваться другими детекторами как основные. Для оценки общего качества детектирования приведены поля с количествами ложных срабатываний также с разделением на корректные конфигурации и ошибочные. Такое разделение демонстрирует возможность уменьшения ложных срабатываний детектора четким заданием правильных значений параметров Bl , AuT_{ESP} и S_{stak} .

В результате анализа установлено, что в ряде случаев детекторы срабатывали на близких, но неправильных значениях AuT_{ESP} (например, 12 и 16 байт) по причине округления длин пользовательской нагрузки до их кратности размеру Bl . В части случаев неопределенность снимается за счет срабатывания других детекторов, результирующие значения длин которых попадают в разные диапазоны кратности Bl .

В ходе эксперимента подтверждена продуктивность «вычитания» данных идентифицированного протокола из общего трафика канала на примере дуплексной передачи RTP-пакетов. Такая процедура не затронула случайные наложения длин от других протоколов ввиду высокой регулярности данных RTP-сеанса.

Обсуждение результатов

Для удобства анализа и интерпретации результатов распределения длин ESP-пакетов визуализировались в виде графиков для интервалов $\Delta t = 0,5$ секунд и длиной пакета, деленной на Bl .

Samba и FTP

На рисунке 4 представлено распределение длин пакетов протоколов Samba и FTP (желтый и красный цвета обозначают направления передачи, оранжевым цветом обозначено совпадение значений).

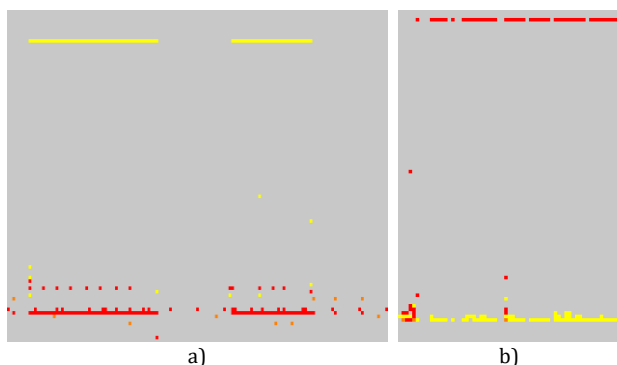


Рис. 4. Распределение длин ESP-пакетов, содержащих сессии Samba (a) и FTP (b) во время передачи файлов

Fig. 4. Distribution of ESP Packet Lengths Containing Samba (a) and FTP (b) Sessions During File Transfer

При загрузке файла с сервера с использованием протоколов на базе TCP в трафике загружающего всегда будут преобладать пакеты подтверждений получения очередных порций данных (TCP Acknowledgment). В пакетах от сервера всегда бу-

дет преобладать максимальный возможный размер пакетов, определяемый максимальным размером передаваемого по сети сегмента Maximum Segment Size (MSS), который, в свою очередь, определяется минимальным значением MTU сети на пути следования пакетов. Таким образом, полученное значение в поле MSS TCP-пакетов от одного отправителя будет отличаться у разных адресатов в зависимости от их способа доступа в сеть [12]. Такой баланс свойственен всем протоколам с короткими запросами и объемными ответами: FTP, Samba, HTTP.

Однако для каждого из них могут выявляться характерные закономерности длин запросов и ответов на них. В Linux реализации протокола Samba версии 2 заметны закономерности передачи трафика: пакет Read AndX Response фиксированной длины всегда предвещает серию пакетов максимального размера объемной передачи данных.

VoIP

Для части протоколов возможно преобладание пакетов фиксированного размера и частоты, определяемые ограничениями протоколов или особенностями их реализаций. При передаче VoIP, в обоих направлениях передачи будет наблюдаться стабильная по длине и интервалу времени составляющая длин RTP-пакетов (рисунок 5). Значение суммарной длины получившегося пакета будет определяться размером порции данных кодека, используемого в сеансе, и размером служебных заголовков, в том числе заголовка ESP.

Средний интервал повторения RTP-пакетов во время разговора также стабилен, и определяется реализацией (размером порций), что позволяет на низко загруженных каналах с малым количеством одновременных передач и различных протоколов выявить такие характерные признаки из общего спектра. При использовании RTP PCMA (G.711 с характеристиками: скорость – 64 кбит/с; пакетная скорость – 50 пакетов/с; размер полезной – 160 байт; полный размер RTP-пакета – 172 байта) размер полного пакета ESP ~ 248 байт, период ~ 20 миллисекунд. При использовании кодеков с большей степенью сжатия размер RTP-пакетов может сократиться, или уменьшится частота появления таких пакетов. Несколько VoIP-сеансов в один момент времени не изменяют распределения длин пакетов, нократно своему количеству уменьшат средний интервал между RTP-пакетами. Если представить изображение в виде тепловой с количествами длин в интервале времени, то можно установить моменты наложения нескольких сеансов.

Также, определив параметры передаваемой RTP-сессии, можно вычесть точки, создаваемые ею из общего распределения, тем самым облегчив распознавание оставшихся протоколов.

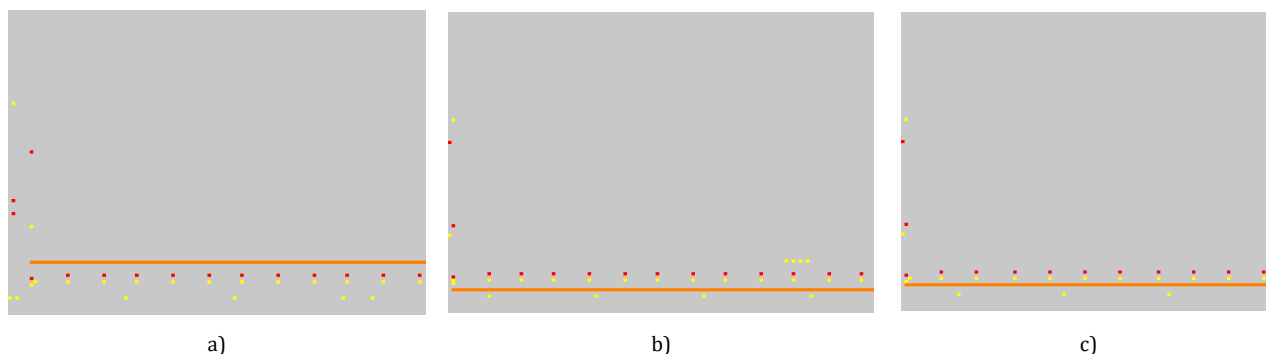


Рис. 5. Распределение длин ESP-пакетов, содержащих VoIP-сессии с кодеками G.711(a), G.729(b) и G.723.1(c)

Fig. 5. Distribution of ESP Packet Lengths Containing VoIP Sessions with Codecs G.711(a), G.729(b) and G.723.1(c)

RDP

Трафик сеанса удаленного рабочего стола по протоколу RDP имеет широкий спектр встречающихся длин пакетов, однако рассмотрение его отдельно по направлениям даёт возможность выявить различия в наблюдаемых диапазонах значений длин и в объемах передаваемых данных (рисунок 6). На рисунке видно, как на большом количестве сеансов проявляются одновременно 3 линии с постоянными значениями длин. Также заметен четкий верхний предел размеров пакетов клиента желтого цвета.

В статье [13] рассматривается возможность определения типа пользовательской активности исследованием исходного RDP-трафика, анализируются статистические характеристики длин передаваемых исходных пакетов, интервалы и тип протоколов передачи. При передаче трафика RDP в IPsec-тоннеле в зависимости от конфигурации тоннеля (обуславливающей значения *Bl*, *AuT_{ESP}* и *S_{stak}*) абсолютные значения длин увеличатся на вычисляемые размеры служебных заголовков, а характеристики, связанные только с интервалами активности не изменятся. Таким образом, можно сделать вывод о потенциальной возможности определения типа пользовательской активности в RDP-сеансе, в случае отсутствия в канале других видов трафика, существенно искажающих общую картину распределения в момент анализа.

BitTorrent

Клиент BitTorrent во время своей работы использует несколько различных протоколов и принимает входящие соединения от множества других клиентов. При отсутствии активных раздач или загрузок превалирует протокол распределенных хеш-таблиц (DHT, аббр. от англ. Distributed Hash Table) [14], использующийся для децентрализованного поиска участников сети. DHT-пакеты присутствуют в обоих направлениях и имеют узкий диапазон длин и, как следствие, создают линии на распределении, кроме того, часто появляются ICMP-пакеты Destination Unreachable от недошедших DHT-пакетов. Также выделяется протокол uTP, пакеты Acknowledgment которого создают четкую линию в распределении длин (рисунок 7). Кроме того, в пакетах BitTorrent в поле DSCP часто устанавливается значение Class Selector 3.

В отличие от остальных рассмотренных протоколов, при функционировании клиента BitTorrent происходит взаимодействие с большим количеством узлов, которые имеют разные типы доступа в Интернет. Следствием этого является широкий диапазон значений параметра Maximum Segment Size для TCP-сессий разных абонентов, что представлено на нижнем рисунке (см. рисунок 7b), где рядом с максимальным значением можно наблюдать несколько линий.

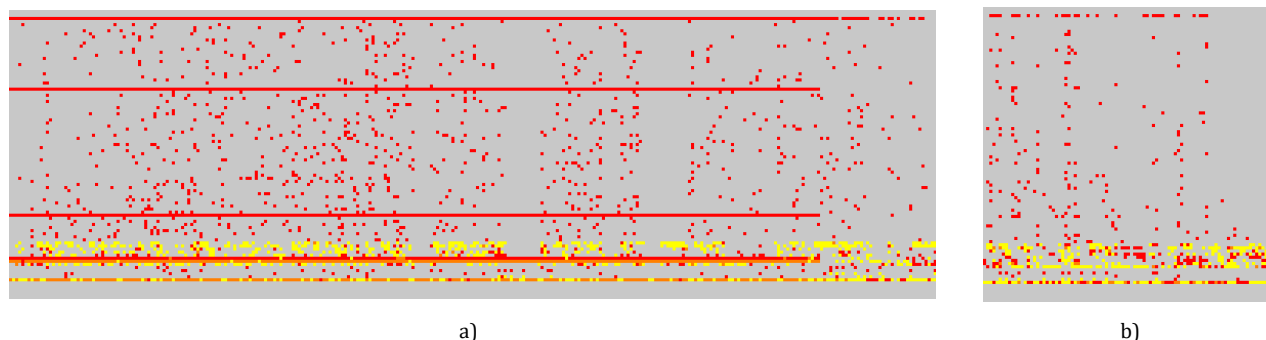


Рис. 6. Распределение длин ESP-пакетов во время сеансов удаленного рабочего стола Windows с горизонтальными линиями (a) и без них (b)

Fig. 6. Distribution of ESP Packet Lengths During Windows Remote Desktop Sessions with(a) and Without Horizontal Lines (b)

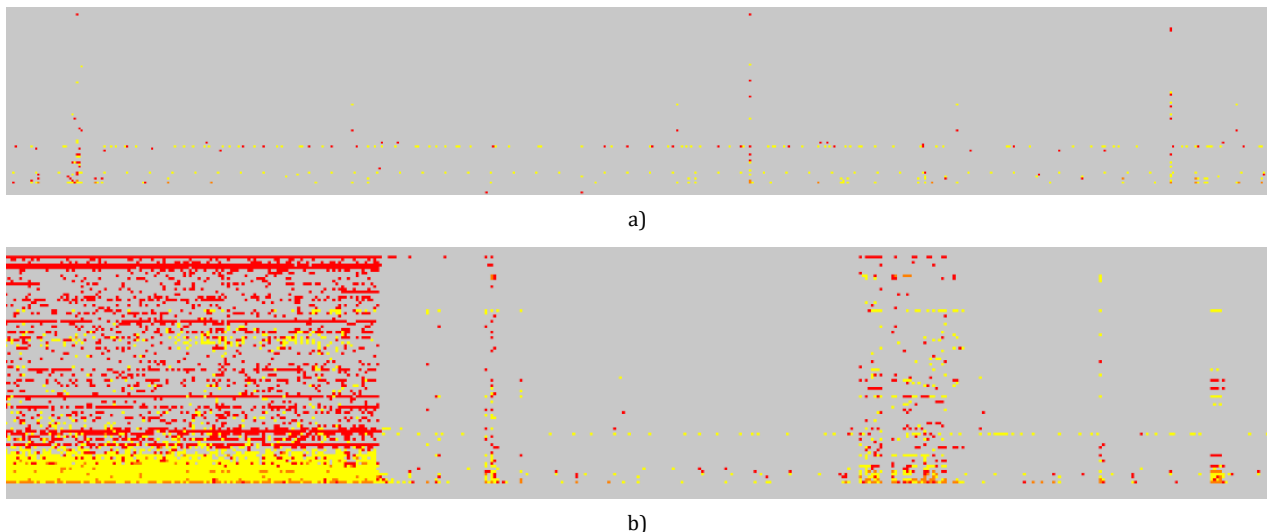


Рис. 7. Распределение длин ESP-пакетов во время функционирования клиента BitTorrent: а) без активных передач, с заметным преобладанием протокола DHT; б) во время загрузки файла

Fig. 7. Distribution of ESP Packet Lengths During the Operation of the BitTorrent Client: a) Without Active Transfers, with a Noticeable Predominance of the DHT Protocol; b) During File Upload

Оценка продуктивности алгоритма

Качество распознавания конкретного протокола в ШКС определяется номенклатурой и информативностью его признаков, а также выбранным интервалом, на котором эти признаки должны проявляться. В ходе эксперимента наблюдались ложные обнаружения RTP пакетов G.729 в RDP-трафике, что было обусловлено периодическим случайным попаданием длин, содержащих пакеты TCP Acknowledgment и RTP пакетов G.729 в одну градацию длин шифрованных пакетов. При увеличении длительности интервала, на котором делается вывод о наличии в трафике VoIP сессий минимум до 6 с, ложные срабатывания исчезали. Выбор малой длины интервала приведет к росту ложных распознаваний различных протоколов. При выборе слишком большой длины признака повышается вероятность несрабатывания этого признака на коротких сессиях.

Препятствиями применению предлагаемого способа могут быть использование искусственной фрагментации пакетов, рандомизация значений длин пакетов или одновременное использование большого количества разных протоколов, взаимно размывающих признаки друг друга. В статье [15] рассматривается противодействие статистическим атакам на IPsec посредством добавления в каждый транспортирующий пакет дополнительной служебной информации. Такое искусственное добавление данных позволяет рандомизировать объем передачи и обеспечивает возможность дополнительной фрагментации пакетов. Однако такое добавление неинформативных данных имеет ряд недостатков:

- необходимость поддержки такого функционала обеими сторонами коммуникации;

- рандомизация длин передаваемых шифрованных пакетов, без добавления неинформативных пакетов в произвольные моменты времени не скрывает график активности абонентов, сильные всплески передач трафика и приблизительный баланс приема-передачи;

- использование сопряжено со значительным увеличением объема трафика за счет добавления в него неинформативных данных; увеличение объемов трафика не всегда технически возможно (особенно при использовании мобильных сетей связи) и часто связано с увеличением затрат на передачу этих данных.

Приведенные недостатки ограничивают массовое использование способов противодействия рандомизацией длин, что позволяет применять описываемые подходы в подавляющем большинстве используемых IPsec-каналов.

Выводы

В работе предложен новый способ определения состава протоколов передающихся в IPsec-канале связи. Он базируется на низкозатратном анализе совокупностей информационных признаков, на основе закономерностей хронологии и длин пакетов.

Конкретизация предлагаемого способа выполнена в виде алгоритма, обеспечивающего обнаружения различных видов трафиков при одновременном нахождении их в ШКС. Продуктивность предложенного способа и реализующего его алгоритма подтверждается результатами эксперимента.

В ходе эксперимента была подтверждена возможность низкологозатратного определения типа трафика, передаваемого в ШКС. В качестве признаков для описания типа трафика используются одновременно разделенные по направлениям характерные константы длин пакетов данных, их последовательности и периодичности.

Практическая значимость результатов заключается в возможности выявлять факты использования определенных протоколов в ШКС, что позволит, например, операторам связи блокировать, замедлять или отдельно тарифицировать соответствующие виды трафика. Кроме того, классификация типов трафика может реализовываться системами пассивного мониторинга для установления фактов использования на контролируемом участке сети запрещенных протоколов (например, BitTorrent, TOR) и информировании администраторов о таких фактах.

Диапазоны длин ESP-пакетов для одинаковых исходных данных смещаются в зависимости параметров используемого алгоритма шифрования, что может повлиять на точность распознавания различными нейронными сетями [1–4], если они не были корректно обучены на работу в некоторых редко используемых режимах. Для компенсации таких отклонений длин следовало бы обучать нейронные сети нешифрованными образцами трафика для каждой комбинации параметров шифрования в отдельности, вычисляя результирующие длины ESP-пакетов по формуле (1).

Рассмотренный в статье алгоритм может быть адаптирован к другим протоколам VPN, позволяющим точно вычислить объем накладных расходов на добавление служебных заголовков и шифрование пакетов вложенной пользовательской нагрузки. Наиболее актуальными примерами таких протоколов являются Wireguard и OpenVPN в режимах, не использующих сжатие трафика.

Список источников

1. Rasteh A., Delpech F., Aguilar-Melchor C., Zimmer R., Shouraki S.B., Masquelier T. Encrypted Internet Traffic Classification Using a Supervised Spiking Neural Network // arXiv preprint arXiv:2101.09818. 2022. URL: <https://arxiv.org/pdf/2101.09818> (дата обращения 07.01.2022).
2. Gupta N., Jindal V., Bedi P. Encrypted Traffic Classification Using eXtreme Gradient Boosting Algorithm // Proceedings of the International Conference on Innovative Computing and Communications (ICICC 2021, Delhi, India, February 2021). Advances in Intelligent Systems and Computing (AISC). Vol. 1394. Singapore: Springer, 2022. PP. 225–232. DOI:10.1007/978-981-16-3071-2_20
3. Draper-Gil G., Lashkari A.H., Mamun M., Ghorbani A. Characterization of Encrypted and VPN Traffic Using Time-Related // Proceedings of the 2nd International Conference on Information Systems Security and Privacy (ICISSP, Rome, Italy, 19–21 February 2016). 2016. PP. 407–414. DOI:10.5220/0005740704070414
4. Islam F.U., Liu G., Liu W. Identifying VoIP traffic in VPN tunnel via Flow Spatio-Temporal Features // Mathematical Biosciences and Engineering. 2020. Vol. 17. Iss. 5. PP. 4747–4772. DOI:10.3934/mbe.2020260
5. Kent S., Seo K. Security Architecture for the Internet Protocol. No. rfc4301. 2005.
6. Atkinson R. IP Encapsulating Security Payload (ESP). No. rfc1827. 1995.
7. Xenakis C., Laoutaris N., Merakos L., Stavrakakis I. A generic characterization of the overheads imposed by IPsec and associated cryptographic algorithms // Computer Networks. 2006. Vol. 50. Iss. 17. PP. 3225–3241. DOI:10.1016/j.comnet.2005.12.005
8. Дмитренко А. Изучаем и выявляем уязвимости протокола IPsec // Хакер. 2015 URL: <https://xakep.ru/2015/05/13/ipsec-security-flaws> (дата обращения 06.04.2022)
9. Akhter A. IPSec Packet Size Calculator // Cisco Community. URL: https://community.cisco.com/legacyfs/online/legacy/4/8/7/27784-IPSec_Calculator_NAT_GRE-Key.htm (дата обращения 24.01.2022)
10. encapcalc // GitHub. URL: <http://github.com/dmbaturin/encapcalc> (дата обращения 09.06.2022)
11. Pérez J.A., Cabrera V.Z.C., Jenecek J. Quality of Service Analysis of site to site for IPsec VPNs for realtime multimedia traffic // Advanced Int'l Conference on Telecommunications and Int'l Conference on Internet and Web Applications and Services (AICT-ICIW'06, Guadelope, French Caribbean, 19–25 February 2006). 2006. URL: https://www.its.bldrdoc.gov/media/33388/per_j_slides1.pdf [Accessed 16th January 2022]
12. Ишкватов С.М., Комаров И.И. Анализ аутентичности трафика на основании данных цифровых отпечатков реализаций сетевых протоколов // Научно-технический вестник информационных технологий, механики и оптики. 2020. Т. 20. № 5. С. 747–754. DOI:10.17586/2226-1494-2020-20-5-747-754
13. Lapczyk L., Skillicorn D.B. Activity Detection from Encrypted Remote Desktop Protocol Traffic // arXiv preprint arXiv:2008.02685. 2020. DOI:10.48550/arXiv.2008.02685
14. Urdaneta G., Pierre G., Steen M.V. A survey of DHT security techniques // ACM Computing Surveys. 2011. Vol. 43. Iss. 2. PP. 1–49. DOI:10.1145/1883612.1883615
15. Kiraly C., Teofili S., Bianchi G., Cigno R.L., Nardelli M., Delzeri E. Traffic Flow Confidentiality in IPsec: Protocol and Implementation // Proceedings of the 3rd IFIP WG 9.2, 9.6/11.6, 11.7/FIDIS International Summer School on the Future of Identity in the Information Society (Karlstad University, Sweden, 4–10 August 2007). The International Federation for Information Processing. Vol. 262. Boston: Springer, 2007. PP. 311–324. DOI:10.1007/978-0-387-79026-8_22

References

1. Rasteh A., Delpech F., Aguilar-Melchor C., Zimmer R., Shouraki S.B., Masquelier T. Encrypted Internet Traffic Classification Using a Supervised Spiking Neural Network. *arXiv preprint arXiv:2101.09818*. 2022. URL: <https://arxiv.org/pdf/2101.09818> [Accessed 07.01.2022]
2. Gupta N., Jindal V., Bedi P. Encrypted Traffic Classification Using eXtreme Gradient Boosting Algorithm. *Proceedings of the International Conference on Innovative Computing and Communications, ICICC 2021, February 2021, Delhi, India. Advances in Intelligent Systems and Computing (AISC)*. Singapore: Springer; 2022. vol.1394. p.225–232. DOI:10.1007/978-981-16-3071-2_20
3. Draper-Gil G., Lashkari A.H., Mamun M., Ghorbani A. Characterization of Encrypted and VPN Traffic Using Time-Related. *Proceedings of the 2nd International Conference on Information Systems Security and Privacy, ICISPP, 19–21 February 2016, Rome, Italy*. 2016. p.407–414. DOI:10.5220/0005740704070414
4. Islam F.U., Liu G., Liu W. Identifying VoIP traffic in VPN tunnel via Flow Spatio-Temporal Features. *Mathematical Biosciences and Engineering*. 2020;17(5):4747–4772. DOI:10.3934/mbe.2020260
5. Kent S., Seo K. *Security Architecture for the Internet Protocol*. No. rfc4301. 2005.
6. Atkinson R. *IP Encapsulating Security Payload (ESP)*. No. rfc1827. 1995.
7. Xenakis C., Laoutaris N., Merakos L., Stavrakakis I. A generic characterization of the overheads imposed by IPsec and associated cryptographic algorithms. *Computer Networks*. 2006;50(17):3225–3241. DOI:10.1016/j.comnet.2005.12.005
8. Dmitrenko A. Studying and identifying IPsec protocol vulnerabilities. *Khaker*. 2015. (in Russ.) URL: <https://xakep.ru/2015/05/13/ipsec-security-flaws> [Accessed 06th April 2022]
9. Akhter A. IPsec Packet Size Calculator. *Cisco Community*. URL: https://community.cisco.com/legacyfs/online/legacy/4/8/7/27784-IPSec_Calculator_NAT_GRE-Key.htm [Accessed 24th January 2022]
10. GitHub. *encapcalc*. URL: <http://github.com/dmbaturin/encapcalc> [Accessed 09th June 2022]
11. Pérez J.A., Cabrera V.Z.C., Jenecek J. Quality of Service Analysis of site to site for IPsec VPNs for realtime multimedia traffic. *Advanced Int'l Conference on Telecommunications and Int'l Conference on Internet and Web Applications and Services AICT-ICIW'06, 19–25 February 2006, Guadelope, French Caribbean*. 2006. URL: https://www.its.bldrdoc.gov/media/33388/per_j_slides1.pdf [Accessed 16th January 2022]
12. Ishkuvatov S.M., Komarov I.I. Traffic Authenticity Analysis Based on Digital fingerprint Data of Network Protocol Implementations. *Scientific and Technical Journal of Information Technologies, Mechanics and Optics*. 2020;20(5):747–754. DOI:10.17586/2226-1494-2020-20-5-747-754
13. Lapczyk L., Skillicorn D.B. Activity Detection from Encrypted Remote Desktop Protocol Traffic. *arXiv preprint arXiv:2008.02685*. 2020. DOI:10.48550/arXiv.2008.02685
14. Urdaneta G., Pierre G., Steen M.V. A survey of DHT security techniques. *ACM Computing Surveys*. 2011;43(2):1–49. DOI:10.1145/1883612.1883615
15. Kiraly C., Teofili S., Bianchi G., Cigno R.L., Nardelli M., Delzeri E. Traffic Flow Confidentiality in IPsec: Protocol and Implementation. *Proceedings of the 3rd IFIP WG 9.2, 9.6/11.6, 11.7/FIDIS International Summer School on the Future of Identity in the Information Society, 4–10 August 2007, Karlstad University, Sweden. The International Federation for Information Processing. vol.262*. Boston: Springer; 2007. p.311–324. DOI:10.1007/978-0-387-79026-8_22

Статья поступила в редакцию 11.09.2022; одобрена после рецензирования 25.11.2022; принята к публикации 28.11.2022.

The article was submitted 11.09.2022; approved after reviewing 25.11.2022; accepted for publication 28.11.2022.

Информация об авторе:

Ишкватов
Сергей Маратович

аспирант факультета безопасности информационных технологий Национального исследовательского университета ИТМО
 <https://orcid.org/0000-0002-4006-3693>

Научная статья

УДК 004.056

DOI:10.31854/1813-324X-2022-8-4-119-129



Разработка схемы контроля доступа к данным на основе иерархии ролей с использованием постквантовых математических преобразований

Анастасия Викторовна Ярмач, yarmak.av@ibks.spbstu.ru

Санкт-Петербургский политехнический университет Петра Великого,
Санкт-Петербург, 195251, Российская Федерация

Аннотация: В работе представлена схема CSIDH-HRBAC, основанная на постквантовых математических преобразованиях и позволяющая реализовать контроль доступа к данным, располагающимся в недоверенной облачной инфраструктуре. CSIDH-HRBAC построена на базе ролевой модели управления доступом с поддержкой системы иерархии ролей. Предлагаемая схема подразумевает наличие доверенной стороны, осуществляющей управление криптографическими ключами, ассоциированными с пользователями, ролями, файлами. Приведено описание основных процедур, связанных с получением доступа к данным, лишением прав доступа, добавлением новых сущностей. Рассмотрены типовые сценарии атак на предложенную схему, в том числе подмена роли, сговор участников с целью вскрытия ключа родительской роли, попытка доступа к данным после отзыва роли у пользователя. Для оценки быстродействия криптографических операций выполнено моделирование ее работы при различных параметрах. Обсуждаются преимущества и ограничения схемы CSIDH-HRBAC. В частности, отмечается необходимость защиты от угроз со стороны администратора, перспектива применения квантово-устойчивых примитивов на основе задач теории решеток.

Ключевые слова: криптографический контроль доступа, эллиптические кривые, изогении, криптография

Источник финансирования: Исследование выполнено при финансовой поддержке Минцифры России в рамках научного проекта № 12/21-к (грант ИБ).

Ссылка для цитирования: Ярмач А.В. Разработка схемы контроля доступа к данным на основе иерархии ролей с использованием постквантовых математических преобразований // Труды учебных заведений связи. 2022. Т. 8. № 4. С. 119–129. DOI:10.31854/1813-324X-2022-8-4-119-129

Post-Quantum Cryptographic Access Control Based on Hierarchical RBAC Model

Анастасия Ярмач, yarmak.av@ibks.spbstu.ru

Peter the Great St. Petersburg Polytechnic University,
St. Petersburg, 195251, Russian Federation

Abstract: The paper considers the isogeny-based cryptographically enforced data access control scheme CSIDH-HRBAC for untrusted cloud. CSIDH-HRBAC is based on a role-based access control model with support for a role hierarchy system. The proposed scheme implies the presence of a trusted party that manages cryptographic keys associated with users, roles, files. The basic procedures for gaining access to data, revoking access rights, adding new entities and updating parameters are given. Typical scenarios of attacks on the proposed scheme are considered, including role substitution, collusion by participants to compute the parent role key, attempt to access data after role revocation from user. To evaluate the

performance of cryptographic operations, the simulation of the basic procedures was performed. The advantages and limitations of the CSIDH-HRBAC scheme are discussed. In particular, the need for protection against threats from the administrator, the prospect of using lattice-based post-quantum cryptographic primitives is noted.

Keywords: cryptographic access control, elliptic curves, isogeny, cryptography

Funding: the reported study was funded by Ministry of Digital Development, Communications and Mass Media of the Russian Federation, project number 12/21-k (grant on Information Security).

For citation: Yarmak A. Post-Quantum Cryptographic Access Control Based on Hierarchical RBAC Model. *Proc. of Telecom. Universities*. 2022;8(4):119–129. (in Russ.) DOI:10.31854/1813-324X-2022-8-4-119-129

Введение

Современные крупномасштабные системы представляют собой класс сложных систем, состоящих из взаимодействующих территориально-распределенных компонентов, построенных на базе технологий Интернета вещей, промышленного Интернета вещей, беспроводных сенсорных сетей и т. п. Большое число узлов системы, их распределенность и избыточность, разнородность вычислительных возможностей и ролей устройств, динамическая топология сети – все эти аспекты накладывают ограничения на применение традиционных способов обеспечения кибербезопасности [1–3].

Ключевыми факторами в развитии систем управления крупномасштабными объектами такого типа представляются, во-первых, переход к групповой, многоадресной передаче данных, обеспечивающей возможность одновременной рассылки информации устройствам, входящим в некоторую группу (групповое взаимодействие узлов), и во-вторых, использование принципа многоуровневого, многослойного и стратифицированного описания архитектуры [4] с введенным отношением вертикальной соподчиненности подсистем.

С распространением облачных технологий многие организации перешли на парадигму аутсорсинга хранения и обработки данных. Появление новой сущности, отвечающей, в том числе, за соблюдение политики управления доступом, ведет к возникновению новых угроз безопасности, так как провайдер облачных услуг может просматривать данные независимо от заданных владельцем прав доступа.

Таким образом, актуальной является задача защиты информации от несанкционированного доступа при ее обработке и хранении в облачном хранилище. Данный аспект стал причиной возросшего интереса к концепции криптографического контроля доступа, которая позволяет обеспечить защиту хранимых в облаке данных с помощью криптографических преобразований, а разграничение доступа к информации осуществлять путем управления соответствующими криптографическими ключами.

1. Способы организации криптографического контроля доступа

Основная проблематика, возникающая при обеспечении контроля доступа к данным в облачном хранилище, включает в себя:

- защиту от угроз, связанных с недоверенным облачным провайдером;
- обеспечение динамического управления доступом, снижение вычислительных и временных затрат при изменении политики доступа к данным;
- учет специфики крупномасштабных систем при реализации управления доступом к данным, в частности иерархической структуры, большого количества пользователей.

Как показано на рисунке 1, в качестве характеристик схем криптографического контроля доступа можно указать следующие:

- возможность интеграции с классическими моделями разграничения доступа;
- используемая криптографическая схема;
- математический аппарат, а также вычислительно сложные задачи, положенные в основу безопасности криптографической схемы;
- рассматриваемые угрозы, от которых обеспечивается защита.



Рис. 1. Характеристики схем криптографического контроля доступа

Fig. 1. Parameters of Cryptographic Access Control Schemes

В настоящий момент известны решения, основанные на мандатной [5] и избирательной [6] моделях контроля доступа. Шифрование на основе атрибутов представляется «криптографическим аналогом» модели разграничения доступа на основе атрибутов [7]. Однако большинство схем построено на базе ролевой модели управления доступом [8–10], что обусловлено ее распространением в больших организациях и облачных платформах [11]. Поэтому представляется обоснованной разработка схемы криптографического контроля доступа, совместимая с моделью разграничения доступа на основе функционально-ролевых отношений.

С точки зрения стойкости рассматриваемых схем криптографического контроля доступа, большинство конструкций используют предположения о сложности задач разложения числа на множители, дискретного логарифмирования, билинейной задачи Диффи – Хеллмана. Данные задачи не позволяют строить квантово-устойчивые конструкции, т. е. обеспечить защиту от нарушителя, располагающего квантовой вычислительной моделью. Из работ, посвященных постквантовым схемам, известны основанные на решетках [12], однако они предполагают использование атрибутной модели контроля доступа.

Среди рассматриваемых решений на основе ролевой модели схема [10] обеспечивает защиту в том числе от угрозы со стороны администратора, что достигается за счет аппаратной технологии Intel-SGX, которая накладывает ограничения на используемую инфраструктуру. Решение CRYPT-DAC [8] в этом смысле является более универсальным, однако предполагает доверие к администратору, осуществляющему управление криптографическими ключами. В качестве криптографической схемы используется гибридное шифрование, что позволяет реализовать ее с помощью существующей криптосистемы с открытым ключом. Однако в CRYPT-DAC не используются постквантовые математические преобразования.

Для учета специфики крупномасштабных систем в качестве основы можно использовать модификацию ролевой политики разграничения доступа, предусматривающую иерархическую систему ролей и являющейся наиболее близкой к реальным организационно-технологическим системам [13]. Предлагаемая схема CSIDH-HRBAC криптографического контроля доступа является развитием работы [14], где в качестве математического аппарата использовались изогении эллиптических кривых. Несмотря на то, что изогении позволяют строить гибкие протоколы постквантовой криптографии, ориентированные на применение в масштабируемых и динамических средах, в работе [14] используется SIDH-конструкция, которая на сегодняшний день счита-

ется уязвимой, а также не учитывает иерархию ролей, как и CRYPT-DAC [8], положенная в ее основу. Таким образом, основное отличие схемы CSIDH-HRBAC состоит в использовании квантово-устойчивой CSIDH-конструкции на изогениях, а также учета отношения иерархии на множестве ролей.

2. Предлагаемая схема криптографического контроля доступа CSIDH-HRBAC

Эллиптические кривые являются объектом изучения алгебраической геометрии, нашедшие свое прикладное применение при построении асимметричных криптографических систем, в том числе постквантовой криптографии.

Изогения $\varphi: E_1(K) \rightarrow E_2(K)$ эллиптических кривых E_1 и E_2 – это рациональное отображение, сохраняющее неподвижной бесконечно удаленную точку: $\varphi(P_\infty) = P_\infty$ [15]:

$$\varphi(x, y) = (r_1(x), r_2(x)y),$$

где $r_1(x) = \frac{p_1(x)}{q_1(x)}$, $r_2(x) = \frac{p_2(x)}{q_2(x)}$ – рациональные функции с взаимно простым числителем и знаменателем; $\deg \varphi = \max\{\deg p_1(x), \deg q_1(x)\}$ – степень изогении.

Задача поиска изогении $\varphi: E_1 \rightarrow E_2$ подразумевает вычисление идеала $\alpha \in Cl(O_D)$ из группы классов идеалов квадратичного порядка O_D , для которого выполняется условие: $E_2 = [\alpha] * E_1$, где E_1 и E_2 – известные эллиптические кривые с $\text{End}(E_1) \cong \cong O_D \cong \text{End}(E_2)$.

В общем случае, криптосистемы с открытым ключом на изогениях эллиптических кривых можно разделить на три семейства – CRS-, SIDH-, CSIDH-схемы [16]. Преимущества представителей последних (высокая скорость вычислений, т. к. используемые степени изогении фиксированы и, как правило, равны 2 и 3, небольшая по сравнению с другими постквантовыми криптосистемами длина параметров) обусловили их широкое применение при построении криптосистем на изогениях.

Однако, как показано в таблице 1, в настоящий момент такой подход не рекомендуется использовать на практике, так как атака, опубликованная в работах [17–18], позволяет решить задачу поиска изогений за полиномиальное время. В основу атаки легла теорема Кани, которую возможно применить за счет особенностей SIDH-схем, в которых между абонентами пересылаются вспомогательные точки (образы точек, являющихся образующими подгруппы группы кручения), а также известна степень секретной изогении. CRS- и CSIDH-схемы построены по другим принципам, т. е. данная атака для них не применима. Поэтому наиболее перспективным представляется подход на основе CSIDH [19], который обеспечивает субэкспоненциальный уровень сложности решения задач поиска изогений и, в то

же время, позволяет уменьшить время вычисления изогении и сократить длину параметров по сравнению с CRS-схемами.

ТАБЛИЦА 1. Сложность решения задачи поиска изогении для различных конструкций

TABLE 1. Complexity of Isogeny Problem for Different Schemes

Сложность решения задачи поиска изогении			
	CRS-схемы	SIDH-схемы	CSIDH-схемы
A	$O(p^{1/4})$	$O(l^8 \log N + \log^2 N)$	$O(p^{1/4})$
B	$L_p[\frac{1}{2}, \sqrt{2}]$	—	$L_p[\frac{1}{2}, \sqrt{2}]$

Условные обозначения: A – классическая вычислительная модель; B – квантовая вычислительная модель; p – характеристика поля; N – степень изогении; l – наибольший простой делитель N .

Пусть $HRBAC = \langle U, R, P, C, F_{PR}, F_{UR}, F_{RR} \rangle$ – модель контроля доступа с иерархической системой ролей, где:

U – множество пользователей;

R – множество ролей;

$P \subseteq \text{Files} \times OP$ – множество прав доступа;

Files – множество файлов;

$OP = \{\text{read}, \text{write}\}$ – операции над файлами;

C – множество сеансов работы пользователей с системой;

$F_{PR} \subseteq P \times R$ – отношение, задающее связь роли и соответствующих прав;

$F_{UR} \subseteq U \times R$ – отношение, определяющее связь пользователя и роли;

$F_{RR} = \{(r_j, r_i) | r_j, r_i \in R \text{ и } r_j \leq r_i\}$ – отношение частичного порядка на множестве R , определяющее иерархию ролей (если справедливо $r_j \leq r_i$, то роль r_i наследует все права доступа роли r_j).

Также вводятся следующие вспомогательные функции [13], необходимые для управления доступом в системе:

– $f_{\text{user}}: C \rightarrow U$, сопоставляющая сеансу работы с системой пользователя, осуществляющего данный сеанс;

– $f_{\text{roles}}: C \rightarrow R$, сопоставляющая набор ролей, доступных пользователю, осуществляющему данный сеанс, с учетом иерархически подчиненных ролей.

Также подразумевается использование следующих криптографических алгоритмов [8]:

– $\text{Enc}_k^{\text{sym}} / \text{Dec}_k^{\text{sym}}$ – алгоритмы шифрования и расшифрования данных на ключе k с помощью симметричного шифра;

– $\text{Enc}_{ek}^{\text{pub}} / \text{Dec}_{dk}^{\text{pub}}$ – алгоритмы шифрования данных на открытом ключе pk и расшифрования данных на закрытом ключе dk с помощью асимметричного шифра;

– $\text{Sign}_{sk} / \text{Verify}_{vk}$ – алгоритмы формирования подписи и проверки подписи с помощью ключей sk и vk соответственно.

В качестве криптосистемы с открытым ключом, необходимой для шифрования ключа dk_r роли r и ключа k_f , предлагается использовать схему шифрования Эль-Гамала на изогениях. В качестве протокола подписи используется подпись CSI-FiSh [20].

Криптографическими ключами управляет администратор организации в соответствии с ролевой политикой доступа. Криптографический контроль доступа осуществляется путем назначения сущностям ролевой политики доступа соответствующих криптографических ключей, а также генерации кортежей, определяющих связь между этими сущностями. Их описание представлено в таблице 2. Облачный провайдер отвечает за хранение файлов пользователей. Предполагается, что перед загрузкой данных в облако все файлы шифруются. Пользователи могут осуществлять загрузку данных из облака, а также вносить изменения в файлы согласно заданным для их роли правам.

ТАБЛИЦА 2. Криптографические ключи сущностей в схеме CSIDH-HRBAC

TABLE 2. Cryptographic Keys for CSIDH-HRBAC

Сущность	Криптографические ключи	Описание
Пользователь $u \in U$	1) Пара ключей (ek_u, dk_u) для чтения файлов 2) Пара ключей (sk_u, vk_u) для записи в файлы	Необходимы для чтения и записи в файлы, хранящиеся у облачного провайдера
Роль $r \in R$	Пара ключей (ek_r, dk_r) для доступа к файлам	Определяют доступ к файлам для заданной роли
Файл $f \in F$	Каждому файлу f соответствует ключ k_f симметричного алгоритма	Используется для шифрования файлов, хранящихся в облаке
Кортеж $fk_{rf} \in FK$ (связь ключа роли и прав доступа)	Если роли r разрешена операция op над файлом f , то существует кортеж: $fk_{rf} = (r, (f, op), \text{Enc}_{ek_r}^{\text{pub}}(k_f))$	Ключ роли и права доступа связаны через кортежи из FK . В каждом кортеже хранится симметричный ключ k_f , зашифрованный на открытом ключе ek_r роли r
Кортеж $rk_{ur} \in RK$ (связь ключа пользователя и ключа роли)	Если пользователю u была выдана роль r , то существует кортеж: $rk_{ur} = (u, r, \text{Enc}_{ek_u}^{\text{pub}}(dk_r))$	Ключи пользователя и роли связаны через кортежи из RK . В таком кортеже хранится закрытый ключ dk_r роли r , зашифрованный на открытом ключе ek_u пользователя u
Кортеж $rr_{ij} \in RR$ (связь ключей ролей)	Если r_j – прямой потомок роли r_i , то существует кортеж: $rr_{ij} = (E_{r_j}^{\text{id}}, y_{ij})$	Открытая информация, необходимая для вычисления ключа подчиненной роли

В рамках предлагаемой схемы криптографического контроля доступа поддерживаются операции генерации ключей, получения доступа на чтение и запись, добавления новых сущностей, смены ключей, лишения прав доступа.

2.1. Инициализация параметров схемы криптографического контроля доступа CSIDH-HRBAC

Для генерации параметров схемы администратору необходимо выполнить следующие действия.

- 1) Сгенерировать характеристику поля:
 $p = 4l_1l_2 \dots l_m \pm 1$, $l_1, l_2, \dots, l_n$ – малые простые.
- 2) Сгенерировать суперсингулярную эллиптическую кривую $E_0(\mathbb{F}_p): y^2 = x^3 + x$ с числом точек $\#E_0(\mathbb{F}_p) = p + 1 = 4l_1l_2 \dots l_n$ и кольцом эндоморфизмов $\text{End}(E_0) \cong O_D$.
- Группа классов $Cl(O_D) = \langle g \rangle$ – циклическая, $\#Cl(O_D) = N$.
- 3) Сгенерировать случайное значение $\alpha_{pub} \leftarrow \mathbb{Z}_N$ и вычислить идеал $[\alpha_{pub}] = g^{\alpha_{pub}}$. Определить изогению $\varphi_0^{pub}: E_0 \rightarrow E_0^{pub}$, $E_0^{pub} = [\alpha_{pub}] * E_0$.
- 4) Сгенерировать случайное значение $\alpha_{sign} \leftarrow \mathbb{Z}_N$ и вычислить идеал $[\alpha_{sign}] = g^{\alpha_{sign}}$. Определить изогению $\varphi_0^{sign}: E_0 \rightarrow E_0^{sign}$, $E_0^{sign} = [\alpha_{sign}] * E_0$.
- 5) Выбрать параметры S, t для протокола цифровой подписи CSI-FiSh на изогениях.
- 6) Сгенерировать случайное значение $\alpha_{roles} \leftarrow \mathbb{Z}_N$ и вычислить идеал $[\alpha_{roles}] = g^{\alpha_{roles}}$. Определить изогению $\varphi_0^{roles}: E_0 \rightarrow E_0^{roles}$, $E_0^{roles} = [\alpha_{roles}] * E_0$.
- 7) Сгенерировать случайное значение $\alpha_{id} \leftarrow \mathbb{Z}_N$ и вычислить идеал $[\alpha_{id}] = g^{\alpha_{id}}$. Определить изогению $\varphi_0^{id}: E_0 \rightarrow E_0^{id}$, $E_0^{id} = [\alpha_{id}] * E_0$. Для каждой роли $r_i \in R$ вычислить кривую-идентификатор роли: $\varphi_{r_i}^{id}: E_0^{id} \rightarrow E_{r_i}^{pub}$, $E_{r_i}^{id} = [\alpha_{r_i}^{id}] * E_0^{id}$ путем задания случайного идеала $\alpha_{r_i}^{id}$.
- 8) Определить криптографическую хэш-функцию $H: \{0,1\}^* \rightarrow \{0,1\}^p$.

Открытыми параметрами схемы CSIDH-HRBAC являются: $p, \{l_i\}, E_0, E_0^{pub}, E_0^{sign}, E_0^{id}, \{E_{r_j}^{id}\}, S, t, E_0^{roles}, H$.

2.2. Генерация ключей

Генерация ключей k_f , используемых для шифрования файлов, выполняется согласно требованиям, заданным для выбранного симметричного алгоритма шифрования данных $\text{Enc}_k^{\text{sym}}/\text{Dec}_k^{\text{sym}}$.

Генерация ключей пользователей для чтения файлов

Для генерации ключей (ek_u, dk_u) пользователя $u \in U$ администратору необходимо выполнить следующие этапы.

Этап 1. Генерация секретной изогении. Выбрать случайное значение $g_u \leftarrow \mathbb{Z}_N$ и вычислить секретную изогению $\varphi_u^{pub}: E_0^{pub} \rightarrow E_u^{pub}$, $E_u^{pub} = [g_u] * E_0^{pub}$.

Этап 2. Назначение ключа пользователю. Установить для u пару (ek_u, dk_u) открытый ключ/закрытый ключ следующим образом:

$$ek_u = E_u^{pub}, dk_u = g_u.$$

Генерация ключей пользователей для записи в файлы

Для генерации ключей (sk_u, vk_u) пользователя $u \in U$ администратору необходимо выполнить процедуру согласно [20].

- 1) Для $i = 1, \dots, S - 1$:
 – сгенерировать случайный идеал $[g_u^{(i)}]$;
 – вычислить изогенную кривую:

$$E_{u,i}^{sign} = [g_u^{(i)}] * E_0^{sign}.$$

2) Установить для u пару (sk_u, vk_u) ключ подписи и ключ проверки подписи следующим образом:

$$sk_u = ([g_u^{(1)}], \dots, [g_u^{(S-1)}]), vk_u = (E_{u,1}^{sign}, \dots, E_{u,S-1}^{sign}).$$

Генерация ключей роли

Иерархия ролей предполагает возможность вычисления закрытого ключа dk_{r_j} роли r_j пользователями с ролью r_i , если $r_j \leq r_i$.

Самый простой способ решения данной задачи – хранение для каждого пользователя u_k с ролью r_i помимо кортежа:

$$rk_{u_k r_i} = \left(u_k, r_i, \text{Enc}_{ek_{u_k}}^{\text{pub}}(dk_{r_i}) \right)$$

кортежей:

$$rk_{u_k r_j} = \left(u_k, r_j, \text{Enc}_{ek_{u_k}}^{\text{pub}}(dk_{r_j}) \right) \text{ для } \forall r_j \leq r_i.$$

Однако это требует значительного объема памяти и осложняет отзыв ключа роли, имеющей много подчиненных ролей.

Для этого предлагается модифицировать схему управления ключами [21], что позволит пользователям роли r_i на основе своего ключа dk_{r_i} и вспомогательной информации вычислять ключ dk_{r_j} подчиненной роли r_j . Для реализации данного механизма можно использовать связь секретной изогении родительской роли с кривой-идентификатором подчиненной роли. Тогда для генерации ключей (ek_{r_i}, dk_{r_i}) роли $r_i \in R$ администратору необходимо реализовать этапы.

Этап 1. Генерация ключа роли. Для роли r_i выбрать случайное значение $g_{r_i} \leftarrow \mathbb{Z}_N$ и положить $(ek_{r_i}, dk_{r_i}) \leftarrow (E_{r_i}, g_{r_i})$, где $\varphi_{r_i}: E_0^{roles} \rightarrow E_{r_i}$, $E_{r_i} = [g_{r_i}] * E_0^{roles}$.

Этап 2. Задание связи с ключами подчиненных ролей. Для каждой роли r_j : $r_j \leq r_i$, являющейся прямым потомком роли r_i , вычислить открытое значение: $y_{ij} = dk_{r_j} \oplus H(j(\varphi_{r_i}(E_{r_j}^{id})))$, где $j(E)$ – это j -инвариант кривой E ; φ_{r_i} – изогения, связывающая открытый ключ роли r_j с кривой-идентификатором роли r_i , т. е. $\varphi_{r_i}(E_{r_j}^{id}) = [g_{r_i}] * E_{r_j}^{id}$, как показано на рисунке 2.

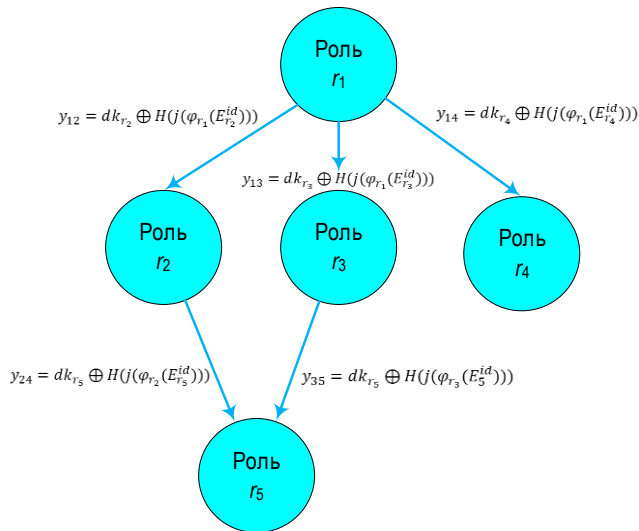


Рис. 2. Иерархия ролей и связь криптографических ключей
Fig. 2. Role-Key Hierarchy in CSIDH-HRBAC

2.3. Получение доступа на чтение

Если пользователь u с ролью r_i хочет получить доступ к файлу f , ему необходимо выполнить следующие шаги.

Шаг 1. Загрузить $rk_{ur_i} = (u, r_i, \text{Enc}_{ek_u}^{\text{pub}}(dk_{r_i}))$ кортеж, содержащий зашифрованный на ключе ek_u пользователя u закрытый ключ dk_{r_i} роли r_i .

Шаг 2. Вычислить $dk_{r_i} \leftarrow \text{Dec}_{dk_u}^{\text{pub}}(dk_{r_i})$.

Шаг 3. Если $((f, \text{read}), r_i) \in F_{PR}$, то загрузить $fk_{r_i f} = (r_i, (f, \text{read}), \text{Enc}_{ek_{r_i}}^{\text{pub}}(k_f))$.

Шаг 4. Вычислить $k_f \leftarrow \text{Dec}_{dk_{r_i}}^{\text{pub}}(k_f)$ и перейти на шаг 8.

Шаг 5. Если $\exists r_j: ((f, \text{read}), r_j) \in F_{PR} \wedge r_j \leq r_i$, то, пока $r_i \neq r_j$, выполнять:

- загрузить $rr_{ik} = (E_{r_k}^{id}, y_{ik})$, где r_k – прямой потомок r_i ;
- вычислить $dk_{r_k} = y_{ik} \oplus H(j(\varphi_{r_i}(E_{r_k}^{id})))$;
- положить $r_i \leftarrow r_k$.

Шаг 6. Загрузить $fk_{r_j f} = (r_j, (f, \text{read}), \text{Enc}_{ek_{r_j}}^{\text{pub}}(k_f))$.

Шаг 7. Расшифровать ключ k_f , используя закрытый ключ роли dk_{r_j} .

Шаг 8. Загрузить зашифрованный файл:

$$F = \text{Enc}_{k_f}^{\text{sym}}(f).$$

Шаг 9. Расшифровать файл $f \leftarrow \text{Dec}_{k_f}^{\text{sym}}(F)$.

Рисунок 3 иллюстрирует последовательность действий, необходимых для получения доступа на чтение.

2.4. Получение доступа на запись

Если пользователь u с ролью r_i хочет осуществить запись в файл f , ему необходимо выполнить следующие действия.

1) Выполнить шаги 1–9 алгоритма получения доступа на чтение (п. 2.3) относительно прав (f, write) .

2) Загрузить в облачное хранилище зашифрованный файл $F' = \text{Enc}_{k_f}^{\text{sym}}(f')$, где f' – это новое содержимое файла f .

3) Сформировать подпись $\sigma = (b_1, \dots, b_t, c_1, \dots, c_t)$ файла F' согласно алгоритму Sign_{sk_u} протокола CSi-FiSh.

4) Отправить значение σ администратору.

Для верификации действий пользователя администратор проверяет, что для:

$$u = f_{\text{user}}(c), r = f_{\text{roles}}(c): \exists (u, r) \in F_{UR} \wedge (r, p = (f, \text{write})) \in F_{PR};$$

В случае успешного выполнения администратор запускает алгоритм Verify_{vk_u} проверки подписи файла F' согласно протоколу CSi-FiSh. Если подпись верна, то файл F заменяется файлом F' . В противном случае файл F' удаляется.

2.5. Лишение прав доступа

При отзыве у пользователя u роли r необходимо выполнить генерацию новых ключей роли и шифрования файлов, а также обновить кортежи RK и FK . Для этого требуется выполнить следующие шаги.

Шаг 1. Сгенерировать новую ключевую пару для роли (ek'_r, dk'_r) .

Шаг 2. Удалить кортеж $rk_{ur} = (u, r, \text{Enc}_{ek_u}^{\text{pub}}(dk_r))$, связывающий пользователя u и роль r .

Шаг 3. Для каждого пользователя $u' \neq u$ с ролью r выполнить замену значений в кортеже rk_{ur} с $(u', r, \text{Enc}_{ek_u}^{\text{pub}}(dk_r))$ на $(u', r, \text{Enc}_{ek_{u'}}^{\text{pub}}(dk'_r))$.

Шаг 4. Для каждого файла f , доступного для r :

- расшифровать файл f и зашифровать его с помощью нового ключа k'_f ;

– выполнить замену значений в кортеже $fk_{r f}$ с $(r, (f, \text{op}), \text{Enc}_{ek_r}^{\text{pub}}(k_f))$ на $(r, (f, \text{op}), \text{Enc}_{ek_{r'}}^{\text{pub}}(k'_f))$.

Шаг 5. Выполнить замену значений в таблице RR для всех ролей, связанных отношением подчиненности или доминирования, используя новую кривую-идентификатор $\tilde{E}_r^{id}$ и обновленные значения $dk_{r_j} \oplus H(j(\varphi'_r(E_r^{id})))$ для всех r_j , являющихся потомками r , и $dk'_r \oplus H(j(\varphi_{r_i}(\tilde{E}_r^{id})))$ для всех r_i , являющихся родительскими для роли r .

Процедура отзыва ключа роли выполняется аналогичным образом, за исключением шага 2, связанного с удалением кортежа, ассоциированного с конкретным пользователем. Добавление новых сущностей и обновление ключей сводятся к операциям генерации новых криптографических ключей и замене или добавлению соответствующих значений в таблицы RK, FK, RR .

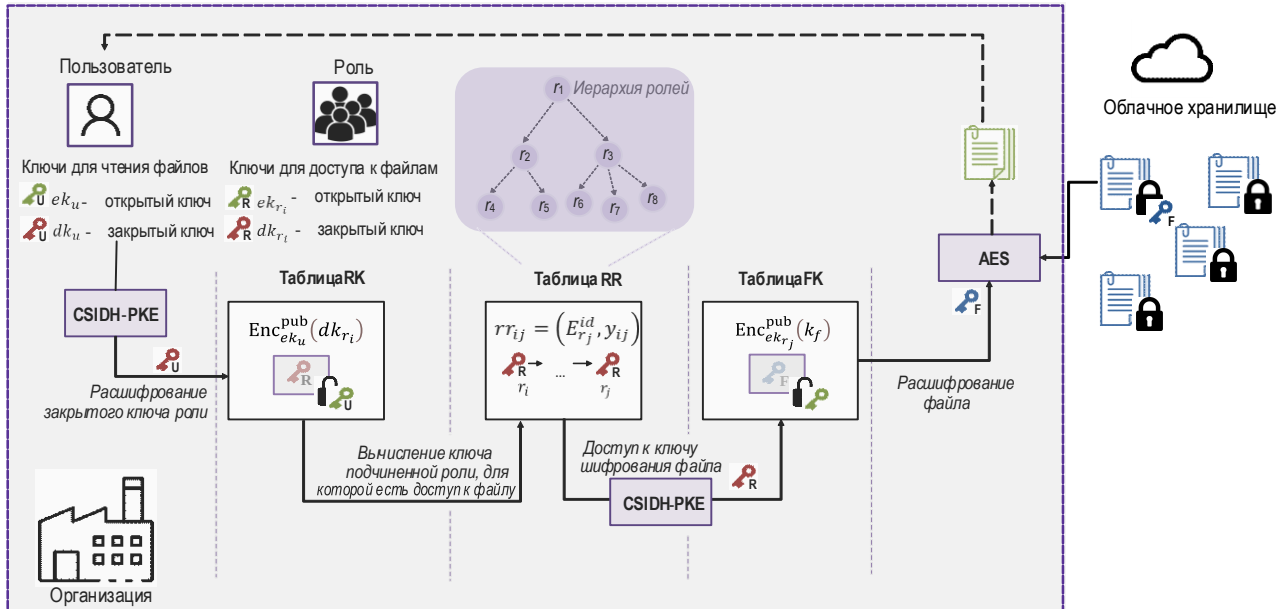


Рис. 3. Получение доступа на чтение

Fig. 3. Read Access in CSIDH-HRBAC

3. Анализ схемы CSIDH-HRBAC

Анализ безопасности включал в себя рассмотрение возможных сценариев атак на предлагаемую схему криптографического контроля доступа.

Сценарий 1. Утечка данных из облака. При реализации данного сценария нарушителю становятся доступны файлы, расположенные в облачном хранилище. В этом случае задача получения доступа к содержимому некоторого файла F сводится к задаче дешифрования шифртекста, т. е. взлома симметричного алгоритма шифрования. Если нарушитель имеет доступ к таблицам RK, FK, RR , то есть знает шифртекст $\text{Enc}_{ek_r}^{\text{pub}}(k_f)$ из кортежа fk_{r_f} , то для получения ключа шифрования файла ему необходимо располагать закрытым ключом dk_r роли r или закрытым ключом dk_u пользователя u , имеющего эту роль. При отсутствии знания о ключах нарушителю необходимо решить задачу поиска изогении φ_u^{pub} или φ_r , которая считается вычислительно сложной.

Сценарий 2. Подмена роли. В данном сценарии нарушителем является пользователь системы с ролью r_j , его цель – выполнить операцию чтения файла или записи в файл, которая доступна для пользователей некоторой роли r_i . Если роли свя-

заны отношением $r_j \leq r_i$, то данное действие подразумевает вычисление закрытого ключа родительской роли. Зная ключи своей роли (ek_r, dk_r) и значение $y_{ij} = dk_{r_j} \oplus H(j(\varphi_{r_i}(E_{r_j}^{id})))$, нарушитель может найти значение $H(j(\varphi_{r_i}(E_{r_j}^{id})))$, однако для нахождения секретной изогении φ_{r_i} (которая соответствует закрытому ключу роли r_i) ему необходимо решить задачу обращения криптографической хэш-функции H , т. е. найти кривую $\varphi_{r_i}(E_{r_j}^{id})$, после чего вскрытие закрытого ключа роли r_i сводится к задаче поиска изогении между кривыми $\varphi_{r_i}(E_{r_j}^{id})$ и $E_{r_j}^{id}$, что, с учетом предположений, имеет субэкспоненциальную сложность для квантового компьютера.

Сценарий 3. Повышение привилегий. Данный сценарий подразумевает попытку пользователя системы выполнить запись в файл, доступный ему только для чтения. В таком случае данное действие будет обнаружено администратором путем анализа политики разграничения прав доступа. Поэтому для прохождения проверки нарушителю необходимо модифицировать соответствующий кортеж в таблице FK .

Сценарий 4. Сговор участников. Пусть имеется сговор пользователей с ролями r_2, r_3 , подчиняющимися одной родительской роли r_1 , с целью восстановления ключа dk_{r_1} этой роли. Обладая общеизвестной информацией $rr_{12} = (E_{r_2}^{id}, y_{12})$, $rr_{13} = (E_{r_3}^{id}, y_{13})$ из таблицы RR , они могут восстановить значения $H(j(\varphi_{r_1}(E_{r_2}^{id})))$ и $H(j(\varphi_{r_1}(E_{r_3}^{id})))$. Тогда вскрытие ключа сводится к реализации сценария 2.

Сценарий 5. Попытка доступа к данным после отзыва участника. Пусть пользователь u пытается получить доступ к файлу f после отзыва у него роли r . Реализация данного сценария аналогична сценарию 1, так как в процессе отзыва участника осуществляется регенерация ключей роли и ключей шифрования данных.

Для моделирования работы схемы использовалась библиотека [22], реализующая базовые операции вычисления изогений, а также позволяющая вычислить подпись на изогениях. В качестве кривых используются кривые в форме Монтгомери, поэтому для задания эллиптической кривой достаточно указать коэффициент A в уравнении кривой $E_0(\mathbb{F}_p): y^2 = x^3 + Ax^2 + x$. Это позволяет избавиться от процедуры вычисления j -инварианта кривой при подсчете элементов из таблицы RR .

Характеристика поля имеет длину 512 бит и задается следующим образом: $p = 4 \cdot 3 \cdot 5 \cdot 7 \cdot \dots \cdot 587 - 1$. Длина ключей (ek_u, dk_u) для чтения составляет 64 и 32 байта, соответственно, ключи (sk_u, vk_u) для записи в файлы имеют длину 16 байт и 16 Кб. В качестве хэш-функции использовался алгоритм Кеска-256, симметричный шифр – AES-256. В таблице 3 представлены результаты тестирования процедуры инициализации параметров схемы. Время генерации параметров зависит от числа ролей, определяемых ролевой политикой доступа, так как для каждой роли необходимо сгенерировать кривую-идентификатор роли. Данный этап может быть распараллелен путем использования нескольких вычислителей, каждый из которых будет взаимодействовать с своим пулом ролей.

Для добавления пользователя в систему необходимо выполнить генерацию ключей для чтения и записи в файл. При этом самым трудоемким этапом является генерация пары ключей для протокола подписи на изогениях. Время, необходимое для данных вычислений, определяется параметром S : при малом значении S процедура генерации параметров осуществляется быстрее, длина открытого ключа минимальна (128 байт), однако время формирования и проверки подписи значительно увеличивается.

При большом значении $S = 2^{15}$ время генерации может достигать нескольких минут, размер открытого ключа равен 2 Мб, но процедуры подписи

сообщения и проверки подписи выполняются быстрее. При моделировании было выбрано значение $S = 2^8$, при котором общее время добавления пользователя в систему в среднем равно 9,97 с.

Операции назначения пользователю роли и предоставления доступа к файлу подразумевают зашифрование закрытого ключа роли и ключа шифрования файла с помощью схемы на изогениях. Среднее время выполнения этих операций равно 81 мс.

ТАБЛИЦА 3. Время инициализации параметров схемы

TABLE 3. Scheme's Parameters Initialization Time

Число ролей	Время, с
10	0,53
100	3,91
500	18,43
1000	39,24

На рисунках 4 и 5 представлены результаты тестирования, позволяющие оценить время, затрачиваемое только на криптографические операции. В частности, использовалось предположение о том, что каждой роли соответствует 10 пользователей, при этом число связей с другими ролями равно 3.

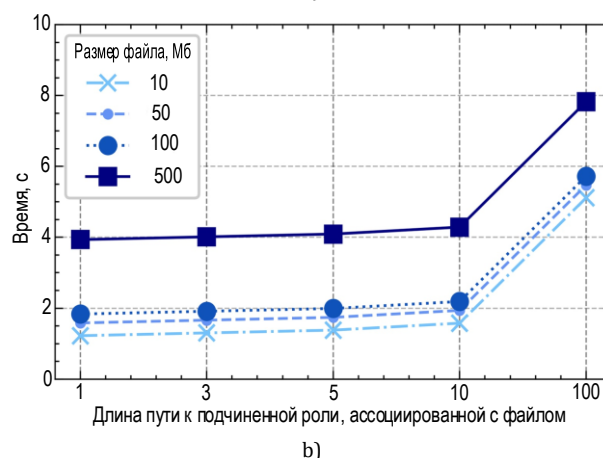
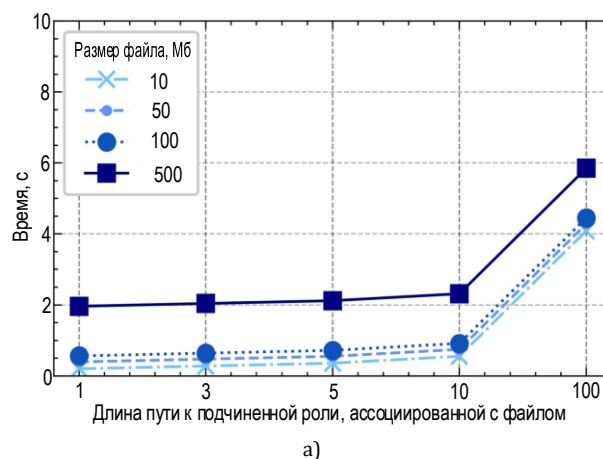


Рис. 4. Результаты тестирования процедур: а) получение доступа на чтение; б) получение доступа на запись в файл

Fig 4. Time for Read Access (a) and Write Access Operations (b)

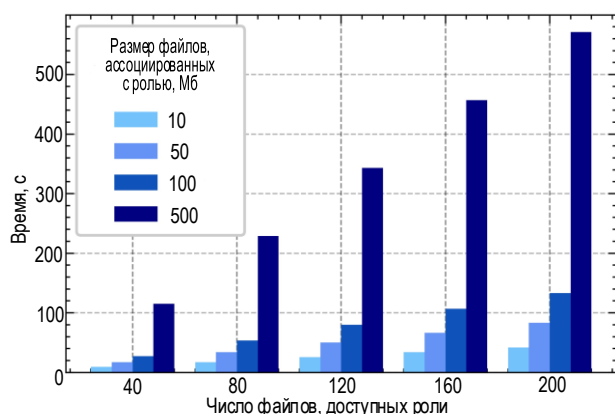


Рис. 5. Результаты тестирования процедуры отзыва роли у пользователя

Fig 5. Time for Revoking Role from User

Как видно из рисунка 4, время выполнения процедуры записи в файл отличается от получения доступа на чтение, что объясняется необходимостью формирования и проверки подписи для верификации вносимых изменений в файл. При доступе к файлу, ассоциированному с подчиненной ролью, пользователю необходимо вычислить закрытый ключ роли. Можно заметить, что данная операция незначительно влияет на скорость выполнения, так как для нахождения ключа роли необходимо рассчитать коэффициент изогнутой кривой, найти значение хэш-функции и выполнить операцию XOR.

При лишении пользователя роли самой затратной, с точки зрения вычислений, является операция обновления ключей шифрования файлов, ассоциированных с данной ролью (т. е. тех, к которым разрешен доступ пользователям, имеющим эту роль). Одним из способов оптимизации является использование повторного шифрования на новом ключе (добавление нового слоя шифрования) вместо операции расшифрования файла и его зашифрования на новом ключе, но в таком случае пользователям необходимо хранить последовательность ключей.

Заключение

В работе представлена схема криптографического контроля доступа CSIDH-HRBAC, основанная на конструкции CRYPT-DAC и применимая для си-

стем, использующих ролевую политику управления доступом к данным. Предложенная схема отличается применением постквантовых математических преобразований для защиты информации, размещенной в недоверенном облачном хранилище, а также с учетом иерархии ролей, который актуален для крупномасштабных систем, имеющих ярко выраженную иерархическую структуру узлов (например, промышленный Интернет вещей, Интернет вещей, интеллектуальные энергосети и др.). Контроль доступа к данным осуществляется за счет использования криптографических алгоритмов и назначения соответствующих ключей, что обеспечивает легкость интеграции.

К преимуществам схемы CSIDH-HRBAC можно отнести отсутствие необходимости в создании и хранении дополнительных кортежей в таблицах FK , RK в случае наличия иерархии ролей (по сравнению с CRYPT-DAC), учет специфики иерархических систем, а также использование квантово-устойчивых примитивов. В качестве ограничений можно отметить следующее: набор прав доступа старших ролей включает только те права, которые не вошли в набор подчиненных ролей; пользователь может принадлежать только одной роли; требуется хранить таблицу RR ; необходимо доверие к администратору, осуществляющему управление криптографическими ключами пользователей.

Дальнейшее направление исследования связано с оптимизацией схемы, в частности, процедур, связанных с лишением прав доступа, а также обеспечением защиты от угрозы со стороны администратора. Также в качестве отдельного направления работы можно отметить использование других квантово-устойчивых примитивов, например, использующих задачи теории решеток, где для задания связи между ключами ролей можно использовать механизм делегирования базиса решетки [23]. В частности, в качестве шифрования можно использовать схему CRYSTALS-Kyber, в качестве цифровой подписи – CRYSTALS-Dilithium, которые являются финалистами конкурса Национального института стандартов и технологий на постквантовые стандарты.

Список источников

1. Krundyshev V., Kalinin M. The Security Risk Analysis Methodology for Smart Network Environments // Proceedings of the International Russian Automation Conference (RusAutoCon, Sochi, Russia, 06–12 September 2020). IEEE, 2020. PP. 437–442. DOI:10.1109/RusAutoCon49822.2020.9208116
2. Ovasapyan T., Moskvina D., Tsvetkov A. Detection of attacks on the Internet of Things based on intelligent analysis of devices functioning indicators // Proceedings of the 13th International Conference on Security of Information and Networks (SIN, Merkez Turkey, 4–7 November 2020). New York: Association for Computing Machinery, 2020. P. 3. DOI: 10.1145/3433174.3433611
3. Александрова Е.Б., Облогина А.Ю., Шкоркина Е.Н. Аутентификация управляющих устройств в сети Интернета вещей с архитектурой граничных вычислений // Проблемы информационной безопасности. Компьютерные системы. 2021. № 2. С. 82–88.
4. Мако Д., Месарович М., Такахара И. Теория иерархических многоуровневых систем. М.: Мир. 1973.

5. Горковенко Е.В. Применение нетрадиционных криптографических преобразований в системах с мандатной политикой управления доступом к информации // Известия Южного федерального университета. Технические науки. 2008. № 8(85). С. 135–141.
6. Di Vimercati S.D.C., Foresti S., Jajodia S., Paraboschi S., Samarati P. Over-encryption: Management of Access Control Evolution on Outsourced Data // Proceedings of the 33rd International Conference on Very Large Data Bases (VLDB, Vienna Austria, 23–27 September 2007). VLDB Endowment Inc., 2007. PP. 123–134.
7. Epishkina A., Zapechnikov S. On Attribute-Based Encryption for Access Control to Multidimensional Data Structures // Proceedings of the First International Early Research Career Enhancement School on Biologically Inspired Cognitive Architectures (BICA) for Young Scientist and Cybersecurity (FIERCES 2017, Moscow, Russia, 1–3 August 2017). Advances in Intelligent Systems and Computing. Vol. 636. Cham: Springer, 2017. PP. 251–256. DOI:10.1007/978-3-319-63940-6_36
8. Qi S., Zheng Y. Crypt-DAC: Cryptographically Enforced Dynamic Access Control in the Cloud // IEEE Transactions on Dependable and Secure Computing. 2019. Vol. 18. Iss. 2. PP. 765–779. DOI:10.1109/TDSC.2019.2908164
9. Chinnnasamy P., Deepalakshmi P. HCAC-EHR: hybrid cryptographic access control for secure EHR retrieval in healthcare cloud // Journal of Ambient Intelligence and Humanized Computing. 2022. Vol. 13. Iss. 2. PP. 1001–1019. DOI:10.1007/s12652-021-02942-2
10. Contiu S., Pires R., Vaucher S., Pasin M., Felber P., Réveillère L. IBBE-SGX: Cryptographic Group Access Control Using Trusted Execution Environments // Proceedings of the 48th Annual IEEE/IFIP International Conference on Dependable Systems and Networks (DSN, Luxembourg, Luxembourg, 25–28 June 2018). IEEE, 2018. PP. 207–218. DOI:10.1109/DSN.2018.00032
11. Punithasurya K., Priya S.J. Analysis of Different Access Control Mechanism in Cloud // International Journal of Applied Information Systems. 2012. Vol. 4. Iss. 2. PP. 34–39. DOI:10.5120/IJAIS12-450660
12. Jemihin Z.B., Tan S.F., Chung G.C. Attribute-Based Encryption in Securing Big Data from Post-Quantum Perspective: A Survey // Cryptography. 2022. Vol. 6. Iss. 3. PP. 40. DOI:10.3390/cryptography6030040
13. Гайдамакин Н.А. Теоретические основы компьютерной безопасности: учебно-методический комплекс. Екатеринбург: Уральский государственный университет им. А.М. Горького, 2008. 2012 с.
14. Крашенинников Э.А., Ярмач А.В., Александрова Е.Б. Контроль доступа к данным облачного хранилища на основе изогений // Методы и технические средства обеспечения безопасности информации. 2022. № 31. С. 139–141.
15. Ростовцев А.Г. Эллиптические кривые в криптографии. Теория и вычислительные алгоритмы. СПб.: НПО «Профессионал», 2010. 364 с.
16. Chenu-de la Morinerie M. Supersingular Group Actions and Post-quantum Key-exchange. DSc Thesis. Paris: Polytechnic Institute of Paris, 2021.
17. Castryck W., Decru T. An efficient key recovery attack on SIDH (preliminary version) // Cryptology ePrint Archive. 2022. P. 2022/975. URL: <https://eprint.iacr.org/2022/975> (Accessed 12th December 2022)
18. Robert D. Breaking SIDH in polynomial time // Cryptology ePrint Archive. 2022. P. 2022/1038. URL: <https://eprint.iacr.org/2022/1038.pdf> (Accessed 12th December 2022)
19. Castryck W., Lange T., Martindale C., Panny L., Renes J. CSIDH: an Efficient Post-Quantum Commutative Group Action // Proceedings of the 24th International Conference on the Theory and Application of Cryptology and Information Security (Brisbane, Australia, 2–6 December 2018). Lecture Notes in Computer Science. Vol. 11274. Cham: Springer, 2018. PP. 395–427. DOI:10.1007/978-3-030-03332-3_15
20. Beullens W., Kleinjung T., Vercauteren F. CSI-FiSh: Efficient Isogeny-Based Signatures Through Class Group Computations // Proceedings of the 25th International Conference on the Theory and Application of Cryptology and Information Security (Kobe, Japan, 8–12 December 2019). Lecture Notes in Computer Science. Vol. 11921. Cham: Springer, 2019. PP. 227–247. DOI:10.1007/978-3-030-34578-5_9
21. Atallah M.J., Blanton M., Fazio N., Friksen K.B. Dynamic and Efficient Key Management for Access Hierarchies // ACM Transactions on Information and System Security. 2009. Vol. 12. Iss. 3. PP. 1–43. DOI:10.1145/1455526.1455531
22. Beullens W. CSI-FiSh // Github repository. 2019. URL: <https://github.com/KULeuven-COSIC/CSI-FiSh> (Accessed 12th December 2022)
23. Agrawal S., Boneh D., Boyen X. Lattice Basis Delegation in Fixed Dimension and Shorter-Ciphertext Hierarchical IBE // Proceedings of the 30th Annual cryptology conference (CRYPTO 2010, Santa Barbara, USA, 15–19 August 2010). Lecture Notes in Computer Science. Vol. 6223. Berlin, Heidelberg: Springer, 2010. PP. 98–115. DOI: 10.1007/978-3-642-14623-7_6

References

1. Krundyshev V., Kalinin M. The Security Risk Analysis Methodology for Smart Network Environments. *Proceedings of the International Russian Automation Conference, RusAutoCon, 06–12 September 2020, Sochi, Russia*. IEEE; 2020. p.437–442. DOI:10.1109/RusAutoCon49822.2020.9208116
2. Ovasapyan T., Moskvina D., Tsvetkov A. Detection of attacks on the Internet of Things based on intelligent analysis of devices functioning indicators. *Proceedings of the 13th International Conference on Security of Information and Networks, SIN, 4–7 November 2020, Merkez Turkey*. New York: Association for Computing Machinery; 2020. p. 3. DOI: 10.1145/3433174.3433611
3. Aleksandrova E.B., Oblogina A.Yu., Shkorkina E.N. Authentication of Intelligent Electronic Devices in IoT Network with the Edge Computing Architecture. *Information Security Problems. Computer Systems*. 2021;2:82–88. (in Russ.)
4. Mesarovic M., Mako D., Takahara Y. Theory of Hierarchical Multilevel Systems. New York, London: Academic Press; 1970. 294 p. (in Italian)
5. Gorkovenko Ye.V. Using of Non-Traditional Cryptographic Transformations in Informational Systems with Mandate Policy of Control Access. *Izvestiya SFedU. Engineering Sciences*. 2008;8(85):135–141. (in Russ.)

6. Di Vimercati S.D.C., Foresti S., Jajodia S., Paraboschi S., Samarati P. Over-encryption: Management of Access Control Evolution on Outsourced Data. *Proceedings of the 33rd International Conference on Very Large Data Bases, VLDB, 23–27 September 2007, Vienna Austria*. VLDB Endowment Inc.; 2007. p.123–134.
7. Epishkina A., Zapechnikov S. On Attribute-Based Encryption for Access Control to Multidimensional Data Structures. *Proceedings of the First International Early Research Career Enhancement School on Biologically Inspired Cognitive Architectures, BICA, for Young Scientist and Cybersecurity, FIERCES 2017, 1–3 August 2017, Moscow, Russia. Advances in Intelligent Systems and Computing, vol. 636*. Cham: Springer; 2017. p.251–256. DOI:10.1007/978-3-319-63940-6_36
8. Qi S., Zheng Y. Crypt-DAC: Cryptographically Enforced Dynamic Access Control in the Cloud. *IEEE Transactions on Dependable and Secure Computing*. 2019;18(2):765–779. DOI:10.1109/TDSC.2019.2908164
9. Chinnnasamy P., Deepalakshmi P. HCAC-EHR: hybrid cryptographic access control for secure EHR retrieval in healthcare cloud. *Journal of Ambient Intelligence and Humanized Computing*. 2022;13(2):1001–1019. DOI: 10.1007/s12652-021-02942-2
10. Contiu S., Pires R., Vaucher S., Pasin M., Felber P., Réveillère L. IBBE-SGX: Cryptographic Group Access Control Using Trusted Execution Environments. *Proceedings of the 48th Annual IEEE/IFIP International Conference on Dependable Systems and Networks, DSN, 25–28 June 2018, Luxembourg, Luxembourg*. IEEE; 2018. p.207–218. DOI:10.1109/DSN.2018.00032
11. Punithasurya K., Priya S.J. Analysis of Different Access Control Mechanism in Cloud. *International Journal of Applied Information Systems*. 2012;4(2):34–39. DOI:10.5120/IJAIS12-450660
12. Jemihin Z. B., Tan S. F., Chung G. C. Attribute-Based Encryption in Securing Big Data from Post-Quantum Perspective: A Survey. *Cryptography*. 2022;6(3):40. DOI:10.3390/cryptography6030040
13. Gaydamakin N. *Theoretical Foundations of Computer Security*. Ekaterinburg: Ural State University A.M. Gorky Publ.; 2008. 2012 p. (in Russ.)
14. Krashenninnikov E.A., Yarmak A.V., Aleksandrova E.B. Isogeny-Based Cloud Storage Data Access Control. *Metody i tekhnicheskiye sredstva obespecheniya bezopasnosti informatsii*. 2022;31:139–141. (in Russ.)
15. Rostovtsev A. *Elliptic Curves in Cryptography. Theory and Computational Algorithms*. St. Petersburg: Professional Publ.; 2010. 364 p. (in Russ.)
16. Chenu-de la Morinerie M. *Supersingular Group Actions and Post-quantum Key-exchange*. DSc Thesis. Paris: Polytechnic Institute of Paris; 2021.
17. Castryck W., Decru T. An efficient key recovery attack on SIDH (preliminary version). *Cryptology ePrint Archive*. P. 2022/975. URL: <https://eprint.iacr.org/2022/975> [Accessed 12th December 2022]
18. Robert D. Breaking SIDH in polynomial time. *Cryptology ePrint Archive*. 2022. P. 2022/1038. URL: <https://eprint.iacr.org/2022/1038.pdf> [Accessed 12th December 2022]
19. Castryck W., Lange T., Martindale C., Panny L., Renes J. CSIDH: an Efficient Post-Quantum Commutative Group Action. *Proceedings of the 24th International Conference on the Theory and Application of Cryptology and Information Security, 2–6 December 2018, Brisbane, Australia. Lecture Notes in Computer Science, vol. 11274*. Cham: Springer; 2018. p.395–427. DOI:10.1007/978-3-030-03332-3_15
20. Beullens W., Kleinjung T., Vercauteren F. CSI-FiSh: Efficient Isogeny-Based Signatures Through Class Group Computations. *Proceedings of the 25th International Conference on the Theory and Application of Cryptology and Information, 8–12 December 2019 Security, Kobe, Japan. Lecture Notes in Computer Science, vol.11921*. Cham: Springer; 2019. p.227–247. DOI:10.1007/978-3-030-34578-5_9
21. Atallah M.J., Blanton M., Fazio N., Frikken K.B. Dynamic and Efficient Key Management for Access Hierarchies. *ACM Transactions on Information and System Security*. 2009;12(3):1–43. DOI:10.1145/1455526.1455531
22. Beullens W. CSI-FiSh. *Github repository*. 2019. URL: <https://github.com/KULeuven-COSIC/CSI-FiSh> [Accessed 12th December 2022]
23. Agrawal S., Boneh D., Boyen X. Lattice Basis Delegation in Fixed Dimension and Shorter-Ciphertext Hierarchical IBE. *Proceedings of the 30th Annual cryptology conference (CRYPTO 2010, Santa Barbara, USA, 15–19 August 2010). Lecture Notes in Computer Science, vol.6223*. Berlin, Heidelberg: Springer; 2010. p.98–115. DOI: 10.1007/978-3-642-14623-7_6

Статья поступила в редакцию 14.11.2022; одобрена после рецензирования 01.12.2022; принята к публикации 06.12.2022.

The article was submitted 14.11.2022; approved after reviewing 01.12.2022; accepted for publication 06.12.2022.

Информация об авторе:

ЯРМАК
Анастасия Викторовна

ассистент Института кибербезопасности и защиты информации Санкт-Петербургского политехнического университета Петра Великого
 <https://orcid.org/0000-0002-7121-6031>

СПбГУТ)))

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

12TH INTERNATIONAL CONFERENCE ON ADVANCED INFOTELECOMMUNICATIONS ICAIT 2023
Международная научно-техническая и научно-методическая конференция
«Актуальные проблемы инфотелекоммуникаций в науке и образовании»



АПИНО
ICAIT

ОСНОВНЫЕ НАУЧНЫЕ НАПРАВЛЕНИЯ:

-  Радиотехнологии связи
-  Инфокоммуникационные сети и системы
-  Информационные системы и технологии
-  Теоретические основы радиоэлектроники и систем связи
-  Цифровая экономика, управление и бизнес-информатика
-  Гуманитарные проблемы информационного пространства
-  Сети связи специального назначения

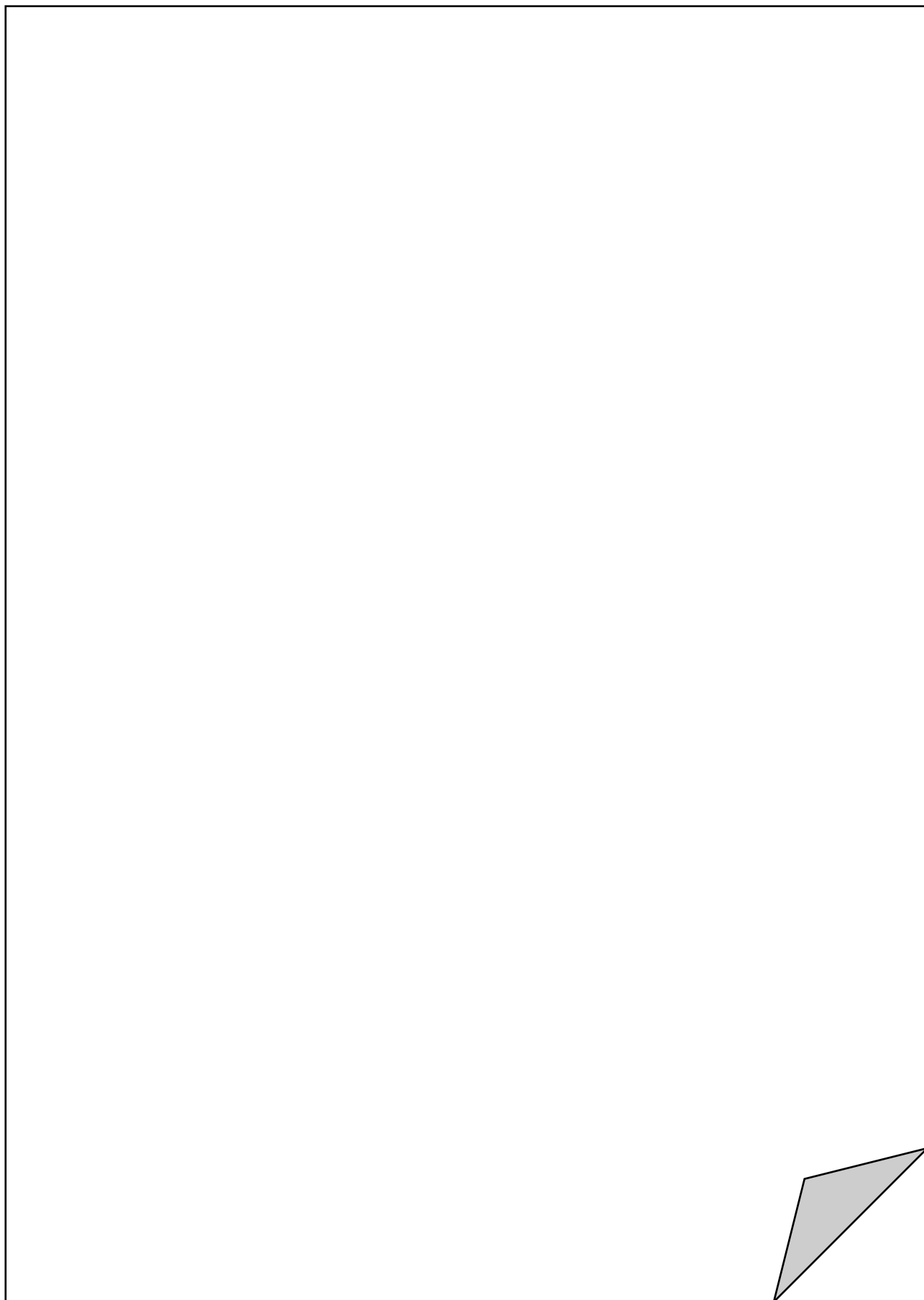
28 ФЕВРАЛЯ –
1 МАРТА 2023

ПОДРОБНОСТИ НА САЙТЕ КОНФЕРЕНЦИИ

APINO.SPBGUT.RU



ДЛЯ ЗАМЕТОК



Выходные данные

Дизайн обложки – ООО «Комильфо»

План издания научной литературы 2022 г., п. 7

Дата выхода в свет	Усл.-печ. л.	Формат	Тираж	Заказ	Свободная цена
27.12.2022	16	60×84 _{1/8}	1000 экз.	№ 1432	

Ответственный редактор **Татарникова И.М.**
Выпускающий редактор **Яшугин Д.Н.**

Адрес СПбГУТ:
193232, Санкт-Петербург, пр. Большевиков, 22/1

Учредитель и издатель:

Федеральное государственное бюджетное образовательное учреждение
высшего образования "Санкт-Петербургский государственный университет
телекоммуникаций им. проф. М.А. Бонч-Бруевича"

E-mail: tuzs@spbgut.ru Web: tuzs.sut.ru VK: vk.com/spbtuzs



Подписной индекс в Объединенном каталоге "ПРЕССА РОССИИ" - 59983