



H&ES RESEARCH

Научно-технический журнал

Scientific and Technical Journal

НАУКОЕМКИЕ ТЕХНОЛОГИИ В КОСМИЧЕСКИХ ИССЛЕДОВАНИЯХ ЗЕМЛИ

HIGH TECHNOLOGIES IN EARTH SPACE RESEARCH

Журнал **H&ES Research** издается с 2009 года, освещает достижения и проблемы российских инфокоммуникаций, внедрение последних достижений отрасли в автоматизированных системах управления, развитие технологий в информационной безопасности, исследования космоса, развитие спутникового телевидения и навигации, исследование Арктики. Особое место в издании уделено результатам научных исследований молодых ученых в области создания новых средств и технологий космических исследований Земли.

Журнал H&ES Research входит в перечень изданий, публикации в которых учитываются Высшей аттестационной комиссией России (ВАК РФ), в систему российского индекса научного цитирования (РИНЦ), а также включен в Международный классификатор периодических изданий.

Тематика публикуемых статей в соответствии с перечнем групп специальностей научных работников по Номенклатуре специальностей:

- 2.2.15 Системы, сети и устройства телекоммуникаций (техн. науки)
- 2.3.1 Системный анализ, управление и обработка информации (техн. науки)
- 2.3.5 Математическое и программное обеспечение вычислительных систем, комплексов и компьютерных сетей (техн. науки)
- 2.3.6 Методы и системы защиты информации, информационная безопасность (техн. науки)
- 2.5.13 Проектирование, конструкция и производство летательных аппаратов (техн. науки)
- 2.5.16 Динамика, баллистика, управление движением летательных аппаратов (техн. науки)

ИНДЕКСИРОВАНИЕ ЖУРНАЛА H&ES RESEARCH

- NEICON • CyberLenika (Open Science) • Google Scholar • OCLC WorldCat • Ulrich's Periodicals Directory • Bielefeld Academic Search Engine (BASE) • eLIBRARY.RU • Registry of Open Access Repositories (ROAR)

Все номера журнала находятся в свободном доступе на сайте журнала www.hes.ru и библиотеке elibrary.ru.

Всем авторам, желающим разместить научную статью в журнале, необходимо оформить ее согласно требованиям и направить материалы на электронную почту: HT-ESResearch@yandex.ru. С требованиями можно ознакомиться на сайте: www.H-ES.ru.

Язык публикаций: русский, английский.
Периодичность выхода – 6 номеров в год.
Свидетельство о регистрации СМИ ПИ № ФС 77-86203 от 27.10.2023
Территория распространения: Российская Федерация, зарубежные страны

Тираж 1000 экз. Цена 1000 руб.
Плата с аспирантов за публикацию рукописи не взимается.

© ООО "ИД Медиа Паблишер", 2024

H&ES Research is published since 2009. The journal covers achievements and problems of the Russian infocommunication, introduction of the last achievements of branch in automated control systems, development of technologies in information security, space researches, development of satellite television and navigation, research of the Arctic. The special place in the edition is given to results of scientific researches of young scientists in the field of creation of new means and technologies of space researches of Earth.

The journal H&ES Research is included in the list of scientific publications, recommended Higher Attestation Commission Russian Ministry of Education for the publication of scientific works, which reflect the basic scientific content of candidate and doctoral theses. IF of the Russian Science Citation Index.

Subject of published articles according to the list of branches of science and groups of scientific specialties in accordance with the specialties:

- 2.2.15 Telecommunication systems, networks and devices
- 2.3.1 System analysis, management and information processing
- 2.3.5 Mathematical and software support for computing systems, complexes and computer networks
- 2.3.6 Methods and systems of information security
- 2.5.13 Design, construction and production of aircraft
- 2.5.16 Dynamics, ballistics, aircraft motion control

JOURNAL H&ES RESEARCH INDEXING

All issues of the journal are in a free access on a site of the journal www.hes.ru and elibrary.ru.

All authors wishing to post a scientific article in the journal, you must register it according to the requirements and send the materials to your email: HT-ESResearch@yandex.ru. The requirements are available on the website: www.H-ES.ru.

Language of publications: Russian, English.
Periodicity – 6 issues per year.
Media Registration Certificate PI No. FS 77-86203 Date of issue: 27.10.2023
Distribution Territory: Russian Federation, foreign countries

Circulation of 1000 copies. Price of 1000 Rub.
Postgraduate students for publication of the manuscript will not be charged

© "Media Publisher", LLC, 2024

ISSN 2409-5419 (Print) ISSN 2412-1363 (Online) WWW.H-ES.RU Дата выхода: 25 мая 2024

3 T.16
2024



СОДЕРЖАНИЕ

Учредитель:

ООО "ИД Медиа Пабlishер"

Издатель:

ДЫМКОВА С.С.

Главный редактор:

ЛЕГКОВ К.Е.

Редакционная коллегия:

БОБРОВСКИЙ В.И., д.т.н., доцент;

БОРИСОВ В.В., д.т.н., профессор,
Действительный член академии военных наук РФ;

БУДКО П.А., д.т.н., профессор;

БУДНИКОВ С.А., д.т.н., доцент,
Действительный член Академии информатизации образования;

ВЕРХОВА Г.В., д.т.н., профессор;

ГОНЧАРОВСКИЙ В.С., д.т.н., профессор, заслуженный деятель науки и техники РФ;

КОМАШИНСКИЙ В.И., д.т.н., профессор;

КИРПАНЕВ А.В., д.т.н., доцент;

КУРНОСОВ В.И., д.т.н., профессор,
академик Международной академии информатизации, Действительный член Российской академии естественных наук;

МОРОЗОВ А.В., д.т.н., профессор,
Действительный член Академии военных наук РФ;

МОШАК Н.Н., д.т.н., доцент;

ПАВЛОВ А.Н., д.т.н., профессор;

ПРОРОК В.Я., д.т.н., профессор;

СЕМЕНОВ С.С., д.т.н., доцент;

СИНИЦЫН Е.А., д.т.н., профессор;

ШАТРАКОВ Ю.Г., д.т.н., профессор,
заслуженный деятель науки РФ.

Адрес издателя:

111024, Россия, Москва,
ул. Авиамоторная, д. 8, корп. 1, офис 323.

Адрес редакции:

194044, Россия, Санкт-Петербург,
Лесной Проспект, 34-36, к. 1,
Тел.: +7(911) 194-12-42.

Адрес типографии:

Россия, Москва, ул. Складочная, д. 3,
корп. 6.

Мнения авторов не всегда совпадают с точкой зрения редакции.

За содержание рекламных материалов редакция ответственности не несет.

Материалы, опубликованные в журнале – собственность ООО "ИД Медиа Пабlishер". Перепечатка, цитирование, дублирование на сайтах допускаются только с разрешения издателя.

АВИАЦИОННАЯ И РАКЕТНО-КОСМИЧЕСКАЯ ТЕХНИКА

Козлов С.В., Кубанков А.Н., Шабанов А.П.

Об информационной поддержке беспилотных воздушных судов на маршрутах железнодорожной логистики

4

ИНФОРМАТИКА, ВЫЧИСЛИТЕЛЬНАЯ ТЕХНИКА И УПРАВЛЕНИЕ

Гришкин В.М., Каримов С.И.

Глубокая нейронная сеть для семантической сегментации спутниковых изображений

12

Казарян М.М., Черкесова Л.В.,

Решетникова И.В., Ревякина Е.А.

Анализ возможностей проведения атак на функции передачи управления консолью операционной системы с применением методов активной разведки

18

Манонина И.В., Шестаков В.В.

Применение вейвлет-анализа для обработки сигналов систем передачи информации

30

РАДИОТЕХНИКА И СВЯЗЬ

Бужин И.Г., Антонова В.М., Гнездилов В.С., Миронов Ю.Б.

Реализация сетевых функций в IP-фабрике центра обработки данных

39

Белов Н.В., Репинский В.Н.

Одновременная передача защищенного сообщения и гамма-ключа к нему в одном частотном канале с приемом на антенную решетку с управляемой поляризационной характеристикой

46

Панкратов Д.Ю., Пахомова А.В.

Применение технологии MIMO для улучшения характеристик физического уровня беспроводных сетей Wi-Fi

55



CONTENTS

AVIATION, SPASE-ROCKET HARDWARE

Kozlov S.V., Kubankov A.N., Shabanov A.P.

Information support for unmanned aircraft along railway logistics routes

4

INFORMATICS, COMPUTER ENGINEERING AND CONTROL

Grishkin V.M., Karimov S.I.

Deep neural network for semantic segmentation of satellite images

12

Kazaryan M.M., Cherkesova L.V., Reshetnikova I.V., Revyakina E.A.

Analysis of attacks possibilities on the operating system control transfer function using active intelligence methods

18

Manonina I.V., Shestakov V.V.

Application of wavelet analysis for signal processing of information transmission systems

30

RF TECHNOLOGY AND COMMUNICATION

Buzhin I.G., Antonova V.M., Gnezdilov V.S., Mironov Yu.B.

Implementing network functions in a data center IP fabric

39

Belov N.V., Repinsky V.N.

Simultaneous transmission of a secured message and a gamma key to it in one frequency channel with reception on an antenna array with controlled polarization characteristics

46

Pankratov D.Y., Pakhomova A.V.

The use of MIMO technology to improve the physical layer characteristics of Wi-Fi wireless networks

55

Founder:

"Media Publisher", LLC

Publisher:

DYMKOVA S.S.

Editor in chief:

LEGKOV K.E.

Editorial board:

BOBROWSKY V.I., PhD, Docent;

BORISOV V.V., PhD, Full Professor;

BUDKO P.A., PhD, Full Professor;

BUDNIKOV S.A., PhD, Docent,

Actual Member of the Academy of Education Informatization;

VERHOVA G.V., PhD, Full Professor;

GONCHAREVSKY V.S., PhD, Full

Professor, Honored Worker of Science

and Technology of the Russian Federation;

KOMASHINSKIY V.I., PhD, Full Professor;

KIRPANEV A.V., PhD, Docent;

KURNOSOV V.I., PhD, Full Professor,

Academician of the International Academy

of Informatization, law and order, Member

of the Academy of Natural Sciences;

MOROZOV A.V., PhD, Full Professor,

Actual Member of the Academy of Military

Sciences;

MOSHAK N.N., PhD, Docent;

PAVLOV A.N., PhD, Full Professor;

PROROK V.Y., PhD, Full Professor;

SEMENOV S.S., PhD, Docent;

SINICYN E.A., PhD, Full Professor;

SHATRAKOV Y.G., PhD, Full Professor;

Honored Worker of Science of the Russian Federation.

Address of publisher:

111024, Russia, Moscow,
st. Aviamotornaya, 8, bild. 1, office 323

Address of edition:

194044, Russia, St. Petersburg,
Lesnoy av., 34-36, h.1,
Phone: +7 (911) 194-12-42.

Address of printing house:

Russia, Moscow, st. Skladochnaya, 3, h. 6

The opinions of the authors don't always coincide with the point of view of the publisher. For the content of ads, the editorial Board is not responsible. All articles and illustrations are copyright. All rights reserved. No reproduction is permitted in whole or part without the express consent of Media Publisher Joint-Stock company.

doi: 10.36724/2409-5419-2024-16-3-4-11

ОБ ИНФОРМАЦИОННОЙ ПОДДЕРЖКЕ БЕСПИЛОТНЫХ ВОЗДУШНЫХ СУДОВ НА МАРШРУТАХ ЖЕЛЕЗНОДОРОЖНОЙ ЛОГИСТИКИ

КОЗЛОВ

Сергей Витальевич¹

КУБАНКОВ

Александр Николаевич²

ШАБАНОВ

Александр Петрович³

АННОТАЦИЯ

Введение: Представленное исследование относится к области решения проблемы повышения пропускной способности железнодорожных магистралей России, используемых для товарообмена между экономическими субъектами. Предметной областью являются задачи применения на маршрутах железнодорожной магистрали дополнительных транспортных ресурсов – беспилотных авиационных систем, используемых для перемещения изделий в центры технической эксплуатации, и обратно на предприятия-эксплуатанты этих изделий. Внимание акцентировано на сети передачи данных железнодорожной магистрали, тракты которой предлагается использовать для передачи управляющей информации в воздушное судно, осуществляющее перемещение изделий в воздушном пространстве над перегонами железнодорожной магистрали. **Цель работы:** Поставлена и решена задача по созданию новой схемы информационно-телекоммуникационной системы для передачи управляющей информации. Схема должна удовлетворять требованию по обеспечению заданных показателей своевременности предоставления информации в воздушное судно, при минимальной стоимости её реализации. Научным результатом является новая модель процесса передачи управляющей информации с использованием трактов в сети передачи данных железнодорожной магистрали и ультракоротковолновых радиостанций в беспилотной авиационной системе. Новизна модели заключается в автоматическом изменении параметров активности трактов в сети передачи данных, в зависимости от местоположения пункта железнодорожной магистрали, над которым в воздушном пространстве осуществляет полёт воздушное судно. Технико-экономический эффект для предприятия железнодорожной магистрали заключается в повышении её пропускной способности за счет привлечения средств беспилотной авиации. Положительный эффект для предприятия беспилотной авиационной системы состоит в сокращении инвестиций на организацию сети передачи данных, за счёт использования сети предприятия железнодорожной магистрали.

Сведения об авторах:

¹ к.т.н., с.н.с., руководитель отделения, Федеральный исследовательский центр "Информатика и управление" РАН, г. Москва, Россия, skozlov@ipiran.ru

² д.в.н., профессор, заведующий кафедрой, Московский технический университет связи и информатики, Москва, Россия, a.n.kubankov@mtuci.ru

³ д.т.н., с.н.с., ведущий научный сотрудник, Федеральный исследовательский центр "Информатика и управление" РАН, г. Москва, Россия, apshabanov@mail.ru

КЛЮЧЕВЫЕ СЛОВА: логистика, железнодорожная магистраль, беспилотная авиационная система, процесс передачи управляющей информации, центры технической эксплуатации.

Для цитирования: Козлов С.В., Кубанков А.Н., Шабанов А.П. Об информационной поддержке беспилотных воздушных судов на маршрутах железнодорожной логистики // Научные исследования в космических исследованиях Земли. 2024. Т. 16. № 3. С. 4-11. doi: 10.36724/2409-5419-2024-16-3-4-11



Введение. Объекты исследования

Объектами настоящего исследования являются процессы передачи информации в логистической сети, построенной с применением транспортных средств железнодорожной магистрали и беспилотной авиационной системы.

Проведено обследование материальных и нематериальных сущностей, относящихся к транспортной логистике, в том числе, рекомендованных в национальных стандартах [1-3], в научных и методических публикациях, например [4-15]. В результате определены следующие информационные процессы в логистической транспортной сети, в составе которых должны воспроизводиться процессы передачи управляющей информации:

процессы управления движением транспортных средств, в том числе, процесс управления полётом судна в воздушном пространстве над железнодорожной магистралью;

процессы записи в базу данных логистической транспортной сети цифровой карты навигаций;

процессы актуализации на цифровой карте навигаций мест нахождения пунктов железнодорожной магистрали, железнодорожных транспортных средств, воздушных судов, станций внешних пилотов и радиостанций;

процессы информационного взаимодействия между предприятиями беспилотной авиационной системы, железнодорожной магистрали и логистической транспортной сети.

В работе использовались термины и определения, относящиеся к области беспилотной авиации, например [1, 2], к организационной, семантической и технической интероперабельности предприятий [3, 11], к методам исследования [4-7, 14, 15], и следующие термины и определения:

Тракт передачи управляющей информации – тракт в сети передачи данных железнодорожной магистрали, состав транзитных узлов в котором изменяется в зависимости от пункта магистрали, над которым осуществляет полёт воздушное судно.

Организационное взаимодействие – обмен информацией на уровне общих целей между предприятиями логистической транспортной сети, железнодорожной магистрали и беспилотной авиационной системы, осуществляемый в соответствии с заключенными договорами.

Семантическое взаимодействие – составная часть организационного взаимодействия на уровне смыслов, которые содержатся в информации, и которые одинаковым образом понимаются субъектами взаимодействующих предприятий.

Техническое взаимодействие – составная часть организационного взаимодействия на уровне протоколов и форматов данных, содержащих информацию.

Характеристика исследования. Постановка задачи.

При проведении исследования выполнены следующие мероприятия.

1. Разработаны технические требования к устройствам, которые задействуются в реализации процесса передачи управляющей информации в воздушное судно. Это, как минимум: сеть передачи данных железнодорожной магистрали;

средства для прямой радиосвязи с воздушным судном – радиостанции с дистанционным управлением, установленные в станционных пунктах и обладающие свойствами приёма управляющей информации из сети передачи данных железнодорожной магистрали;

станция внешнего пилота, воспроизводящая процессы передачи управляющей информации по трактам в сети передачи данных железнодорожной магистрали.

2. формулированы задачи исследования:

разработка новой структурной схемы информационно-телекоммуникационной системы для информационной поддержки полёта воздушного судна на маршрутах железнодорожной логистики;

создание на базе информационно-телекоммуникационной системы новой модели для процесса передачи управляющей информации в воздушное судно, осуществляющее перемещение технических изделий по маршрутам логистической транспортной сети в воздушном пространстве над железнодорожной магистралью.

3. С целью выполнения этого требования разработаны структурные схемы гипотетической информационно-телекоммуникационной системы, которая должна обеспечивать передачу управляющей информации в беспилотной авиационной системе в существующих условиях:

организационного взаимодействия предприятий логистической транспортной сети, железнодорожной магистрали и беспилотной авиационной системы;

технического и семантического взаимодействия информационных систем и баз данных на предприятиях логистической транспортной сети, железнодорожной магистрали и беспилотной авиационной системы, в части приёма, обработки и передачи информации, относящейся к процессам логистики, в том числе, к процессам актуализации на цифровой карте мест нахождения транспортных средств, включая воздушные суда;

заданы показатели своевременности предоставления управляющей информации в воздушное судно – максимально допустимое время T_{max} . передачи и минимально допустимая вероятность P_{min} . превышения этого времени.

4. Выполнен сравнительный анализ схем построения информационно-телекоммуникационной системы в беспилотной авиационной системе как основы для воспроизводства нового процесса передачи управляющей информации в воздушное судно:

цель анализа – определить оптимальную схему, как материальную основу для воспроизводства нового процесса передачи управляющей информации в воздушное судно;

критерий оценки – минимальная стоимость проектных и внедренческих работ при заданных показателях своевременности предоставления управляющей информации T_{max} . и P_{min} .

в результате определена наиболее эффективная схема, на основании которой создана *новая цифровая модель процесса передачи управляющей информации в воздушное судно*.

Новизна модели определяется автоматическим изменением данных об адресе конечного узла в тракте передачи управляющей информации, которым является пункт магистрали, над которым осуществляет полёт воздушное судно.

Актуальность новой модели обусловлена действием негативных условий санкций [13], в частности, в отношении предприятий-участников международной торговли, и обоснована ожидаемым положительным эффектом, достигаемым от применения модели в логистической транспортной сети. Это:

повышение пропускной способности железнодорожной магистрали, за счёт дополнительных грузовых потоков, осуществляемых беспилотными авиационными системами;

оперативно-технический эффект для предприятий-эксплуатантов технических изделий, транспортируемых на воздушных судах, достигаемый благодаря ускорению доставки изделий к местам проведения ремонта, технического обслуживания, модернизации и обратно – к местам их эксплуатации [11].

Схемы информационно-телекоммуникационной системы

При разработке схем информационно-телекоммуникационной системы, на основе которых должны выполняться функции процесса передачи управляющей информации в воздушное судно беспилотной авиационной системы, применены гипотетический подход и дедуктивный метод.

С помощью гипотетического подхода применённого при обследовании научно-технических решений – моделей и методов, например [4, 5, 7, 9, 11, 12], и изучении национальных стандартов, например [1-3] разработана функциональная модель процесса передачи управляющей и контрольной информации в беспилотной авиационной системе, в которой передача информации осуществляется в автономном режиме – без привлечения средств связи и передачи данных из числа средств других предприятий в транспортной логистике (рис. 1).



Рис. 1. Функциональная схема процесса передачи управляющей информации в беспилотной авиационной системе

На рисунке (рис. 1) видно, что формирование управляющей информации осуществляется как реакция на контрольную информацию, которая передаётся в станцию внешнего пилота.

В состав контрольной информации входят, как минимум, информация:

о текущем состоянии механизмов управления полётом, которые регулируются на основании управляющей информации;

о месте нахождения воздушного судна на цифровой карте логистической транспортной сети;

о метеорологических и других показателях внешней среды, в которой совершает полёт воздушное судно, и которые негативно влияют или могут оказать негативное влияние на его движение по маршруту логистической транспортной сети.

Следует заметить, что процесс передачи управляющей информации является подпроцессом в общем процессе управления полетом воздушного судна. Инициация данного процесса производится на основании результатов анализа контрольной информации о состоянии бортовых движительных механизмов и условий внешней среды.

Другие, помимо процесса передачи управляющей информации, функции процесса управления полётом, например функция передачи контрольной информации, гипотетически могут быть реализованы либо устройствами из состава беспилотной авиационной системы, либо извне – средствами других предприятий, например из состава системы управления предприятия логистической транспортной сети (рис. 1).

Исключением является контрольная информация о состоянии движительных механизмов, передаваемая с борта воздушного судна.

Исходя из намерения разработки оптимальной схемы информационно-телекоммуникационной системы, обеспечивающей воспроизводство процесса передачи управляющей информации в соответствии с функциональной схемой (рис. 1), были разработаны несколько гипотетических схем, обеспечивающих реализацию данного процесса при следующих режимах эксплуатации беспилотной авиационной системы:

1) передача управляющей информации осуществляется в беспилотной авиационной системе при её использовании в автономном режиме;

2) передача управляющей информации осуществляется в режиме обеспечения организационного взаимодействия предприятий беспилотной авиационной системы, железнодорожной магистрали и логистической транспортной сети.

Схема 1 – схема информационно-телекоммуникационной системы для автономного режима беспилотной авиационной системы со станциями внешнего пилота, укомплектованными, в том числе, радиостанциями с возможностью прямой связи с воздушным судном. Схема 1 отображена на рисунке 2.

Характерное свойство, которое присуще первой схеме: передача управляющей информации осуществляется в режиме ультракоротковолновой радиосвязи между воздушным судном и станцией внешнего пилота (1, 2, ..., K) с соответствующей ей, радиостанцией (1, 2, ..., K).

Режим прямой ультракоротковолновой радиосвязи предусматривает ограничения по дальности передачи информации, что обуславливает необходимость увеличивать в информационно-телекоммуникационной системе число станций внешнего пилота, укомплектованных радиостанциями и, как следствие, дополнительно привлекать внешних пилотов. При этом:

передача полномочий по управлению пилотируемым воздушным судном между внешними пилотами осуществляется либо за счёт создания специальной сети передачи данных, либо за счёт аренды трактов в сети передачи данных другого предприятия.

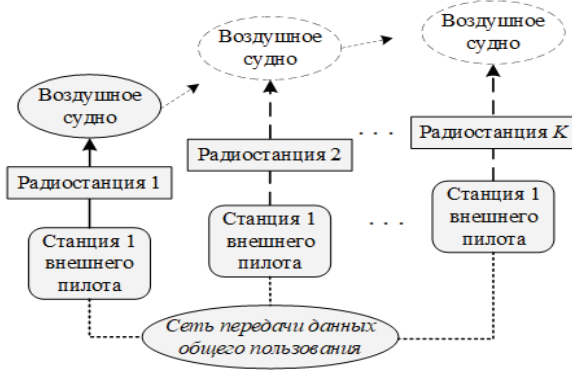


Рис. 2. Структурная схема информационно-телекоммуникационной системы с возможностями реализации процесса передачи информации в беспилотной авиационной системе (Схема 1)

Схема 2 – схема информационно-телекоммуникационной системы для автономного режима беспилотной авиационной системы с одной станцией внешнего пилота и дистанционно управляемыми этой станцией радиостанциями с возможностью их прямой связи с воздушным судном. Схема 2 отображена на рисунке 3.

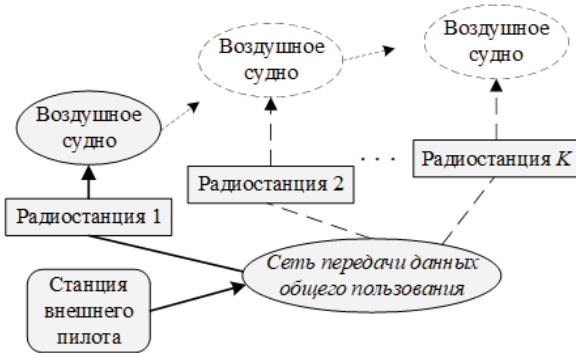


Рис. 3. Структурная схема информационно-телекоммуникационной системы с возможностями реализации процесса передачи информации в беспилотной авиационной системе (Схема 2)

Характерные свойства, которые присущи второй схеме:

Информационно-телекоммуникационная система представляет собой совокупность станции внешнего пилота, маршрутов в сети передачи данных общего пользования и дистанционно управляемых радиостанций (1, 2, ..., K);

связь между станцией внешнего пилота и радиостанциями осуществляется посредством сети передачи данных, в которой по протоколам данной сети организуются маршруты для передачи информации в ту или иную радиостанцию, в зависимости от того, в какой из их зон ответственности осуществляет полёт воздушное судно;

каждая радиостанция обеспечивает прямую ультракоротковолновую радиосвязь с воздушным судном.

Режим дистанционной ультракоротковолновой радиосвязи в совокупности с применением сети передачи данных общего пользования, используемый в анализируемой схеме 2:

с одной стороны, по сравнению со схемой 1, увеличивает время передачи информации из станции внешнего пилота до

воздушного судна и, тем самым, затрудняет выполнение требований, предъявляемых к своевременности предоставления информации в воздушное судно;

с другой стороны, уменьшает число станций внешнего пилота и, тем самым, повышает технико-экономический эффект в целом для беспилотной авиационной системы.

Схема 3 – схема информационно-телекоммуникационной системы в режиме обеспечения организационного взаимодействия предприятий беспилотной авиационной системы, железнодорожной магистрали и логистической транспортной сети. Схема 3 отображена на рисунке 4.

Ряд свойств, присущих второй схеме (рис. 3) информационно-телекоммуникационной системы, в частности, использование возможностей маршрутизации в сети передачи данных и возможностей ультразвуковой радиосвязи с воздушным судном, также присущи и третьей схеме, представленной на рисунке 4.

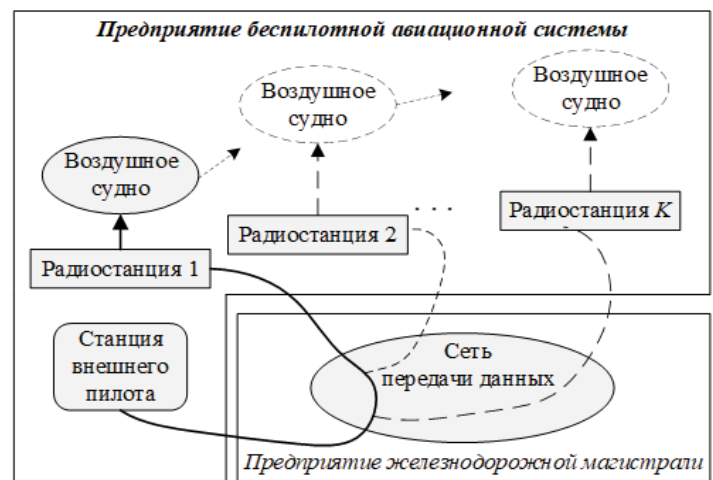


Рис. 4. Структурная схема информационно-телекоммуникационной системы с возможностями реализации процесса передачи информации в беспилотной авиационной системе (Схема 3)

В то же время, есть существенные отличия, которые обусловлены фактором организационного взаимодействия предприятия беспилотной авиационной системы и предприятиями железнодорожной магистрали и логистической транспортной сети.

Признаком организационного взаимодействия является факт наличия договорных соглашений между указанными предприятиями, в которых учтены интересы обеих сторон. Как следствие, очевидны следующие преимущества рассматриваемой схемы (рис. 4):

использование ресурсов предприятия беспилотной авиационной системы в бизнес-процессах предприятия железнодорожной магистрали позволяет обеспечить более быструю доставку для ряда приоритетных грузов, например, технических изделий, что увеличивает грузооборот в целом и, в частности улучшает экономические показатели этого предприятия;

использование в бизнес-процессах предприятия беспилотной авиационной системы ресурсов (сеть передачи данных) предприятия железнодорожной магистрали и контрольной информации, добываемой на основе ресурсов предприятия логи-

стической транспортной системы, позволяет сократить стоимость аренды трактов, выделяемых в сети для передачи информации в воздушное судно, и снизить стоимость владения контрольной информацией. Это достигается за счёт взаимного учёта интересов указанных предприятий.

Новая модель процесса передачи управляющей информации

При проведении структурно-функционального анализа различных схем информационно-телекоммуникационной системы по критерию своевременности предоставления информации и минимизации сил и средств, сформулировано следующее утверждение.

Схема 3 информационно-телекоммуникационной системы (рис. 4), построенная на основании принципа обеспечения организационного взаимодействия предприятий логистической транспортной сети, беспилотной авиационной системы и железнодорожной магистрали, и предназначенная для передачи управляющей информации из станции внешнего пилота в воздушное судно:

имеет преимущество перед схемами 1 и 2 (рис. 2 и 3), которое заключается в сокращении сроков выполнения проектных и инновационных работ по вводу беспилотной авиационной системы в логистическую транспортную сеть, построенную с использованием сил и средств железнодорожной магистрали;

является базовым элементом для разработки новой модели процесса передачи управляющей информации из станции внешнего пилота в воздушное судно беспилотной авиационной системы.

На основании сформулированного утверждения разработана цифровая модель информационно-телекоммуникационной системы, как материальной основы для реализации нового процесса передачи управляющей информации.

Цифровая модель информационно-телекоммуникационной системы размещена в базе данных станции внешнего пилота и отображает взаимосвязанные данные об их элементах, которые обеспечивают реализацию процесса передачи информации в беспилотной авиационной системе (рис. 5).

На рисунке обозначено:

S – станция внешнего пилота;

V – воздушное судно;

$G\{G_1; G_2; \dots G_K\}$ – сеть пунктов G_i железнодорожной магистрали;

$R\{R_1; R_2; \dots R_K\}$ – сеть радиостанций R_i с дистанционным управлением, установленных в пунктах G_i железнодорожной магистрали;

$L\{L_1; L_2; \dots L_K\}$ – множество трактов в сети передачи данных, которые выделены для передачи данных из станции внешнего пилота до соответствующих радиостанций $\{R_i\}$, установленных в пунктах $G\{G_1; G_2; \dots G_K\}$ железнодорожной магистрали;

$L\{L_1[\mu_{1i}]; L_2[\mu_{2i}]; \dots L_K[\mu_{ki}]\}$ – параметры $\{\mu_{ji}\}$ трактов $\{L_i\}$ в сети передачи данных железнодорожной магистрали;

$G\{G_1[R_1]; G_2[R_2]; \dots G_K[R_K]\}$ – параметры пунктов $\{G_i\}$ в железнодорожной магистрали – соответственно радиостанции $R\{R_1; R_2; \dots R_K\}$;

$R\{R_1[R_{1i}]; R_2[R_{2i}]; \dots R_K[R_{ki}]\}$ – параметры $\{R_{ji}\}$ в сети радиостанций $\{R_j\}$, размещенных в пунктах $\{G_i\}$ железнодорожной магистрали, и которые настроены с целью приема данных из трактов $\{L_i\}$ сети передачи данных железнодорожной магистрали.

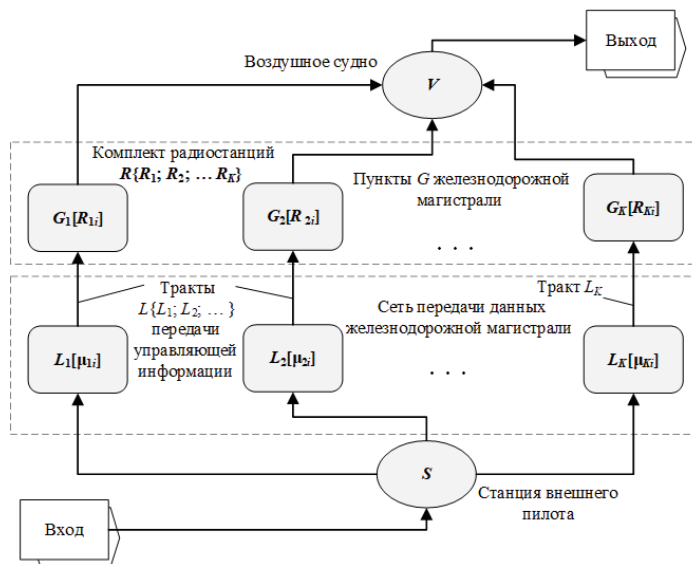


Рис. 5. Цифровая модель информационно-телекоммуникационной системы с возможностями реализации процесса передачи информации в беспилотной авиационной системе

Новое, по сравнению с известными цифровыми моделями-аналогами (рис. 2, 3), характерное свойства цифровой модели информационно-телекоммуникационной структуры (рис. 5) состоит в способности изменять параметры μ_{ji} активности трактов $\{L_1[\mu_{1i}]; L_2[\mu_{2i}]; \dots L_K[\mu_{ki}]\}$ в сети передачи данных железнодорожной магистрали.

Процесс производства таких изменений по своей сути является процессом актуализации трактов передачи информации и представляет собой составную часть (подпроцесс) в процессе передачи управляющей информации от станции внешнего пилота в воздушное судно.

В новом подпроцессе актуализации трактов передачи данных выполняют следующие действия.

1. Прием в станции внешнего пилота контрольной информации из логистической транспортной сети о местоположении воздушного судна.

2. Фиксация местоположения судна на цифровой навигационной карте и определение радиостанции, например R_j из сети радиостанций $R\{R_1; R_2; \dots R_K\}$, в зоне радиовидимости которой, находится воздушное судно.

3. Оценка выполнения условия – например, «параметр активности радиостанции R_j , например $[R_{ji}]$ равен 1 (единице)?»: если $[R_{ji}] = 1$, то радиостанция активна, изменения в цифровой модели не производят.

4. Если $[R_{ji}] = 0$, то радиостанция неактивна, и производятся следующие действия:

параметр активности радиостанции R_j устанавливается в состояние активности $[R_{ji}] = 1$;

параметр активности $[R_{ki}]$ радиостанции R_k , которая находилась в состоянии активности, устанавливается в состояние неактивности $[R_{ji}] = 0$;

параметр активности $[\mu_{ji}]$ тракта из числа трактов $\{L_1[\mu_{11}]; L_2[\mu_{21}]; \dots L_k[\mu_{k1}]\}$ в сети передачи данных, который совместим с радиостанцией R_j , устанавливается в состояние активности – $[\mu_{ji}] = 1$;

параметр активности $[\mu_{ki}]$ тракта L_k из числа линий $\{L_1[\mu_{11}]; L_2[\mu_{21}]; \dots L_k[\mu_{k1}]\}$ в сети передачи данных, который находился в состоянии активности, устанавливается в состояние неактивности $[\mu_{ki}] = 0$.

На рисунке 6 отображена новая модель процесса передачи управляющей информации от станции внешнего пилота в воздушное судно беспилотной авиационной системы.

В данной модели процесс отображается в виде последовательности выполнения функций с приведением существенных объектов, которые автоматически исполняют эти функции – станции внешнего пилота, радиостанции и воздушного судна, тракта в сети передачи данных железнодорожной магистрали.

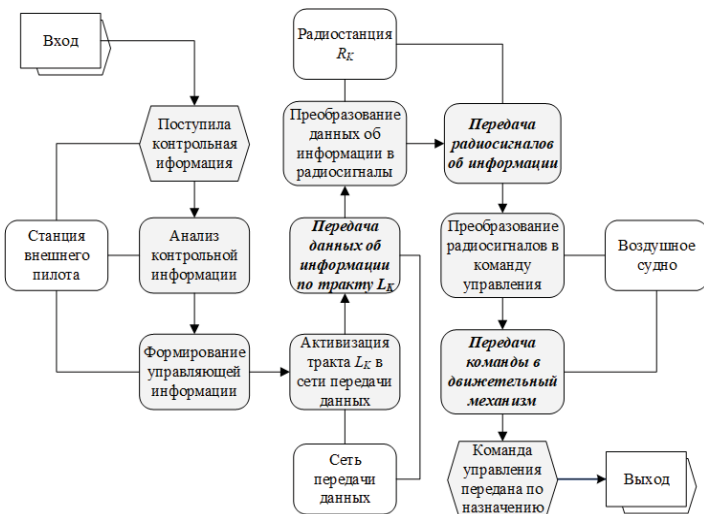


Рис. 6. Новая модель процесса передачи управляющей информации от станции внешнего пилота в воздушное судно беспилотной авиационной системы (на примере тракта L_k и радиостанции G_k)

Область применения новой модели процесса передачи управляющей информации распространяется на известные методы управления движением беспилотных судов в воздушном пространстве.

Заключение

Тема исследования относится к вопросам применения информационно-телекоммуникационных технологий при решении задач транспортной логистики, организуемой на базе существующих железнодорожных магистралей с применением вновь вводимых в транспортную логистику средств беспилотных авиационных систем.

Решена научная задача о создании новой модели процесса передачи управляющей информации в воздушное судно, осуществляющей перемещение технических изделий с целью

производства технологического обслуживания, выполнения других работ и возвращения на предприятия-эксплуатанты изделий.

Научным результатом исследования является новый функционал процесса передачи управляющей информации, относящийся (а) к использованию при передаче информации сети передачи данных железнодорожной магистрали, (б) к выполнению актуализации компонентов в тракте передаче данных этой сети в зависимости от места нахождения судна в воздушном пространстве логистической сети, (в) к поступлению в станцию внешнего пилота контрольной информации из предприятия логистической транспортной сети.

Достигнутый научный результат добавил в общий процесс управления полетом новое качество – автоматическое управление передачей управляющей информацией, базируясь на совместные усилия и ресурсы предприятий логистической транспортной сети, железнодорожной магистрали и беспилотной авиации.

Обоснована актуальность применения новой модели в логистических процессах с использованием беспилотных авиационных систем, в том числе, в условиях действующих санкций [13] в отношении предприятий-участников международной торговли.

Значимыми эффектами от применения новой модели процесса передачи управляющей информации являются:

экономический – для беспилотной авиации – снижение затрат на стационарное оборудование и на оплату труда внешних пилотов, что существенно для протяжённых логистических маршрутов;

техничко-экономический эффект для железнодорожных магистралей – повышение пропускной способности достигается за счет дополнительного грузооборота с использованием беспилотных авиационных систем;

оперативно-технический эффект, по сравнению с железнодорожной логистикой, для изделий, транспортируемых на воздушных судах – сокращение сроков технического обслуживания и других работ за счёт уменьшения времени на доставку изделий в центры обслуживания, и обратно.

Литература

- ГОСТ Р 56122-2014 «Воздушный транспорт. Беспилотные авиационные системы. Основные требования». Национальный стандарт Российской Федерации. Москва, Российский институт стандартизации, 2015. 10 с.
- ГОСТ Р 59796-2021 «Информационные технологии. Интероперабельность. Термины и определения». Национальный стандарт Российской Федерации. Москва, Российский институт стандартизации, 2021. 12 с.
- ГОСТ Р 59519-2021 «Беспилотные авиационные системы. Компоненты беспилотных авиационных систем. Спецификация и основные технические требования». Национальный стандарт Российской Федерации. Москва, Российский институт стандартизации, 2021. 10 с.
- Крикунов И.С., Файзуллин А.Р., Бенсон И.Н. Моделирование и совершенствование российско-китайской транспортной сети в текущих экономических условиях // Экономика и управление: проблемы, решения. 2024. Т. 1, № 1(142). С. 59-69. DOI: 10.36871/ek.up.r.2024.01.01.008. EDN SXKGCW.

5. Анохов И.В., Римская О.Н. Этапы развития транспортных коридоров: механизация, роботизация, интеллектуализация и перспективы цифровизации // Стратегические решения и риск-менеджмент. 2022. Т. 13, № 1. С. 72-79. DOI 10.17747/2618-947X-2022-1-72-79. EDN YTAIDV.

6. Никифорова Г.И. Исследование информационного взаимодействия железнодорожного и морского транспорта в логистических цепях доставки груза // Известия Петербургского университета путей сообщения. 2022. Т. 19, № 1. С. 82-89. DOI: 10.20295/1815-588X-2022-19-1-82-89. EDN LREQHF.

7. Kozlov S.V., Shabanov A.P., Kubankov A.N. Unmanned aircraft systems in logistics processes with network management // Wave Electronics and Its Application in Information and Telecommunication Systems. 2023. Vol. 6, No. 1, pp. 210-216. DOI: 10.1109/WECONF57201.2023.10148019. EDN JРХВНГ.

8. Макаренко С.И. Интероперабельность организационно-технических систем. Монография. СПб.: Научно-технологии, 2024. 313 с., ISBN 978-5-6048123-9-6.

9. Зацаринный А.А., Козлов С.В., Шабанов А.П. Интероперабельность консолидируемых организационных систем // Проблемы управления. 017. № 6. С. 43-49. EDN ZVMPDD.

10. Грушио А.А., Грушио Н.А., Забейайло М.И. и др. Анализ цепочек причинно-следственных связей // Информатика и ее применения. 2022. Т. 16, № 2. С. 68-74. DOI: 10.14357/19922264220209. EDN HPSLTU.

11. Малащенко Ю.Е., Назарова И.А. Сравнительный анализ узловых мультипоточков в многопользовательской сетевой системе // Информатика и ее применения. 2024. Т. 18, № 1. С. 40-45. DOI: 10.14357/19922264240106. DN АКСМСQ.

12. Зацаринный А.А., Ионенков Ю.С. Методический подход к выбору ключевых показателей эффективности для оценки организаций информационно-технологической сферы // Системы и средства информатики. 2023. Т. 33, № 2. С. 79-87. DOI: 10.14357/08696527230208. EDN TNTNGN.

13. Смешко О.Г., Плотников В.А., Вертакова Ю.В. Государственная инвестиционная политика как инструмент преодоления угроз национальной экономической безопасности, вызванных антироссийскими санкциями // Экономика и управление. 2023. Т. 29, № 7. С. 747-762. DOI: 10.35854/1998-1627-2023-7-747-762. EDN HTJWFJ.

14. Кочеткова И.А., Власкина А.С., Эсенг Манге П.Л.Э., Шоргин В.С. Задача разделения ресурса беспроводной сети по задержке передачи эластичного трафика // Системы и средства информатики. 2024. Т. 34, № 1. С. 23-32. DOI 10.14357/08696527240102. EDN WXYRQV.

15. Тельнов Ю.Ф., Казаков В.А., Брызгалов А.А., Федоров И.Г. Методы и модели обоснования прикладных сценариев цифровизации производственных и бизнес-процессов сетевых предприятий // Бизнес-информатика. 2023. Т. 17, № 4. С. 73-93. DOI 10.17323/2587-814X.2023.4.73.93. EDN WZKQ GK.

INFORMATION SUPPORT FOR UNMANNED AIRCRAFT ALONG RAILWAY LOGISTICS ROUTES

SERGEY V. KOZLOV

Moscow, Russia

ALEXANDER N. KUBANKOV

Moscow, Russia

ALEXANDER P. SHABANOV

Moscow, Russia

ABSTRACT

Introduction: The presented research relates to the field of tasks to solve the problem of increasing the capacity of Russian railways used for commodity exchange between economic entities. The subject area is the tasks of using additional transport resources on railway routes – unmanned aircraft systems used to move technical products to technical operation centers and back to the enterprises operating these products. Attention is focused on the data transmission network of the railway, the paths of which are proposed to be used to transmit control information to an aircraft carrying out the movement of products in the airspace along the routes of the railway.

The purpose of the work: The task has been set and solved to create a novel scheme of an information and telecommunications system for transmitting control information that meets the criterion of

KEYWORDS: *logistics, railway, unmanned aviation system, control information transmission process, technical operation centers*

ensuring the specified indicators of timely provision of information to the aircraft, at a minimum cost. The scientific result is a novel model of the information transmission process using paths in the railway data transmission network and ultrashort radio stations of an unmanned aircraft system. The novelty of the model lies in the automatic change of the parameters of the activity of paths in the data transmission network, depending on the location of the railway point over which the aircraft is flying in the airspace. The technical and economic effect for the railway company is to increase its productivity by attracting funds from unmanned aircraft. The positive effect for the unmanned aviation enterprise is to reduce investments in the organization of a data transmission network by using the network of the railway company.



REFERENCES

1. GOST R 56122-2014, "Airtransport. Unmanned aircraft systems. General requirements". The national standard of the Russian Federation. Moscow, Russian Institute of Standardization, 2015. 10 p.
2. GOST R 59796-2021, "Information technology. Interoperability. Terms and definitions". The national standard of the Russian Federation. Moscow, Russian Institute of Standardization, 2021. 12 p.
3. GOST R 59519-2021, "Unmanned aircraft systems. Components of unmanned aircraft systems. Specification and general technical requirements". The national standard of the Russian Federation. Moscow, Russian Institute of Standardization, 2021. 10 c.
4. I.S. Krikunov, A.R. Fayzullin, I.N. Benson, "Modeling and improvement of the Russian-Chinese transport network in the current economic conditions". *Ekonomika i upravlenie: problemy resheniya*, vol. 1, no. 1, pp. 59-69, 2024. <https://doi.org/10.36871/ek.up.p.r.2024.01.01.008>.
5. I.V. Anokhov, O.N. Rimskaya, "Stages of transport corridor development: Mechanisation, robotisation, intellectualization and digitalization perspectives". *Strategic Decisions and Risk Management*, vol. 13, no. 1, pp. 72-79, 2022. DOI: 10.17747/2618-947X-2022-1-72-79.
6. G.I. Nikiforova, "Research of Informational Interaction Between Railway and Sea Transport in Logistic Chains of Cargo Delivery". *Proceedings of Petersburg Transport University*, vol. 19, iss. 1, pp. 82-89, 2022. DOI: 10.20295/1815-588X-2022-1-82-89.
7. S.V. Kozlov, A.N. Kubankov, A.P. Shabanov, "Unmanned aircraft systems in logistics processes with network management". *Wave Electronics and Its Application in Information and Telecommunication Systems (WECONF-2022)*, vol. 6, no. 1, pp. 210-216, 2023. DOI: 10.1109/WECONF57201.2023.10148019.
8. S.I. Makarenko, "Interoperability of organizational and technical systems". Saint Petersburg, Naukoemkie Tehnologii Publ., 2024. 313 p. ISBN 978-5-6048123-9-6.
9. A.A. Zatsarinnyy, S.V. Kozlov, A.P. Shabanov, "Interoperability of consolidated organizational systems". *Problems of Management*, no. 6, pp. 43-49, 2017. https://elibrary.ru/download/elibrary_30685203_12457864.pdf.
10. A.A. Grusho, N.A. Grusho, M.I. Zabezhailo, A.A. Zatsarinnyy, E.E. Timonina, and S. Ya. Shorgin, "Cause-and-effect chain analysis". *Informatics and applications*, vol. 16, iss. 2, pp. 68-74, 2022. DOI: 10.14357/19922264220209.
11. Yu. E. Malashenko, I. A. Nazarova, "Analysis of node multiflows in a multiuser network system". *Informatics and applications*, vol. 18, iss. 1, pp. 40-45, 2024. DOI: 10.14357/19922264240106.
12. A.A. Zatsarinnyy, Yu.S. Iononkov, "Methodological approach to the selection of key performance indicators for evaluating the information and technology organizations". *Systems and Means of Informatics*, vol. 33, no. 2, pp. 79-87, 2023. DOI: 10.14357/08696527230208.
13. O.G. Smeshko, V.A. Plotnikov, Yu.V. Vertakova, "State investment policy as a tool to overcome threats to national economic security caused by anti-Russian sanctions". *Economics and Management*, vol. 29, no. 7, pp. 747-762, 2023. <https://doi.org/10.35854/1998-1627-2023-7-747-762>.
14. I.A. Kochetkova, A.S. Vlaskina, P.L. E. Eseng Mangué, V.S. Shorgin, "Radio resource allocation for elastic traffic transmission with latency fairness in networks". *Systems and Means of Informatics*, vol. 34, no. 1, pp. 23-32, 2024 (In Russian). DOI: 10.14357/08696527240102.
15. Y.F. Telnov, V.A. Kazakov, A.A. Bryzgalov, I.G. Fiodorov, "Methods and models for substantiating application scenarios for the digitalization of manufacturing and business processes of network enterprises". *Business Informatics*, vol. 17, no. 4, pp. 73-93, 2023. DOI 10.17323/2587-814X.2023.4.73.93.

INFORMATION ABOUT AUTHORS:

Sergey V. Kozlov, PhD, Head of the Division, Federal Research Center "Computer Science and Control" Russian Academy of Sciences, Moscow, Russia, skozlov@ipiran.ru

Alexander N. Kubankov, PhD, Full Professor, Head of Department, Moscow Technical University of Communication and Informatics, Moscow, Russia [Москва, a.n.kubankov@mtuci.ru](mailto:a.n.kubankov@mtuci.ru)

Alexander P. Shabanov, PhD, leading researcher, Federal Research Center "Computer Science and Control" Russian Academy of Sciences, Moscow, Russia, apshabanov@mail.ru

For citation: Kozlov S.V., Kubankov A.N., Shabanov A.P. Information support for unmanned aircraft along railway logistics routess. *H&ES Reserch*. 2024. Vol. 16. No. 3. P. 4-11. doi: 10.36724/2409-5419-2024-16-3-4-11 (In Rus)

doi: 10.36724/2409-5419-2024-16-3-12-17

ГЛУБОКАЯ НЕЙРОННАЯ СЕТЬ ДЛЯ СЕМАНТИЧЕСКОЙ СЕГМЕНТАЦИИ СПУТНИКОВЫХ ИЗОБРАЖЕНИЙ

ГРИШКИН

Валерий Михайлович ¹

КАРИМОВ

Сардор Илхом угли ²

АННОТАЦИЯ

Введение: Семантическая сегментация изображений, получаемых при дистанционном зондировании Земли является достаточно актуальной задачей. В настоящее время эта задача решается с помощью глубоких нейронных сетей. Однако эти сети требуют больших вычислительных затрат, как на этапе обучения, так и при их использовании. **Методы:** Несмотря на значительное развитие методов и алгоритмов классификации объектов на изображениях, задача сегментации остается частично нерешенной. Отсутствует универсальный и широко принятый подход, лежащий в основе большинства алгоритмов. Общего алгоритма, который бы обеспечивал оптимальную сегментацию для любого изображения, также не существует. Одним из методов повышения производительности такой архитектуры является применение высокопроизводительных кодеров. Для сравнения результатов сегментации было также проведено обучение сети с архитектурой U-net, настроенной на работу с теми же изображениями. Обучение этой сети проводилось на том же наборе данных и с теми же метапараметрами обучения. **Результаты:** В данной работе предлагается архитектура нейронной сети, позволяющая снизить эти затраты и увеличить точность семантической сегментации спутниковых изображений. Тестирование проводилось на тестовом множестве изображений с использованием обученной нейронной сети. Архитектура основывается на структурах кодер – декодер, где в кодере и декодере используются глубинные свертки, существенно уменьшающие вычислительные затраты. В работе приводятся экспериментальные результаты, показывающие эффективность предлагаемой архитектуры.

Сведения об авторах:

¹ кандидат технических наук, доцент,
Санкт-Петербургский государственный
университет, г. Санкт-Петербург,
Россия,
orcid.org/0000-0002-2080-1898

² аспирант, Санкт-Петербургский
государственный университет,
г. Санкт-Петербург, Россия,
orcid.org/0000-0002-3035-0330

КЛЮЧЕВЫЕ СЛОВА: сегментация изображений, архитектура кодер-декодер, глубинная свертка.

Для цитирования: Гришкин В.М., Каримов С.И. Глубокая нейронная сеть для семантической сегментации спутниковых изображений // Научные технологии в космических исследованиях Земли. 2024. Т. 16. № 3. С. 12-17. doi: 10.36724/2409-5419-2024-16-3-12-17



Введение

Семантическая сегментация изображений представляет собой процесс выделения локальных областей на изображении, соответствующих различным классам объектов. В контексте сегментации изображений дистанционного зондирования Земли (ДЗЗ), этот метод находит применение в различных областях, таких как геоинформатика, георесурсотехника, автоматическое создание карт рельефа, градостроительство, анализ землепользования, а также при мониторинге ледовой обстановки, и др.

Несмотря на значительное развитие методов и алгоритмов классификации объектов на изображениях, задача сегментации остается частично нерешенной. Во многих случаях некоторые этапы процесса все еще выполняются операторами вручную, что приводит к значительным временным затратам. Кроме того, отсутствует универсальный и широко принятый подход, лежащий в основе большинства алгоритмов. Общего алгоритма, который бы обеспечивал оптимальную сегментацию для любого изображения, также не существует.

В настоящее время существует множество методов семантической сегментации изображений, основанных на применении сверточных нейронных сетей (CNN). В целом такие методы обеспечивают достаточно хорошую производительность и точность сегментации относительно небольших изображений. При этом различные архитектуры CNN используются для классификации и плотной маркировки этих изображений. Однако эти нейросетевые методы обработки изображений имеют определенные недостатки и далеки от совершенства. Изображения земной поверхности, получаемые со спутников, имеют высокое разрешение, что приводит к большим вычислительным затратам при их сегментации. Таким образом, разработка методов, позволяющих снизить вычислительные затраты и повысить качество сегментации, является достаточно актуальной.

В настоящее время нет четко регламентированных правил реализации структуры CNN – количество слоев, количество и размер карт признаков, размер матриц свертки, выбор алгоритма обучения. При проектировании структуры CNN следует учитывать, что небольшое количество сетевых параметров может снизить точность классификации. Однако большое количество параметров увеличивает вычислительную сложность и не всегда улучшает классификационные возможности сети.

Семантическая сегментация в компьютерном зрении заключается в назначении семантической метки каждой связанной области изображения. Почти все современные архитектуры CNN для сегментации изображений следуют принципам, изложенным в [1]. Основная идея состоит в том, чтобы изменить традиционную классификацию CNN таким образом, чтобы на выходе был не вектор вероятности, а карта вероятности классов. Как правило, стандартная CNN используется в качестве кодировщика, который формирует карты признаков для различных уровней разложения изображения. За кодировщиком следует декодер, который масштабирует карты признаков до исходных пространственных размеров входного изображения. Затем для каждого класса полу-

чается тепловая карта. Глубокие сети семантической сегментации, обычно основаны на принципах полной свертки и архитектурах кодер – декодер [2].

Как правило кодер представляет собой последовательность сверточных слоев с последующей пакетной нормализацией (BN) и выпрямленной линейной функцией активации (ReLU). За блоками свертки следует слой пуллинга. Фактически кодер – это обычная сверточная сеть, обучаемая для классификации входного изображения. Декодер имеет такое же количество слоев и выполняет функцию интерполяции выхода кодера. На последнем уровне декодера, для формирования выходного сегментированного изображения, как правило, используется свертка 1×1 с последующей сигмоидальной функцией активации.

Нейронные сети SegNet [2] и Unet [3], которые показали хорошие результаты в области семантической сегментации изображений, имеют структуру кодер – декодер. Архитектура SegNet основана на сверточных слоях VGG-16 [4]. Особенность этой архитектуры заключается в том, что интерполирующие слои декодера соединены с соответствующими пулинг слоями кодера. При этом, по сохраненным индексам максимальных значений карты признаков из слоя пуллинга кодера, формируется интерполированная карта признаков соответствующего слоя декодера. Таким образом уменьшаются вычислительные затраты при обучении всей сети. Основным достоинством данной архитектуры является относительно высокая производительность. Однако, на практике они показывают невысокое разрешение карт сегментации и недостаточную точность для изображений высокого разрешения.

В сети Unet, также, как и в сети SegNet, при выполнении пуллинга применяется максимизация по области 2×2 пикселя. После прохождения нескольких серий сверточных и субдискретизирующих слоев входное изображение преобразуется в абстрактные карты признаков, являющиеся выходами соответствующих кодирующих блоков. Сеть Unet можно рассматривать как модифицированную версию первой, в которой объединяются выходные данные слоев декодера с картами признаков из кодера на том же уровне. При этом интерполяция в слоях декодера производится с помощью транспонированной свертки [5]. Данная архитектура показала существенное повышение точности сегментации изображений различной природы, а также возможность обучаться на небольшом объеме данных. Недостатками Unet, является относительно низкая производительность и большая ресурсоемкость. Эти недостатки связаны с достаточно сложными и ресурсоемкими архитектурами, применяемых кодеров, таких как ResNet [6], Inception [7], EfficientNet [8].

Предлагаемый метод

Используемые архитектуры

Изображения, получаемые при дистанционном зондировании Земли, характеризуются высоким разрешением. Средние размеры этих изображений, как правило, составляют даже более чем 2000×2000 пикселей, в то время как большинство CNN рассчитано на входное разрешение 256×256 пикселей.

При пропорциональном разделении исходного изображения на соответствующие фрагменты общее время сегментации возрастает пропорционально количеству фрагментов. Для сегментации изображений больших размеров необходимо, по мере возможности, повышать производительность используемой архитектуры нейронной сети, соблюдая необходимую точность сегментации. Как уже отмечалось, архитектура сети Unet обладает хорошей точностью, поэтому именно эта архитектура и используется далее. Одним из методов повышения производительности такой архитектуры является применение высокопроизводительных кодеров. В настоящее время, одним из таких кодеров является сеть MobilNet [9], которая уменьшает количество используемой памяти для вычислений, сохраняя при этом высокую точность предсказаний. Эта, предварительно обученная, сеть работает даже на мобильных устройствах.

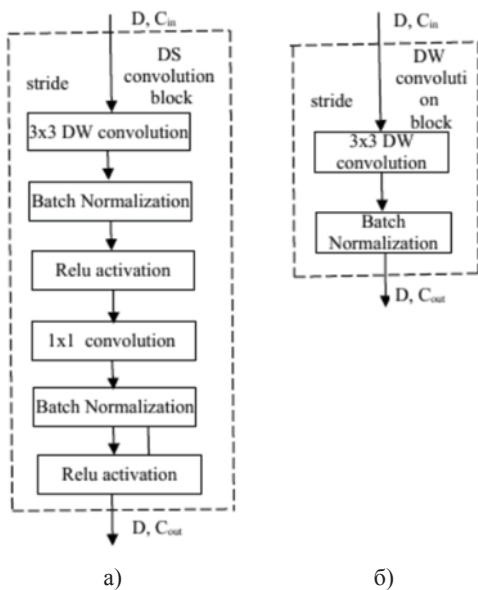


Рис. 1. Сверточные блоки:

а) блок глубинной разделяемой свертки (DS); б) блок глубинной свертки (DW); D – размерность изображения, C_{in} , C_{out} – количество входных и выходных каналов, $stride$ – шаг свертки

Архитектура MobilNet основана на применении глубинной разделяемой свертке DSW (depthwise separable convolution), которая разлагает стандартную свертку на глубинную свертку DW (depthwise convolution) и свертку 1×1 , называемую точечной сверткой (pointwise convolution). Стандартная свертка одновременно фильтрует и объединяет входы в новый набор выходов за один шаг. В то время как, глубинная разделяемая свертка выполняется в два этапа.

На первом этапе глубинная свертка применяет один фильтр к каждому входному каналу. На втором этапе точечная свертка объединяет выходные данные с глубинной сверткой. Таким образом разделяемая по глубине свертка разбивает стандартную свертку на два слоя: отдельный слой для фильтрации и отдельный слой для объединения. Такая схема приводит к резкому сокращению вычислений и размера модели.

В архитектуре сети используются два типа блоков, показанных на рисунке 1. Первый тип реализует глубинную разделяемую свертку DSW, с применением пакетных нормализаций и функций активаций ReLU. Второй тип представляет собой глубинную свертку с пакетной нормализацией и такой же функцией активации. В основном, в этих блоках используются свертки с шагом равным 1 ($stride = 1$). Шаг свертки равный двум ($stride = 2$) применяется для понижения пространственной размерности.

Из сверточных блоков, формируется два типа базовых блоков сверточного уровня. Структура блоков первого и второго типов показана на рисунках 2 и 3. Базовый блок первого типа использует остаточное соединение (residual connection). При этом результат применения ко входу последовательных сверток типа DS и DW суммируется с результатом отдельной свертки.

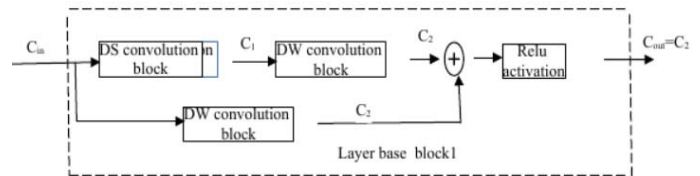


Рис. 2. Структура базового блока сверточного уровня первого типа:
 C_{in} , C_{out} – количество входных и выходных каналов;
 C_1 – количество каналов глубинной разделяемой свертки,
 C_2 – количество каналов глубинной свертки

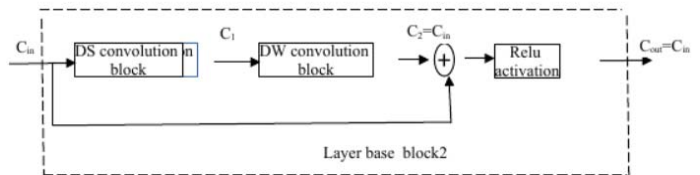


Рис. 3. Структура базового блока сверточного уровня второго типа:
 C_{in} , C_{out} – количество входных и выходных каналов;
 C_1 – количество каналов глубинной разделяемой свертки,
 C_2 – количество каналов глубинной свертки

Каждый сверточный слой сети образуется комбинацией этих базовых блоков. На рисунке 4 показана структура сверточного слоя сети, состоящего из базового блока первого типа и N базовых блоков второго типа.

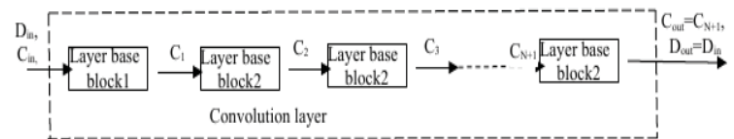


Рис. 4. Сверточный слой сети:

D_{in} , D_{out} – размерности входных и выходных карт признаков;
 C_{in} , C_{out} – входное и выходное количество каналов; C_1 – количество каналов базового блока первого типа, C_2, \dots, C_{N+1} – количество каналов в соответствующих блоках второго типа

Кодирующая часть сети начинается обычным сверточным слоем со сверткой 3×3 и шагом свертки 2, с последую-



щей пакетной нормализацией и использованием максимального пулинга. Затем следуют несколько сверточных слоев. Каждый такой сверточный слой представляет собой последовательность базовых блоков сверточного уровня (рис. 4). Каждом слой традиционно увеличивает число фильтров и понижает пространственную размерность карт признаков.

В данной работе применяется кодер, состоящий из четырех сверточных слоев. Параметры используемых сверточных слоев приведены в таблице 1.

Таблица 1

Параметры сверточных слоев кодера

Номер слоя	Размерность входа D_{in}	Размерность выхода D_{out}	Число каналов входа C_{in}	Число каналов выхода C_{out}	Количество блоков типа 1	Количество блоков типа 2
1	512	128	3	64	-	-
2	128	128	64	256	1	2
3	128	64	256	512	1	3
4	64	32	512	1024	1	5

Декодирующая часть сети представляет собой несколько уровней, каждый из которых сначала повышает размерность входной карты признаков и объединяет этот результат с картой признаков, полученной с предыдущего уровня кодера. Затем результат объединения обрабатывается глубинными свертками с применением пакетной нормализации и функции активации Relu. На рисунке 5 показана структура декодирующего слоя сети, используемая в данной работе.

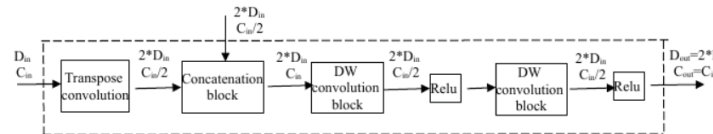


Рис. 5. Структура декодирующего слоя:

D_{in} , D_{out} – размерности входных и выходных карт признаков;
 C_{in} , C_{out} – входное и выходное количество каналов

Для повышения размерности входной карты признаков используется свертка транспонирования, повышающая размерность карты признаков в два раза. При этом количество каналов уменьшается в два раза. Эти изменения позволяют согласовать размерность и количество каналов, с картой признаков, поступающих с предыдущего слоя кодера. После объединения этих карт формируется новая карта признаков, размерность которой соответствует размерности соответствующего слоя кодера, а число каналов равно количеству каналов входа. Эта полученная карта признаков обрабатывается с помощью двух блоков глубоинной свертки. Выходом декодирующего слоя является карта признаков, которая подается на следующий слой декодирования.

Входами последнего декодирующего слоя служат карта признаков предпоследнего слоя декодера и входное изображение. Этот слой содержит дополнительную глубокую свертку с числом каналов равным числу классов, распознаваемых на изображении, и сигмоидальной функцией активации. Выходом слоя является «тепловая» карта, представляющая собой сегментированное изображение.

Предварительная обработка

Спутниковые изображения с высоким разрешением слишком велики, чтобы их можно было обработать непосредственно на нейронной сети. Простое уменьшение масштаба исходных изображений приведет к потере точности сегментации. Поэтому первым этапом предварительной обработки является разделение изображений набора данных и соответствующих им масок на фрагменты. При проектировании сети была выбрана размерность входных изображений 512x512 пикселей, которая позволяет с одной стороны уменьшить вычислительные затраты при обучении и использовании сети, а, с другой стороны, обеспечит достаточную точность сегментации. Полученные фрагменты изображений и масок масштабируются до указанной размерности. В данной работе каждое исходное изображение разбивается на 16 фрагментов

Каждый цветовой канал фрагмента изображения нормализуется к единичному диапазону. Трехканальные изображения фрагментов масок преобразуется в многоканальные изображения, где каждый канал соответствует тому или иному типу. При этом пиксель каждого канала, соответствующий типу данного канала, кодируется единичным значением, а пиксель, не соответствующий типу канала, кодируется нулем. В результате формируется рабочий набор данных, состоящий из фрагментов изображений и соответствующих им масок.

Экспериментальные результаты

Набор данных

Для обучения сети используется предварительно подготовленный набор данных LandCover [10], дополненный размеченными снимками, относящимися к районам Центральной Азии. Набор содержит 1146 спутниковых изображений районов земной поверхности высокого разрешения. Помимо самих изображений в него входят маски, отображающие тип земной поверхности для каждого пикселя соответствующего изображения. В наборе данных присутствуют следующие типы – сельскохозяйственные земли, пастбища, бесплодные земли, здания и сооружения, лесные массивы, водные массивы. Остальные типы поверхности, не входящие в этот перечень, отображаются как неизвестный тип. Маска представляет собой обычное изображение, где значение каждого пикселя кодируется определенным цветом, соответствующим типу поверхности.

Все изображения из исходного набора данных подвергаются предварительной обработке в соответствии с описанной выше процедурой. В результате формируется рабочий набор данных, состоящий из 18336 фрагментов изображений и соответствующих им масок. Полученный рабочий набор разбивается случайным образом на обучающий, валидационный и тестовый наборы данных, которые составляют 60%, 20% и 20% от объема рабочего набора.

Обучение сети

При обучении сети используется метод трансферного обучения. Кодированная часть сети построена на описанной выше модификации архитектуры MobilNet, обученной на

наборе данных ImageNet [11]. Поэтому начальная инициализация весов кодера производится непосредственно весами этой обученной модели. Веса декодирующей части сети инициализируются случайными числами. Такой подход позволяет существенно сократить время, затрачиваемое на обучение предлагаемой сети для сегментации спутниковых изображений.

Для обучения сети используется функция потерь, основанная на коэффициенте Дайса. Он представляет собой метрику сходства двух множеств и вычисляется следующим образом:

$$dsc = 2 * (x \cap y) / (|x| + |y|)$$

где x – предсказанный класс пикселя, а y – истинный класс того же пикселя, полученный из соответствующего канала маски. $|x|$ и $|y|$ – количество элементов в каждом наборе. Тогда соответствующая функция потерь определяется как

$$Loss_dsc = 1 - dsc$$

Для итеративного обновления весов сети в процессе обучения используется алгоритм оптимизации Adam [12]. Этот алгоритм является расширением стохастического градиентного спуска. При обучении сети применялся рекомендуемый параметр скорости обучения равный 10^{-5} , а также применялись алгоритмы автоматического уменьшения скорости обучения и ранней остановки обучения, если потери не снижались в течение нескольких эпох. Сеть обучалась с использованием пакетной нормализации, при этом был экспериментально выбран размер пакета равный 4.

Для сравнения результатов сегментации было также проведено обучение сети с архитектурой Unet, настроенной на работу с теми же изображениями. Обучение этой сети проводилось на том же наборе данных и с теми же метаметрами обучения. При этом в процессе обучения сети Unet настраивается около 31,4 миллиона параметров. Обучение предлагаемой сети MbUnet требует настройки 20,6 миллиона параметров. Таким образом, при использовании предлагаемой сети, вычислительные затраты существенно снижаются. На рисунке 6 показаны графики обучения сети Unet и предлагаемой сети MbUnet. Графики показывают, что предлагаемая архитектура MbUnet, позволила повысить точность сегментации на 3%.

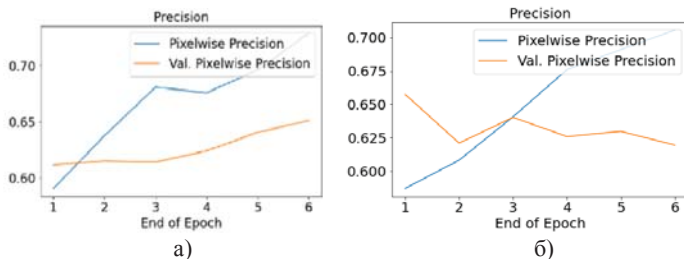


Рис. 6. Графики обучения сетей Unet и MbUnet в зависимости от эпох обучения: а) изменение точности для Unet; б) изменение точности для MbUnet

Тестирование

Тестирование проводилось на тестовом множестве изображений с использованием обученной нейронной сети.

Результатом обработки каждого из тестовых изображений являются 16 частей сегментированного изображения. Каждая из этих частей представляет собой многоканальное бинарное изображение. Количество каналов равно числу сегментируемых типов земной поверхности.

Для визуализации эти многоканальные изображения преобразуются в обычные RGB изображения с помощью таблицы, в которой каждому типу поверхности соответствует определенный цвет. Затем из 16 таких изображений формируется полноразмерное изображение, отражающее результат сегментации. Пример сегментации спутникового изображения показан на рисунке 7.

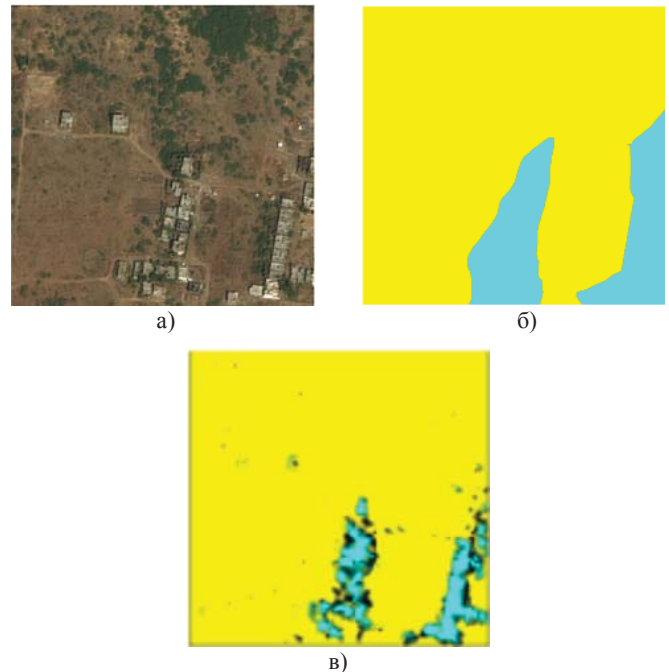


Рис. 7. Пример сегментации спутникового изображения: а) исходное изображение; б) размеченная маска; в) результат сегментации

При тестировании, с помощью соответствующих размеченных масок из тестового набора, определяется также по-пиксельная точность сегментации. Средняя точность на тестовом наборе составила около 64%, что соответствует точности на валидационном наборе, использовавшемся при обучении сети.

Заключение

Предложенный подход позволяет получить достаточно высокую точность сегментации спутниковых изображений по сравнению с существующими решениями. Подход основан на применении архитектуры кодер – декодер аналогичной архитектуре сети Unet. При этом в качестве кодера используется модификация сети MobilNet. В декодере для каждого слоя размерность карт входных признаков повышается с помощью свертки транспонирования и объединяется с картами признаков соответствующего ему слоя кодера и обрабатывается глубокой сверткой.



Применение глубинных сверток как в кодере, так и в декодере, позволило достичь существенного сокращения вычислительных затрат при обучении глубокой нейронной сети и повысить ее быстродействие.

Литература

1. Long J., Shelhamer E., Darrell T. Fully Convolutional Networks for Semantic Segmentation // Proc. of the IEEE Conference on Computer Vision and Pattern Recognition, 2015. pp. 3431-3440, doi: 10.48550/arXiv.1411.4038
2. Badrinarayanan V., Kendall A., Cipolla R. SegNet: A Deep Convolutional Encoder-Decoder Architecture for Image Segmentation. doi: 10.48550/arXiv.1511.00561
3. Ronneberger O., Fischer P., Brox T. U-net: Convolutional networks for biomedical image segmentation // Conf. on Medical image computing and computer-assisted intervention, Springer, Cham, 2015. pp. 234-241, doi: 10.48550/arXiv.1505.04597
4. Simonyan K., Zisserman A. Very deep convolutional networks for large-scale image recognition. doi: 10.48550/arXiv.1409.1556
5. Zeiler M., Taylor G., Fergus R. Adaptive Deconvolutional Networks for Mid and High Level Feature Learning // Proc. of the Int. Conf. on Computer Vision, Washington, DC, USA, IEEE Computer

- Society, 2011., pp. 2018-2025, doi:10.1109/ICCV.2011.6126474.
6. He K., Zhang X., Ren S., Sun J. Identity Mappings in Deep Residual Networks // Computer Vision – ECCV 2016. ECCV 2016. Lecture Notes in Computer Science, vol 9908. Springer, Cham, doi:10.1007/978-3-319-46493-0_
7. Szegedy C., Vanhoucke V., Ioffe S., Shlens J., Wojna Z. Rethinking the Inception Architecture for Computer Vision // IEEE Conf. on Computer Vision and Pattern Recognition, Las Vegas, NV, USA, 2016, pp. 2818-2826, doi: 10.1109/CVPR.2016.308.
8. Tan M., Quoc. V. Le. EfficientNet: Rethinking Model Scaling for Convolutional Neural Networks. doi:10.48550/arXiv.1905.11946
9. Howard A.G., Zhu M., et al. MobileNets – Efficient Convolutional Neural Networks for Mobile Vision Applications. doi: 10.48550/arXiv.1704.04861
10. Boguszewski A., Batorski D., et al. LandCover.ai: Dataset for Automatic Mapping of Buildings, Woodlands, Water and Roads from Aerial Imagery. doi: 10.48550/arXiv.2005.02264
11. Deng J., Dong W., Socher R., Li L.-J., Li K., Li F.-F. ImageNet: A large-scale hierarchical image database // IEEE Conference on Computer Vision and Pattern Recognition, Miami, FL, USA, 2009, pp. 248-255, doi: 10.1109/CVPR.2009.5206848.
12. Kingma D., Ba J. Adam: A Method for Stochastic Optimization. doi: 10.48550/arXiv.1412.6980

DEEP NEURAL NETWORK FOR SEMANTIC SEGMENTATION OF SATELLITE IMAGES

VALERY M. GRISHKIN
 St. Petersburg, Russia

SARDOR I. KARIMOV
 St. Petersburg, Russia

ABSTRACT

Introduction: Semantic segmentation of images obtained from remote sensing of the Earth is a fairly urgent task. Currently, this problem is solved using deep neural networks. However, these networks require large computational costs, both during the training phase and during their use. This paper proposes a neural network architecture that

KEYWORDS: *image segmentation, codec-decoder architecture, deep convolution.*

can reduce these costs and increase the accuracy of semantic segmentation of satellite images. **Result:** The architecture is based on encoder-decoder structures, where deep convolutions are used in the encoder and decoder, which significantly reduces computational costs. The paper presents experimental results showing the effectiveness of the proposed architecture.

REFERENCES

1. J. Long, E. Shelhamer, T. Darrell, "Fully Convolutional Networks for Semantic Segmentation," *Proc. of the IEEE Conference on Computer Vision and Pattern Recognition*, 2015, pp. 3431-3440, doi: 10.48550/arXiv.1411.4038
2. V. Badrinarayanan, A. Kendall, R. Cipolla, "SegNet: A Deep Convolutional Encoder-Decoder Architecture for Image Segmentation", doi: 10.48550/arXiv.1511.00561
3. O. Ronneberger, P. Fischer, T. Brox, "U-net: Convolutional networks for biomedical image segmentation," *Int. Conf. on Medical image computing and computer-assisted intervention*, Springer, Cham, 2015, pp. 234-241, doi: 10.48550/arXiv.1505.04597
4. K. Simonyan, A. Zisserman, "Very deep convolutional networks for large-scale image recognition," doi: 10.48550/arXiv.1409.1556
5. M. Zeiler, G. Taylor, and R. Fergus, "Adaptive Deconvolutional Networks for Mid and High Level Feature Learning," *Proc. of the Int. Conf. on Computer Vision*, Washington, DC, USA, IEEE Computer Society, 2011., pp. 2018-2025, doi:10.1109/ICCV.2011.6126474.
6. K. He, X. Zhang, S. Ren, J. Sun "Identity Mappings in Deep Residual

- Networks," *Computer Vision - ECCV 2016. ECCV 2016. Lecture Notes in Computer Science*, vol. 9908. Springer, Cham, doi:10.1007/978-3-319-46493-0_38
7. C. Szegedy, V. Vanhoucke, S. Ioffe, J. Shlens and Z. Wojna, "Rethinking the Inception Architecture for Computer Vision," *IEEE Conf. on Computer Vision and Pattern Recognition*, Las Vegas, NV, USA, 2016, pp. 2818-2826, doi: 10.1109/CVPR.2016.308.
8. M. Tan, Quoc. V. Le, "EfficientNet: Rethinking Model Scaling for Convolutional Neural Networks," doi: 10.48550/arXiv.1905.11946
9. A. G. Howard, M. Zhu, et al., "MobileNets - Efficient Convolutional Neural Networks for Mobile Vision Applications," doi: 10.48550/arXiv.1704.04861
10. A. Boguszewski, D. Batorski, et al., "LandCover.ai: Dataset for Automatic Mapping of Buildings, Woodlands, Water and Roads from Aerial Imagery," doi: 10.48550/arXiv.2005.02264
11. J. Deng, W. Dong, R. Socher, L.-J. Li, K. Li and F.-F. Li, "ImageNet: A large-scale hierarchical image database," *IEEE Conference on Computer Vision and Pattern Recognition*, Miami, FL, USA, 2009, pp. 248-255, doi: 10.1109/CVPR.2009.5206848.
12. D. Kingma, J. Ba. "Adam: A Method for Stochastic Optimization," doi: 10.48550/arXiv.1412.6980

INFORMATION ABOUT AUTHORS:

Valery M. Grishkin, Candidate of Technical Sciences, Associate Professor, St. Petersburg State University, St. Petersburg, Russia
Sardor I. Karimov, graduate student, St. Petersburg State University, St. Petersburg, Russia

For citation: Grishkin V.M., Karimov S.I. Deep neural network for semantic segmentation of satellite images. *H&ES Reserch*. 2024. Vol. 16. No. 3. P. 12-17. doi: 10.36724/2409-5419-2024-16-3-12-17 (In Rus)

АНАЛИЗ ВОЗМОЖНОСТЕЙ ПРОВЕДЕНИЯ АТАК НА ФУНКЦИИ ПЕРЕДАЧИ УПРАВЛЕНИЯ КОНСОЛЬЮ ОПЕРАЦИОННОЙ СИСТЕМЫ С ПРИМЕНЕНИЕМ МЕТОДОВ АКТИВНОЙ РАЗВЕДКИ

КАЗАРЯН

Михаил Михайлович¹

ЧЕРКЕСОВА

Лариса Владимировна²

РЕШЕТНИКОВА

Ирина Витальевна³

РЕВЯКИНА

Елена Александровна⁴

АННОТАЦИЯ

Введение: В данной работе проведено исследование возможности проведения атак на функции передачи управления консолью с применением методов активной разведки. **Методы:** проводится сканирование портов, перебор директорий, модификация параметров, перебор учётных данных по пользовательскому словарю. В отличие от других исследований, в которых рассматриваются устаревшие методы индикации возможности атак, разработанное авторами средство использует новейшие известные векторы атак. В качестве примера одним из таких векторов является CVE-2018-20062 – уязвимость фреймворка ThinkPHP, позволяющая получить полный контроль над сервером посредством доступа к его консоли. Также можно выделить вектор CVE-2018-12536 – уязвимость компонента DefaultServlet HTTP-сервера Jetty связана с недостатками обработки ошибок при использовании неверных запросов. **Результаты исследования:** эксплуатация уязвимости может позволить нарушителю, действующему удалённо, получить несанкционированный доступ к защищаемой информации путем отображения сообщения InvalidPathException, включенного в отчет об ошибках. Разработанное, в рамках данного исследования, программное средство поставляется в виде двух модулей, в первом модуле содержится основная программа с реализованными в ней механизмами индикации возможности проведения атак, с упором на актуальные на сегодняшний день веб-приложения и сервисы. Проверка на возможность атаки для любого сетевого узла состоит в том, что сначала составляется перечень запросов, целью которых является выявление слабых мест веб-приложения, работающего на сервере, также к данным запросам составляется перечень ожидаемых ответов от сервера. Далее запросы отправляются на сервер, программа ожидает ответы от сервера, и, если ожидаемые ответы из составленного перечня совпадают с действительными, то данный факт сигнализирует о возможности проведения атаки на исследуемое веб-приложение. Во втором модуле хранятся словари локализации, отвечающие за наличие в программе двух языков интерфейса – русского и английского.

Сведения об авторах:

¹⁻⁴ Донской государственный технический университет, Ростов-на-Дону, Россия,
irina_reshetnikova@mail.ru

КЛЮЧЕВЫЕ СЛОВА: информационная безопасность, анализ сетевого трафика, кибератака, сетевые пакеты, активная разведка, вектор атаки.

Для цитирования: Казарян М.М., Черкесова Л.В., Решетникова И.В., Ревякина Е.А. Анализ возможностей проведения атак на функции передачи управления консолью операционной системы с применением методов активной разведки // Научные исследования в космических исследованиях Земли. 2024. Т. 16. № 3. С. 18-29.

doi: 10.36724/2409-5419-2024-16-3-18-29



Введение

Анализ трафика – это необходимое и востребованное направление в реализации защищённой сети, в которую входит, как анализ отдельных пакетов, так и диагностика сложных проблем, с учётом контекста работы исследуемого веб-сервиса. Результаты такого анализа полезны при составлении модели работы сети, так как на сегодняшний день существует реальная угроза массированных хакерских атак.

Анализ трафика можно рассматривать как основной инструмент для перехвата конфиденциальных данных пользователей сети. Сам анализ производится с использованием специализированных программных средств, которые также известны как снифферы (с англ. «нюхачи») [1].

Данный вид ПО выполняет два действия:

1. Собирает все пакеты, проходящие через сетевой узел;
2. Выбирает из собранных пакетов те, где содержится информация об учётных данных пользователя.

На данный момент в публичных сетях достаточно распространены следующие протоколы:

- HTTP – веб-страницы, документы, передача произвольных данных;
- FTP – передача файлов, работа с файловой системой;
- TELNET – предоставление доступа к функциональным возможностям устройства;
- SMTP – отправка и ретрансляция почтовых сообщений между серверами или клиентом и сервером;
- POP3 – получение сообщений с почтового сервера (письмо полностью сохраняется на клиентской стороне и удаляется с сервера);
- IMAP – получение сообщений с почтового сервера (клиенту передается только заголовок письма, по которому можно получить доступ к сообщению, лежащему на почтовом сервере);
- NNTP – получение новостного материала. Обмен данными между серверами новостей;
- IRC – отправка и получение сообщений в режиме реального времени.

Все перечисленные выше протоколы транслируют информацию в незашифрованном виде, либо применяют слабые методы шифрования, поэтому любые сведения, начиная от паролей для доступа к сетевым ресурсам, и, заканчивая коммерческой тайной или личной информацией, будут скомпрометированы при использовании этих протоколов. Также при отсутствии шифрования существует вероятность подмены запроса, отправляемого на сервер, что при некорректной настройке сервера может позволить злоумышленнику необходимые для него сведения или полный доступ к серверу жертвы.

В данной работе поставлены следующие цели:

- показать развитие подходов и методов анализа с исторической точки зрения;
- выделить популярные техники анализа трафика, которые используются в большинстве программных решений;
- провести обзор на программные средства для анализа трафика;
- реализовать программный модуль, производящий поиск уязвимостей в сетевых узлах;

Методы и материалы

Существует два основных направления развития технологий анализа сетевого трафика:

- Увеличение качества исследования изучаемого сетевого пакета, другими словами – повышение уровня модели OSI, данные которой анализируются;
- Получение на выходе исчерпывающей информации о характеристиках потока, к которому относится пакет, и других потоков, связанных с данными.

В следующих разделах будут рассмотрены оба этих направления развития.

Глубина анализа сетевых пакетов



Рис. 1. Уровни развития технологии анализа сетевого трафика по «глубине»

Согласно данной модели, технологические процессы изучения трафика формировались поочередно, любой дальнейший процесс наследовал долю предшествующих элементов, а также добавлял собственные. Можно отметить три степени формирования технологических процессов [2], которые приведены на рисунке 1.

Рассмотрим эти уровни более детально.

Поверхностный анализ пакетов (SPI)

Данная технология проверяет заголовки пакетов (которые представляют собой информацию, размещенную в начале блока данных, такую как IP-адреса отправителя и получателя), в отличие от тела или “полезной нагрузки” пакета. Этот вид проверки пакетов позволяет сообщениям оставаться нескомпрометированными, поскольку содержимое пакетов не отслеживается, а информация в заголовке используется только для маршрутизации пакета. Технологии SPI управляют (относительно) упрощенными брандмауэрами, работающими в операционных системах Windows XP, Windows Vista и OS X. Эти брандмауэры стоят между конкретным клиентским компьютером и сетью, к которой он подключен.

Они ограничивают возможность отправки или получения указанного пользователем содержимого клиентским компьютером. Когда сервер отправляет пакет на клиентский компьютер, технологии SPI проверяют информацию о заголовке пакета и сравнивают его с черным списком. Эти брандмауэры, в частности, фокусируются на IP-адресах источника и назначения, к которым пытается получить доступ пакет. Если в пакете находится заголовок, параметры которого числятся в черном списке, то такой пакет не будет доставлен. Когда технология SPI отказывается доставлять пакет, она просто отказывается передавать его без уведомления источника о том, что пакет был отклонен [3].

Анализ пакетов на транспортном и сеансовом уровнях (MPI)

Работает, как прокси-сервер, который находится между компьютерами конечных пользователей и интернет – провайдером или интернет-шлюзом. Эти прокси-серверы могут проверять информацию заголовка пакета по своему проверочному списку синтаксического анализа. Когда пакет поступает на прокси-сервер, он анализируется по списку синтаксического анализа, который системные администраторы могут легко обновить. Список синтаксического анализа позволяет разрешать или запрещать определенные типы пакетов в зависимости от их типов формата данных и их соответствующего расположения в Интернете, а не только от их IP-адреса.

Устройства MPI могут считывать уровень представления полезной нагрузки пакета и идентифицировать аспекты данного уровня. Используя устройства MPI, администраторы могут запретить клиентским компьютерам получать флэш-файлы с YouTube или файлы изображений с сайтов социальных сетей. Технологии MPI могут определять приоритетность одних пакетов перед другими, изучая команды приложения, расположенные на уровне приложений, и форматы файлов на уровне представления. Устройства MPI страдают от плохой масштабируемости, что ограничивает их полезность для интернет – провайдеров, где десятки тысяч приложений могут передавать пакеты в любой момент времени [4].

Этот метод позволяет решать более широкий круг задач, помимо настройки прав доступа, данная технология также справляется со следующими задачами:

- сохранение данных трафика в кеш;
- изучение трафика, который был подвержен шифрованию или сжатию;
- возможность наложения запрета на выполнение отдельных команд;
- в случае работы в режиме прокси-сервера, может служить как оптимизатор подключения к Интернету.

Существенный минус технологии MPI заключается в том, что на каждую команду и протокол необходим свой входной-выходной порт. Помимо этого, режим работы прокси потребляет много процессорного времени, что снижает быстродействие системы в целом. Для оптимизации работы прокси-сервера был создан протокол ICAP, идея которого заключалась в том, чтобы переложить процедуру проверки безопасности пакетов на сторонние серверы. Такая система организована в антивирусном продукте ClamAV, который может подключаться к прокси-серверам Squid и NetCache [5].

Данные условия значительно ограничивают возможность использования этой технологии на уровне провайдеров, учитывая большую ширину их каналов связи и множество обрабатываемых протоколов.

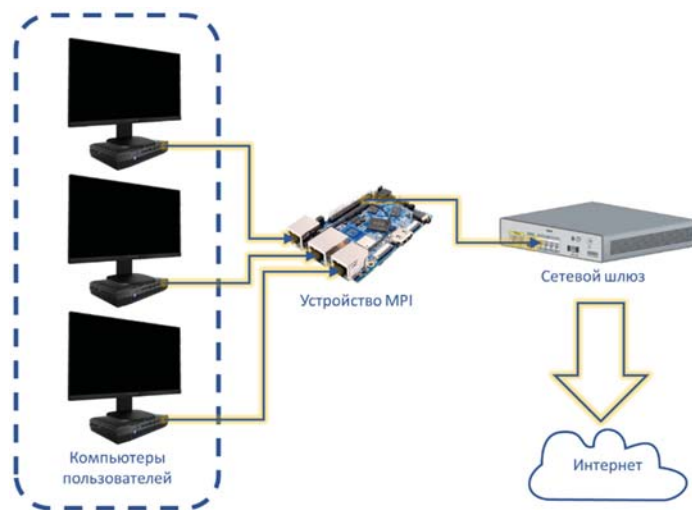


Рис. 2. Схема применения устройств анализа на основе технологии MPI

Глубокий анализ пакетов (DPI)

Также используют более специфичное название – DPP (Deep Packet Processing), данная технология производит над пакетом следующие действия:

- модификация;
- фильтрация;
- перенаправление.

На данный момент оба названия имеют одинаковый смысл. Такой вид анализа можно назвать закономерным приемником MPI. В этой системе парсер считывает содержимое пакета полностью, решение по дальнейшей судьбе пакета принимается не только исходя из данных, лежащих в пакете, но и исходя из специфики сетевых программ и протоколов. Для этих целей могут использоваться вероятностные данные.

Например, проведение опыта по установлению числа встреч определенных символов, размеров пакетов, время задержки между поступлением пакетов. Метод DPI стал широко распространен по причине резкого увеличения вычислительных мощностей процессоров, скорости их памяти и, конечно же, из-за высокой степени точности анализа [6].

В противовес MPI, этот метод создавался для быстрой обработки и определения множества приложений в реальном времени. Отсюда следует, что DPI обладает хорошими способностями к расширению по сетевым каналам, также в базе данного решения содержатся тысячи известных сетевых приложений. В любом реализуемом проекте DPI выступает, как модуль, устанавливающий соответствие пакета к классу протоколов сети. Также стоит отметить, что точность этой операции зависит от целей, возложенных на систему:

- тип протокола или программы (например, Web, Peer-to-Peer, VoIP);
- определенный протокол уровня приложения (HTTP, BitTorrent, SIP-телефония);

• приложение, использующее протокол (Google Chrome, µTorrent, Skype).

Важно отметить, что соответствие между классами различных уровней точности не однозначно, что показано на рисунке 3.

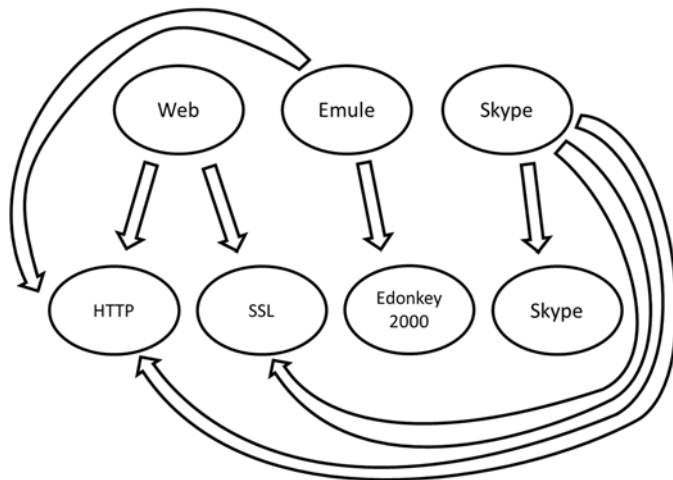


Рис. 3. Различия между идентификацией приложений (сверху) и протоколов (снизу)

Сегодня глубокий анализ пакетов – это стандарт для программ, сканирующих трафик. Такой вид приложений относится к области крайне важных решений в сфере сетевой безопасности, особенно с точки зрения буквы закона. Так, за последние несколько лет было утверждено множество стандартов, технических условий и рекомендаций. Несмотря на то, что данный метод и не сыскал популярности в межсетевых экранах, но существуют решения, использующие данную технологию. Например, экраны Hogwash и Shield [5, 6].

В качестве следующего ответвления в сфере анализа можно выделить учёт поведения потока пакетов в сети, в данной группе существует два метода исследования трафика:

- с учетом состояния в потоке;
- без учета состояния в потоке.

Это применимо только к протоколам, которые осуществляют соединение при помощи транспортного протокола. То есть перед наладкой канала для передачи данных происходит процесс «установления соединения», где абоненты производят обоюдную передачу специальной цепочки пакетов, получившей название «рукопожатие», по окончании процесса передачи данных соединение закрывается. К такому виду протоколов относятся:

- Протокол передачи данных (TCP);
- UDP (при условии, что поверх него организован протокол с установлением соединения, например, протокол QUIC).

Следовательно, исключать метод исследования трафика с учетом состояния установления соединения для UDP пакетов невозможно [6].

Чтобы дать точную характеристику вышеизложенным методам, необходимо раскрыть такое понятие, как «поток пакетов». Встречаются разнообразные трактования этого явления. Информация о самых распространенных из них изложена на веб-странице суперкомпьютерного центра Сан-Диего

(SDSC). Рассмотрим однонаправленный поток транспортного уровня. В самом потоке можно выделить следующие характеристики:

- IP-адрес источника;
- порт источника;
- IP-адрес конечного узла;
- порт конечного узла;
- протокол.

Опираясь на данную модель, легко установить, в чем заключается отличие подхода исследования трафика с учетом состояния в потоке и без учета состояния в потоке. В первом случае в расчет берутся сведения о том, каком потоку принадлежит исследуемый пакет, а также учитывается информация, полученная в процессе изучения предыдущих ранее пакетов, относящихся к этому же потоку. Стоит заметить, что метод анализа трафика с учетом состояния в потоке имеет весьма нечеткое определение. Поэтому такой метод от одной реализации к другой может иметь различную точность, качество оптимизации, быстродействие [7]. Возможный на практике вариант градации продемонстрирован на рисунке 4.



Рис. 4. Градации полноты учёта состояния в потоке

Перечень степеней исследования состояния в потоке, представлен следующими уровнями:

- исследование некоторых пакетов, игнорируя потоки и состояния (Packet Based No State, PBNS);
- исследование пакетов по потокам (Packet Based Per Flow State, PBFS);
- исследование данных в пределах одного потока (Message Based Per Flow State, MBFS), т.е. совершен сбор IP-фрагментов в IP-пакеты (IP- нормализация) и сборка TCP-сегментов в TCP-сеансы (TCP- нормализация);
- исследование данных в рамках протокола (Message Based Per Protocol State, MBPS), т.е. принимается во внимание состояние автомата протокола (его способность к работе с различными типами данных). Пример автомата состояний протокола HTTP приведён на рисунке 5. Вершины соответствуют состояниям, рёбра – условиям перехода, к которым могут относиться получение и передача данных, результаты их обработки, истечение таймаута.

Обычно, разработки, использующие метод DPI, имеют отношение к исследованию без учета состояния в потоке – анализ производится лишь над отдельными пакетами в одном потоке без сохранения состояния между их исследованиями.

– база данных, содержащая статистические данные, информацию о проверке пакетов, а также журналы, содержащие сведения о доступе к ресурсам системы. Также DPI возможно использовать, как средство для сбора полезной информации, межсетевое экрана или как система обнаружения и предотвращения вторжений.

Далее будет продемонстрирован базовый алгоритм действия инфраструктурных методов исследования сетевого трафика, который используется на практике в слабоизмененном виде. Также будут рассмотрены стадии исследования с кратким перечнем их характеристик.



Рис. 6. Схема использования системы DPI для применения политик к сетевому трафику

Базовый алгоритм инфраструктурных методов исследования сетевого трафика

Базовый алгоритм исследования сетевых пакетов, подразделяется на следующие этапы, которые проградированы по степени представления объекта исследования:

1. Сбор данных, находящихся в исследуемых сетевых подключениях. Итогом данного этапа являются полученные пакеты:

- Частичное исследование пакетов – вид анализа, при котором рассматривается не все содержимое пакета, а лишь его некоторая часть. Практика применения такого вида исследования показала его эффективность в решении задачи определения протокола пакета;
- Отбор пакетов по заданным параметрам подразумевает перехват пакетов, удовлетворяющих им, исходя из настроек безопасности системы. С течением времени, данная технология обросла большим количеством методов отбора [12];
- Для систем, где необходима высокая точность исследования трафика, необходимо считывать данные проходящего через узел трафика полностью [13].

2. Распределение пакетов по потокам, с опорой на информацию об их источнике. Такое исследование подразделяется на два вида:

- с учетом данных пакета;
- с учетом данных потока.

Их отличия продемонстрированы на рисунке 7. Анализ с учетом данных потока наиболее распространен по причине низких требований к аппаратной части, что вызвано малым объемом обрабатываемых данных. Данный способ анализа позволяет работать с пакетами, как локально, так и удаленно.

Чтобы передать данные из места сбора до места анализа задействуется множество протоколов. Список данных, записываемых при анализе, может быть разным от реализации к реализации, однако, можно выделить основные данные, которые используются наиболее часто [14]:

- IP адреса источника и адресата;
- протокол транспортного уровня;
- в случае протоколов TCP/UDP – номера портов источника/адресата [15];
- набор счётчиков: количество переданных пакетов и байт, время создания и завершения потока.



Рис. 7. Различия типичных схем packet (слева) и flow-based (справа) анализа

Стоит заметить, что этот способ достаточно экономно распоряжается ресурсами аппаратной части, но он недостаточно гибок – не позволяет устанавливать число принимаемых данных. Также, во множестве практических задач число потоков не многим меньше числа пакетов, по причине наличия множества непродолжительных потоков, состоящих из небольшого числа пакетов [16]. Чтобы регулировать число таких потоков, была применена технология отбора пакета по заданным условиям.

Однако, по причине ограниченности памяти, устройство не сможет собирать данные одного потока бесконечное количество времени. Поэтому в данной системе вводится параметр, ограничивающий максимальную продолжительность исследования.

3. Выполнение разделения пакетов по протоколам прикладного уровня или веб-приложению. В качестве объекта для исследования выступает поток сети протокола или приложения. Далее над объектом могут производиться дополнительные преобразования, характер которых напрямую связан с решаемой прикладной задачей. В общем случае можно выделить следующие преобразования [17]:

- разбор полей протокола (protocol parsing);
- сборка сессии протокола для протоколов с установленным соединением;
- извлечение данных приложения (content extraction) – страниц сайтов (HTML), файлов различных типов (исполняемые, изображения, текстовые документы, и т.д.), электронных писем, аудио-видео потоков и т.д.;
- разбор данных приложения (application content parsing).

Дополнительно стоит обратить внимание на то, что кроме данных подходов есть другой источник информации о сетевом трафике – это иерархически организованные сведения, доступ к которым происходит при помощи протокола управления сетью [18].

Приложения для сбора, хранения и передачи данных в формате MIB используются во множестве устройств. Обмен информацией происходит по протоколу SNMP. Сведения, получаемые данным способом, обладают небольшим размером и не связаны с каким-либо протоколом. В качестве примера таких характеристик, можно привести сведения о числе пакетов и общем числе байт, прошедших через определенный интерфейс сети на определенном устройстве.

Также стоит заметить, что причиной роста популярности технологий MIB и распределения пакетов по потокам являются споры о законности глубокого анализа трафика, так как исследование трафика с такой точностью посягает на права частной жизни. Поэтому в различных научных трудах, трафик перед проведением высокоточного анализа шифруется с использованием средств защиты информации [19].

Результаты

Разработка программного средства анализа возможностей проведения атак на функции передачи управления консолью операционной системы с применением методов активной разведки

В качестве среды разработки была выбрана IDLE (Integrated Development and Learning Environment) – это интегрированная среда для разработки (и обучения), которая поставляется вместе с Python. Сама IDLE написана на Python с использованием библиотеки Tkinter, поэтому является кроссплатформенным приложением (может работать на Windows, Mac OS, Linux).

Так же IDLE можно представить как текстовый редактор с подсветкой синтаксиса, автозаполнением, умным отступом и другими функциями для удобства написания кода на Python.

Для разработки графической части программы была выбрана библиотека tkinter – кроссплатформенная библиотека для разработки графического интерфейса на языке Python. Она входит в стандартный пакет библиотек Python.

Данная библиотека обладает следующими достоинствами:

- Поддержка встроенных в Windows форм, окон и элементов;
- Наличие трёх видов упаковщиков (Выравнивание элементов: по краю, по сетке или принудительное присвоение координат);
- Лаконичность кода по сравнению с WinAPI.

Описание работы и тестирование программы

Разработанное программное средство представляет собой утилиту, которая проверяет хосты на наличие уязвимостей функций передачи управления в работающих на них приложениях или веб-сервисах, путем проведения активной разведки – проверки наличия открытых портов, анализа ответа сервера на запросы с искаженными указателями данных.

Данный продукт состоит из следующих модулей:

- список `ip_list` – хранит введенные ip-адреса или ip-маски подсетей;
- список `port_list` – хранит введенные порты;
- список `scan_results_1` – хранит результаты сканирования;

- переменные семейства `main_` – хранят параметры кнопки графического интерфейса и экземпляр объекта главного окна;
- переменная `langs` – импортирует из модуля `languages` список доступных языков;
- список `scan_sets` – хранит настройки выбора активных модулей;
- переменная `progress` – хранит процентное значение выполнения сканирования для индикации хода выполнения программы;
- `operations` – расчетная переменная, хранящая в себе число запланированных к выполнению операций;
- `step` – расчетная переменная, хранящая в себе величину шага для индикации хода выполнения программы;
- `hnap_timer` – переменная, фиксирующая задержку между отправляемыми запросами;
- функция `progr_add` – отвечает за обновления информации о ходе выполнения сканирования и показаний индикатора;
- `proxy_pump` – класс, подготовленный для запуска в режиме многопоточной обработки, отвечает за поиск небезопасных прокси-серверов;
- `proxy_scan` – функция запуска сканирования прокси-серверов;
- `hnap_pump` – класс, подготовленный для запуска в режиме многопоточной обработки, отвечает за поиск устройств с уязвимостью по протоколу H NAP;
- `hnap_scan` – функция запуска сканирования уязвимости H NAP;
- `ThinkPHP_pump` – класс, подготовленный для запуска в режиме многопоточной обработки, отвечает за поиск устройств с уязвимостью в веб-приложении ThinkPHP;
- `ThinkPHP_scan` – функция запуска сканирования уязвимости в ThinkPHP;
- `MyAdmin_pump` – класс, подготовленный для запуска в режиме многопоточной обработки, отвечает за поиск устройств с уязвимостью в веб-приложении phpMyAdmin;
- `MyAdmin_scan` – функция запуска сканирования уязвимости в phpMyAdmin;
- `BruteForce_pump` – класс, подготовленный для запуска в режиме многопоточной обработки, отвечает за перебор учетных данных в формах входа;
- `BruteForce_scan` – функция запуска перебора;
- `HJS_pump` – класс, подготовленный для запуска в режиме многопоточной обработки, отвечает за поиск небезопасных Hudson Java серверов;
- `HJS_scan` – функция запуска сканирования Hudson Java сервера;
- `SQLite_pump` – класс, подготовленный для запуска в режиме многопоточной обработки, отвечает за поиск небезопасных SQLite серверов;
- `SQLite_scan` – функция запуска сканирования SQLite серверов;
- `scan_sets_ind` – функция, устанавливающая флаги в меню выбора модулей сканирования;
- `is_port_valid` – функция, проверяющая правильность ввода номера порта;



- `is_ip_valid` – функция, проверяющая правильность ввода ip-адреса;
- функции `value_input_wnd` – выполняет отображение различных окон-приглашений ко вводу данных;
- функция `refresh_ip_port` – сохраняет обновленную информацию о перечне сканируемых ip-адресов и портов;
- функции семейства `scan_` – отвечают за работу окон настроек сканирования, выбора подключаемых модулей;
- функция `language_change` – отвечает за перезапуск главного окна, при смене языка;
- функция `language_settings` – отвечает за работу окна настроек языка;
- функция `main_window` – отвечает за работу окна главного меню.

Состав вспомогательного модуля `languages.py`:

- словарь `LOCALIZED_STRINGS` – содержит в себе строки локализации для русского и английского языков.

Модули, отвечающие за проведение поиска уязвимостей, работают в рамках теории принятия решений, в частности, производится решение вероятностной задачи, которая выражена следующими условиями:

$$\begin{cases} P = \left(\frac{1}{N}\right)^k \\ P > x \end{cases}$$

где P – это вероятность возможности существования уязвимости, k – число успешных проверок на уязвимость, N – общее число проверок, реализованных в модулях, x – значение вероятности, в случае превышения которого, есть основание полагать о существовании уязвимости.

Каждый из этих модулей работает по следующей схеме (рис. 8).

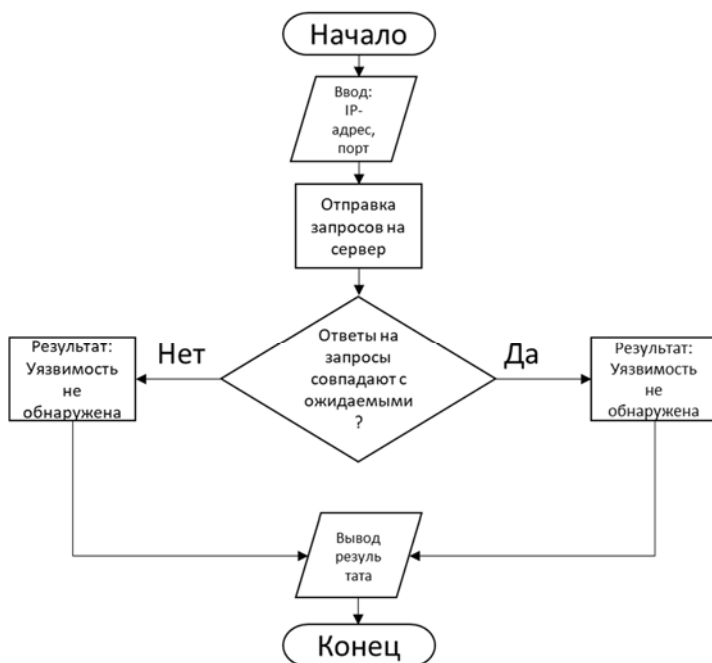


Рис. 8. Общая блок-схема работы модуля сканирования уязвимости

При запуске программы пользователю становится доступно главное окно (рис. 9), где есть возможность перейти к настройкам сканирования, указать список модулей для сканирования, а также запустить сканирование и просмотреть результаты его работы

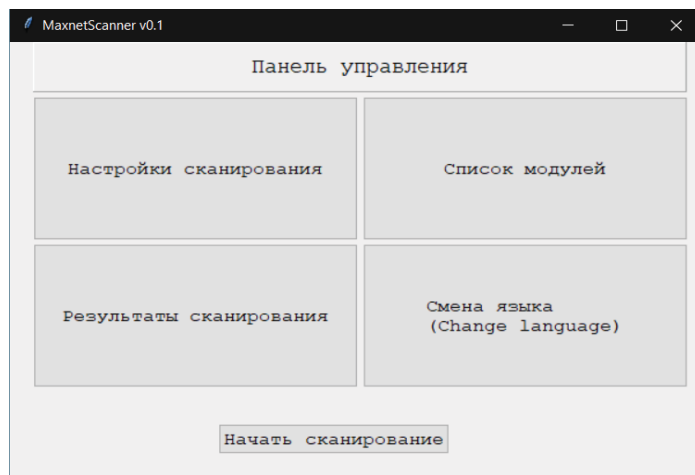


Рис. 9. Главное окно программы

В окне настроек сканирования пользователю предоставляется возможность добавления IP-адресов узлов и номеров портов для сканирования (рис. 10).

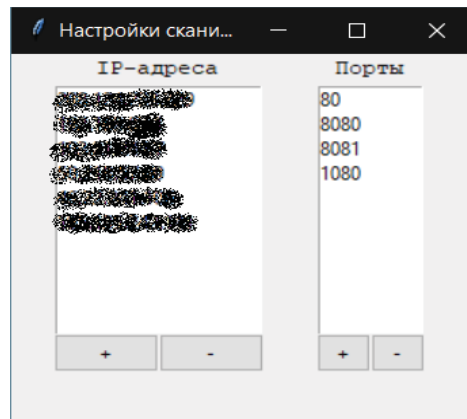


Рис. 10. Окно настроек параметров сканирования

Выбор модулей для сканирования узлов в сети возможен при помощи окна выбора модулей, доступного из главного меню, пункт «Список модулей» (рис. 11).

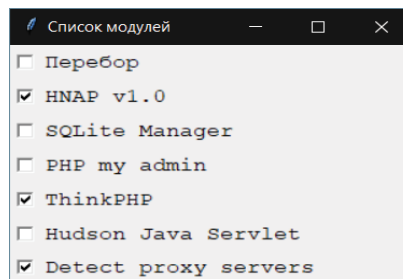


Рис. 11. Окно выбора модулей

Стоит отметить, что в отличие от Router Scan, данный продукт запускает модули параллельно и выводит результаты работы модулей раздельно, что позволяет получить более детальную картину о наличии возможных уязвимостей.

Результаты сканирования записываются в специальную таблицу, которая доступна из главного меню по нажатию кнопки «Результаты сканирования» (рис. 12).

IP-адрес	Порт	Состояние	Комментарии
	8089	Успех	ThinkPHP
	80	Успех	Прокси-сервер
	8089	Успех	Прокси-сервер
	8089	Успех	Стандартный набор инстр
	443	Успех	Прокси-сервер
	80	Успех	Прокси-сервер
	8081	Успех	Расширенный набор инс
	8081	Успех	Прокси-сервер
	8081	Успех	Прокси-сервер
	8089	Успех	phpMyAdmin
	8089	Успех	Небезопасный SQLite Man
	8089	Успех	Небезопасный HJS
	8081	Успех	Успешный вход с admin:1

Рис. 12. Окно демонстрации результатов поиска уязвимостей

При запуске сканирования откроется специальное окно, в котором пользователю демонстрируется ход выполнения работы, путем заполнения индикатора выполнения, в соответствии с процентом завершения запущенного сканирования (рис. 13).

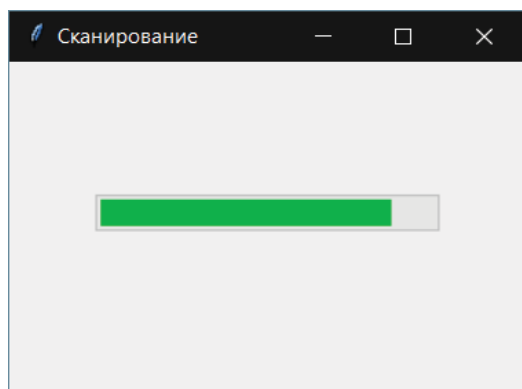


Рис. 13. Окно индикатора выполнения сканирования

Также в программе реализована возможность смены языка, для этого необходимо в главном окне выбрать пункт «Смена языка (Change language)», вид окна выбора языка показан на рисунке 14.

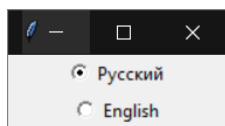


Рис. 14. Панель выбора языка

При выборе языка произойдет перезапуск главного окна для смены строк локализации.

Сравнение с аналогами

В настоящий момент существует множество различных уязвимостей в действующих системах и устройствах. Среди них можно выделить особо распространенные бреши, которые несут наибольшую опасность для пользователей [20-23].

HNAP (Home Network Administration Protocol) – протокол управления домашней сетью, созданный компанией Pure Networks. Дает возможность управлять устройствами сети. В данном протоколе были обнаружены серьезные проблемы безопасности в плане разграничения доступа к объектам системы, поэтому устройства, вышедшие на рынок после 2016 года, более не поддерживают этот протокол.

SQLite Manager – система управления SQLite сервером, реализованная на PHP. Уязвима к выполнению произвольного PHP кода, путем добавления последнего в параметры запроса.

Hudson Java – это серверы семейства Hudson Ci и Jenkins Ci, написанные на Java. Данные системы являются инструментами для непрерывной разработки. Поддержка данного ПО была прекращена в 2016 году. Уязвимы к выполнению произвольного Java кода.

phpMyAdmin – веб-приложение, реализованное на PHP, его основная задача – администрирование базы данных на MySQL. Подвержена атакам типа XSS, SQL инъекциям и эксплоитам, позволяющим выполнение произвольного кода.

ThinkPHP – это облегченная среда разработки веб-приложений на PHP. В конце 2018 года была обнаружена уязвимость, связанная с использованием метода invokeFunction в теле GET-запроса, что позволяет запускать произвольный код на сервере. Несмотря на выпуск патчей, данная проблема до сих пор выявляется в новых версиях этого фреймворка [24].

В таблице представлено сравнение по возможностям проведения различных атак и работоспособности на различных системах разработанного программного средства с существующими программными продуктами:

Таблица 1

Сравнительный анализ программных средств

Программы Исследуемые возможности	RouterScan	MaxnetScanner	Patratror	Retina
Поддержка Windows	+	+	+	+
Поддержка Linux	+	+	+	+
Перебор	+	+	+	-
HNAP	+	+	-	+
PhpMyAdmin	+	+	+	+
ThinkPHP	-	+	+	-
Hudson Java Servlet	+	+	+	-
SQLite Manager	+	+	+	+
Обнаружение прокси-серверов	+	+	-	+

Также были проведены практические испытания, по качеству поиска уязвимостей и затраченному времени на их обнаружение для каждого рассматриваемого программного продукта.



Все тесты проводились в выделенной для испытаний локальной сети. Для достижения максимальной объективности исследования были подобраны веб-приложения, которые могут обладать уязвимостями, обрабатываемыми в рассматриваемых программных продуктах.

Таким образом, в локальной сети были задействованы: два маршрутизатора с поддержкой небезопасной версии HNAP, 5 серверов с администрированием при помощи phpMyAdmin, два сервера с фреймворком ThinkPHP, три сервера на Java с расширением Hudson servlet, два SQLite сервера и один прокси-сервер, работающий без шифрования передаваемых данных. Результаты исследования представлены на следующих диаграммах (рис. 15, 16):



Рис. 15. Диаграмма числа найденных программами уязвимостей

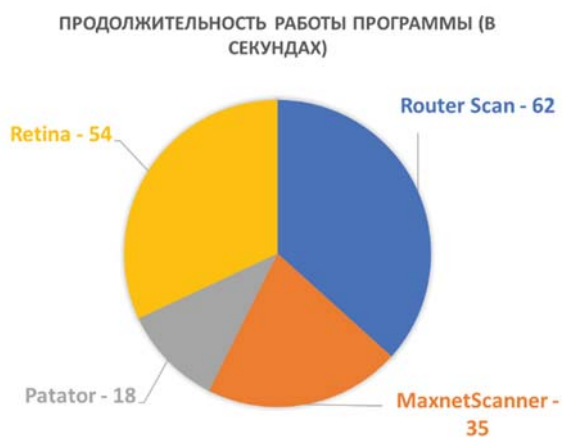


Рис. 16. Диаграмма времени работы программ в тестовой локальной сети

В результате проведения исследования было установлено, что полученное в процессе разработки программное средство MaxnetScanner лучше всего показало себя в тестировании систем на предмет наличия в них уязвимости фреймворка ThinkPHP и сервера Hudson Java Servlet, по остальным показателям разработанная программа уступила лишь незначительно в обнаружении уязвимостей в веб-приложении phpMyAdmin.

По быстрдействию полученный программный продукт занял второе место среди исследуемых.

Таким образом, исходя из информации, представленной в таблице 1 и на рисунках 15 и 16, программный продукт MaxnetScanner, который был разработан в рамках текущего исследования, показал себя конкурентноспособным, превзойдя в некоторых аспектах существующие на рынке программные решения.

Обсуждение

Результатом данной работы является программное обеспечение MaxNetScanner2022, которое выявляет возможность осуществления атаки на функции передачи управления системой, с применением активных средств разведки. Стоит отметить, что данный вид атак достаточно распространен в сети и включает в себя такие методы как: подмена данных в запросе, передача в тело запроса символов, которые сервер может считать без их экранирования, что может вызвать неадекватное поведение веб-приложения и дать возможность выполнять на стороне удаленного сервера код злоумышленника.

Авторы этого исследования описывают современные подходы к анализу трафика, они приходят к выводу, что выбор метода анализа должен исходить из целесообразности применяемых средств, относительно конкретной задачи, то есть необходимо учитывать размер затрат на анализ, и адекватность его глубины в плане нагрузки на исследуемую систему. Также авторы отмечают, что атаки с применением активных средств разведки являются наиболее опасными по причине того, что они имеют характер массовости, могут распространять вредоносное программное обеспечение и способны destabilизировать работу системы при помощи простой множественной отправки запросов, которые сервер не может обработать без ответа и тратит свое процессорное время на их обработку.

Изучив свежие статьи об атаках на функции передачи управления системой, авторы сделали заключение, что современные веб-приложения могут быть подвержены таким атакам с применением средств активной разведки, так как на сегодняшний день большинство компаний и различного рода сообществ уделяет недостаточно внимания настройке и тестированию серверов, веб-приложений и сетевых экранов.

Заключение

Результатом проделанной работы является программная реализация модуля, производящего поиск уязвимостей в сетевых узлах.

По ходу выполнения работы были изучены теоретические основы анализа трафика, развитие подходов и методов анализа, а также рассмотрены существующие на сегодняшний день программные решения.

Проанализированы и пошагово описаны алгоритмы анализа трафика.

В программе были реализованы:

- графический интерфейс;
- актуальные шаблоны поиска уязвимостей;
- параллельная работа модулей.

Таким образом, поставленные в научной работе задачи были выполнены, а цели достигнуты. Опыт, полученный в

ходе выполнения исследования и приобретенные навыки, будут полезны в дальнейшем обучении и профессиональной деятельности.

Литература

1. Sniffer. https://www.opennet.ru/base/sec/arp_snif.txt.html, дата обращения 01.06.2022.
2. Lin Y., Lin P. et al. Guest Editorial Deep Packet Inspection: Algorithms, Hardware, and Applications // Proc. IEEE Journal on Selected Areas in Communications, 2014, pp. 1781-1783.
3. Рекомендация МСЭ-Т Y.2770 “Требования к углубленной проверке пакетов в сетях последующих поколений” издание 1.0, 20.11.2012.
4. Рекомендация МСЭ-Т Y.2771 “Структура углубленной проверки пакетов”, 01.07.2014.
5. Рекомендация МСЭ-Т Y.2772 “Механизмы сетевых элементов”, 29.04.2016
6. Рекомендация МСЭ-Т Y.2773 “Модели и метрики рабочих характеристик углубленной проверки пакетов”, 17.02.2017.
7. Филимонов П., Иванов М. Современные подходы к классификации трафика физических каналов сети Интернет // Труды 18-ой Международной конференции (DCCN-2015), 19-22 октября 2015 г. С. 466-474.
8. Yichiet A., Selvakumar M., Shankar K. A temporal-aware signature extraction method using sliding-window mechanism for scalable, cost-effective and accurate traffic classification // Proc. IEEE ICCSCE, 2017, pp. 156-161.
9. Bosshart P., Daly D., Gibb G. et al. “Programming protocol-independent packet processors. SIGCOMM Computer Communications Review”, 2013.
10. Bremner-Barr A., Harchol Y., Hay D., Koral Y. Deep packet inspection as a service // CoNEXT, 2014, pp. 271-282.
11. Gerald C., Gilbert R., Thomas B. Wireshark Go Deep. 2006. Available online: <https://www.wireshark.org/> (accessed on 01 Jun 2022). дата обращения 01.06.2022.
12. Srisuresh P., Holdrege M. IP Network Address Translator (NAT) Terminology and Considerations. RFC 2663, IETF. 1999. Available online: <https://www.hjp.at/doc/rfc/rfc2663.html> (accessed on 1 Jun 2022), дата обращения 01.06.2022.
13. Software NAT. <http://www.nat32.com/v2/>, дата обращения 01.06.2022.
14. DDoS. <http://ddos-protection.ru/chto-takoe-ddos>, дата обращения 01.06.2022.
15. IANA Service Name and Transport Protocol | Port Number Registry. <http://www.iana.org/assignments/service-names-port-numbers/service-names-port-numbers.xhtml>, дата обращения 01.06.2022.
16. Afek Y., Bremner-Barr A., Harchol Y., Hay D., Koral Y. MCA2: multi-core architecture for mitigating complexity attacks // ANCS, pp. 5-6, 2012.
17. Nguyen X.-H., Nguyen X.-D., Huynh H.-H., Le K.-H. Realguard: A Lightweight Network Intrusion Detection System for IoT Gateways // Sensors, 2022, no. 22, 432. <https://doi.org/10.3390/s22020432>.
18. Abro G.E.M., Zulkifli S.A.B.M., Masood R.J., Asirvadam V.S., Laouti A. Comprehensive Review of UAV Detection, Security, and Communication Advancements to Prevent Threats // Drones 2022, no. 6, 284.
19. Oruc A., Amro A., Gkioulos V. Assessing Cyber Risks of an INS Using the MITRE ATT&CK Framework // Sensors 2022, no. 22, 8745.
20. Router Scan v2.60 Beta by Stas'M. Available online: <http://stascorp.com/load/1-1-0-56> (дата обращения 01.06.2022).
21. <https://drweb.datasystem.ru/catalog/view/645/>, дата обращения 01.06.2022.
22. BeyondTrust. Retina Network Security Scanner. Available online: <https://www.beyondtrust.com/products/retina-network-security-scanner/>, дата обращения 01.06.2022.
23. Электронный сборник статей по материалам XXX студенческой международной научно-практической конференции. Новосибирск: Изд. «СибАК». 2015. № 3 (29) [Электронный ресурс]. Режим доступа. URL: [http://www.sibac.info/archive/Technic/3\(29\).pdf](http://www.sibac.info/archive/Technic/3(29).pdf)
24. Albalawi M., Aloufi R., Alamrani N., Albalawi N., Aljaedi A., Alharbi A.R. Website Defacement Detection and Monitoring Methods: A Review // Electronics 2022, no. 11, 3573.

ANALYSIS OF ATTACKS POSSIBILITIES ON THE OPERATING SYSTEM CONTROL TRANSFER FUNCTION USING ACTIVE INTELLIGENCE METHODS

MIKHAIL M. KAZARYAN

Don State Technical University, Rostov-on-Don, Russia

LARISA V. CHERKESOVA

Don State Technical University, Rostov-on-Don, Russia

IRINA V. RESHETNIKOVA

Don State Technical University, Rostov-on-Don, Russia,
irina_reshetnikova@mail.ru

ELENA A. REVYAKINA

Don State Technical University, Rostov-on-Don, Russia

ABSTRACT

Introduction. This paper examines the possibility of carrying out attacks on console control transfer functions using active reconnaissance methods. Ports are scanned, directories are searched, parameters are modified, and credentials are searched through a user dictionary. Unlike other studies that consider outdated methods for indicating the possibility of attacks, the tool developed by the authors uses the lat-

KEYWORDS: information security, network traffic analysis, cyber attack, network packets, active intelligence, attack vector.

est known attack vectors. **Methods:** as an example, one such vector is CVE-2018-20062, a vulnerability in the ThinkPHP framework that allows you to gain full control over the server by accessing its console. You can also highlight the vector CVE-2018-12536 – a vulnerability in the DefaultServlet component of the Jetty HTTP server is associated with deficiencies in error handling when using invalid requests. Exploitation of the vulnerability could allow a remote attacker to gain unauthorized access to protected information by displaying an InvalidPathException



message included in the error report. **Results:** The software developed as part of this research is supplied in the form of two modules; the first module contains the main program with mechanisms implemented in it to indicate the possibility of attacks, with an emphasis on currently relevant web applications and services. Checking for the possibility of an attack for any network node consists of first compiling a list of requests, the purpose of which is to identify the weak points of a web application running on the server, and also compiling a list of expected responses

from the server for these requests. Next, requests are sent to the server, the program waits for responses from the server, and if the expected responses from the compiled list coincide with the actual ones, then this fact signals the possibility of an attack on the web application under study. The second module stores localization dictionaries, which are responsible for the presence of two interface languages in the program – Russian and English.

REFERENCES

1. Sniffer. https://www.opennet.ru/base/sec/arp_snif.txt.html, дата обращения 01.06.2022.
2. Y. Lin, P. Lin, et al., "Guest Editorial Deep Packet Inspection: Algorithms, Hardware, and Applications" // *Proc. IEEE Journal on Selected Areas in Communications*, 2014, pp. 1781-1783.
3. ITU-T Recommendation Y.2770 "Requirements for advanced packet inspection in next-generation networks" edition 1.0, 11/20/2012.
4. ITU-T Recommendation Y.2771 "Deep Packet Inspection Framework", 07/01/2014.
5. ITU-T Recommendation Y.2772 "Network element mechanisms", 04/29/2016.
6. ITU-T Recommendation Y.2773 "Deep Packet Inspection Performance Models and Metrics", 02/17/2017.
7. P. Filimonov, M. Ivanov, "Modern approaches to traffic classification of physical Internet channels" // *Proceedings of the 18th International Conference (DCCN-2015)*, October 19-22, 2015, pp. 466-474.
8. A. Yichiet, M. Selvakumar, K. Shankar, "A temporal-aware signature extraction method using sliding-window mechanism for scalable, cost-effective and accurate traffic classification" // *Proc. IEEE ICC-SCE*, 2017, pp. 156-161.
9. P. Bosshart, D. Daly, G. Gibb, et al., "Programming protocol-independent packet processors," *SIGCOMM Computer Communications Review*, 2013.
10. A. Bremler-Barr, Y. Harchol, D. Hay, Y. Koral, "Deep packet inspection as a service," *CoNEXT*, 2014, pp. 271-282.
11. C. Gerald, R. Gilbert, B. Thomas, "Wireshark Go Deep". 2006. Available online: <https://www.wireshark.org/> (accessed on 01 Jun 2022). дата обращения 01.06.2022.
12. P. Srisuresh, M. Holdrege, "IP Network Address Translator (NAT) Terminology and Considerations. RFC 2663," IETF. 1999. Available online: <https://www.hjp.at/doc/rfc/rfc2663.html> (accessed on 1 Jun 2022), дата обращения 01.06.2022.
13. Software NAT. <http://www.nat32.com/v2/>, accessed 01.06.2022.
14. DDoS. <http://ddos-protection.ru/chto-takoe-ddos>, accessed 01.06.2022.
15. IANA Service Name and Transport Protocol | Port Number Registry. <http://www.iana.org/assignments/service-names-port-numbers/service-names-port-numbers.xhtml>, accessed 01.06.2022.
16. Y. Afek, A. Bremler-Barr, Y. Harchol, D. Hay, Y. Koral, "MCA2: multi-core architecture for mitigating complexity attacks," // *ANCS*, pp. 5-6, 2012.
17. X.-H. Nguyen, X.-D. Nguyen, H.-H. Huynh, K.-H. Le, "Realguard: A Lightweight Network Intrusion Detection System for IoT Gateways," *Sensors* 2022, no. 22, 432. <https://doi.org/10.3390/s22020432>.
18. G.E.M. Abro, S.A.B.M. Zulkifli, R.J. Masood, V.S.Asirvadam, A. Laouti, "Comprehensive Review of UAV Detection, Security, and Communication Advancements to Prevent Threats," *Drones*. 2022, no. 6, p. 284.
19. A. Oruc, A. Amro, V. Gkioulos, "Assessing Cyber Risks of an INS Using the MITRE ATT&CK Framework," *Sensors*. 2022, no. 22, p. 8745.
20. Router Scan v2.60 Beta by Stas'M. Available online: <http://stascorp.com/load/1-1-0-56> (accessed 01.06.2022).
21. <https://drweb.datasystem.ru/catalog/view/645/>, accessed 01.06.2022.
22. BeyondTrust. Retina Network Security Scanner. Available online: <https://www.beyondtrust.com/products/retina-network-security-scanner/>, accessed 01.06.2022.
23. Collection of articles based on the materials of the XXX student international scientific and practical conference. Novosibirsk 2015. No. 3 (29). URL: [http://www.sibac.info/archive/Technic/3\(29\).pdf](http://www.sibac.info/archive/Technic/3(29).pdf)
24. M. Albalawi, R. Aloufi, N. Alamrani, N. Albalawi, A. Aljaedi, A.R. Alharbi, "Website Defacement Detection and Monitoring Methods: A Review," *Electronics*, 2022, no. 11, p. 3573.

For citation: Kazaryan M.M., Cherkesova L.V., Reshetnikova I.V., Revyakina E.A. Analysis of attacks possibilities on the operating system control transfer function using active intelligence methods. *H&ES Reserch*. 2024. Vol. 16. No. 3. P. 18-29. doi: 10.36724/2409-5419-2024-16-3-18-29 (In Rus)

ПРИМЕНЕНИЕ ВЕЙВЛЕТ-АНАЛИЗА ДЛЯ ОБРАБОТКИ СИГНАЛОВ СИСТЕМ ПЕРЕДАЧИ ИНФОРМАЦИИ

МАНОНИНА

Ирина Владимировна¹

ШЕСТАКОВ

Владимир Владимирович²

АННОТАЦИЯ

Введение: В настоящее время применение вейвлет-анализа позволяет решать различные задачи по формированию и обработке информации, выполнять измерительные задачи, производить сжатие и восстановление сигналов с малыми искажениями. **Цель исследования:** заключается в изучении и анализе возможностей применения вейвлет-преобразования для обработки и анализа сигналов в системах передачи информации. **Методы:** с помощью вейвлет обработки возможно осуществлять эффективное распознавание образов с лучшими показателями, чем при многомер-ном статистическом анализе; для цифровых систем обработки информации позволяет разрабатывать современные методы и алгоритмы обработки сигналов, полученных от различных радаров и гидроакустических датчиков, позволяя улучшить разрешение и точность определения объектов; для инфокоммуникационных систем широко применяется при обработке данных, передаваемых по сети, для улучшения качества передачи данных и снижения потребляемой пропускной способности сети, особенно где требуется эффективная обработка сигналов и данных в реальном времени; выполняя базовые алгоритмы спектрального анализа, фильтрации и синтеза сигналов, что позволяет более экономично использовать технические ресурсы; получить более эффективные методы обработки, сжатия и восстановления передаваемых по цифровым каналам связи сигналов с малыми искажениями. **Результаты:** в результате были рассмотрены методы пороговой вейвлет-обработки сигнала с использованием различных функций порога. Произведено определение оптимального уровня вейвлет-разложения с последующим оцениванием качества обработки. А также проведен последующий сравнительный анализ для выбранного сигнала связи путем определения оценки риска относительно теоретического риска, оценки среднеквадратичного отклонения и оценки выходного отношения сигнал/шум.

Сведения об авторах:

¹ к.т.н., доцент, Московский технический университет связи и информатики, Москва, Россия, ivm@mtuci.ru

² к.т.н., доцент, Московский технический университет связи и информатики, Москва, Россия, shvvov@mtuci.ru

КЛЮЧЕВЫЕ СЛОВА: вейвлет-анализ, метод пороговой обработки, оценка риска, шумовая составляющая, пороговые функции

Для цитирования: Манонина И.В., Шестаков В.В. Применение вейвлет-анализа для обработки сигналов систем передачи информации // Научные исследования в космических исследованиях Земли. 2024. Т. 16. № 3. С. 30-38. doi: 10.36724/2409-5419-2024-16-3-30-38



Введение

Вейвлет-анализ является одним из мощных и гибких аппаратов для исследований, а также его преимуществом является функциональное многообразие при обработке сигналов. Одной из возможных задач является задача сжатия видеoinформации и последующая передача по телекоммуникационным каналам связи. Обычно в видеокодеках используются блочные дискретные косинусное преобразования. Но использование для данной задачи дискретного вейвлет-преобразования позволяет избежать эффекта «блочности» (когда наблюдаются резкие переходы на границах блоков преобразования при высоких степенях сжатия), возникающего при использовании дискретного косинусного преобразования, тем самым теоретически предоставляя возможность добиваться лучшего качества восстановленных изображений [1].

Кроме того, вейвлет-анализ позволяет анализировать сигнал на разных масштабах и уровнях детализации, и при последующей пороговой обработке это позволяет обнулить или уменьшить до определённого уровня коэффициенты, которые считаются шумом.

Основными преимуществами такого метода обработки радиотехнических сигналов является их универсальность, эффективное выделение слабых сигналов на фоне шума, для отдельных сигналов слабая зависимость параметров вейвлет-фильтров от спектральных характеристик самого сигнала, кроме того, вейвлет-фильтрация позволяет достичь лучшего соотношения сигнал-шум. Благодаря этим преимуществам, метод вейвлет-фильтрации широко применяется в различных областях радиотехники, включая радиосвязь, радиолокацию, радионавигацию и др.

Особенности дискретного вейвлет-преобразования сигнала

В пространстве Гильберта дискретное вейвлет-преобразование (ДВП) сигнала s представляет собой разложение сигнала по базису, состоящего из сдвигов и растяжений вейвлет-функции ψ_{jk} . Математически ДВП записывается следующим образом:

$$s = \sum_{j \in \mathbb{Z}} \sum_{k \in \mathbb{Z}} \langle s, \psi_{jk} \rangle \psi_{jk} \quad (1)$$

где $\psi_{jk}(t) = 2^{j/2} \psi(2^j t - k)$ – вейвлет-функция; j, k – параметры (индексы) масштаба и сдвига соответственно; $\langle s, \psi_{jk} \rangle$ – скалярное произведение функций; $\{\psi_{jk}\}_{j,k \in \mathbb{Z}}$ – ортонормированный базис в пространстве Гильберта.

Для больших индексов j элементы разложения описывают высокочастотные составляющие сигнала, т.к. порождаются сдвигами функции $\psi(2^j t)$, колеблющимися с большой частотой. При этом чем больше значение j , тем уже носитель $\psi(2^j t)$, и для выделения высокочастотных составляющих окно сужается.

Наличие масштабирования вейвлет-функции, что сравнимо с изменением частот гармоник в разложении сигнала с помощью преобразования Фурье, а также сдвига вейвлет-функции в пространстве позволяет с большей точностью представить локальные особенности сигналов, проявляющиеся в виде сингулярностей, например, различных скачков или разрывов, в отличие от разложения сигнала с помощью гармонических функций.

В системах передачи информации на приёме поступивший сигнал рассматривают, как состоящий из полезной (информационной) и шумовой составляющих. При этом, в подавляющем большинстве случаев, шумовую составляющую по характеру воздействия рассматривают как аддитивную флуктуационную помеху, представляющую собой случайный процесс с нормальным распределением и постоянной спектральной плотностью мощности на всех частотах. Т.е. данный тип помехи имеет практически неограниченный спектр частот, и такую помеху называют «белым» гауссовским шумом.

Будем рассматривать на входе приёмного устройства дискретный сигнал, заданный в виде отсчётов, который можно описать следующей моделью:

$$S_i = x_i + \xi_i, i = 1, \dots, N \quad (2)$$

где x_i – последовательность значений исходного сигнала; ξ_i – последовательность значений «белого» гауссовского шума $(0, \sigma_\xi^2)$, $N=2^J$ – число отсчётов функции сигнала, J – количество уровней разложения.

Производя ДВП (1) принятого сигнала (2), получим следующий набор дискретных вейвлет-коэффициентов:

$$Y_{jk} = \mu_{jk} + \xi_{jk}, j = 0, \dots, J-1, k = 0, \dots, 2^j - 1 \quad (3)$$

где μ_{jk} – вейвлет-коэффициенты вектора значений функции s ; ξ_{jk} – случайные независимые нормально распределённые величины с нулевым средним и дисперсией σ_ξ^2 .

Одной из задач вейвлет-обработки сигнала является подавление шумовой составляющей, которая в большинстве случаев определяется детализирующими коэффициентами. То есть для удаления шумовой составляющей обработке подвергаются только детализирующие коэффициенты. При этом используемые методы подавления шумовой составляющей, как правило, основываются на разработке алгоритма, приводящего к минимизации некоторой функции потерь, которая количественно определяет расстояние между истинным сигналом и его оценкой. Наиболее распространённой функцией потерь, используемой для решения такой задачи, является среднеквадратичная погрешность (или среднеквадратичный риск).

Метод пороговой обработки

Для подавления шумовой составляющей применяется метод, основанный на пороговой обработке полученных в результате ДВП вейвлет-коэффициентов [2, 3]. Такой метод можно сравнить с методом однократного отсчёта с пороговым сравнением, который в системах передачи информации

реализуется посредством регенерации зашумленного сигнала импульсно-кодовой модуляции.

В состав такого регенератора входят отсчетное и решающее устройства, и в тактовые моменты времени на выходе отсчетного устройства (идеального дискретизатора) формируются отсчеты $y_k = \int_0^T y(t) \delta(t - t_k) dt$, подаваемые на вход решающего устройства. В решающем устройстве происходит сравнение полученного отсчета с пороговым напряжением (порогом) U_0 . И на выходе решающего устройства, согласно методу порогового сравнения, выносятся два решения: 1) наличие сигнала, если $y_k \geq U_0$; 2) отсутствие сигнала, если $y_k \leq U_0$.

Аналогичным образом при пороговой обработке коэффициенты, оказавшиеся ниже определенного порогового значения, считаются шумовой составляющей и обнуляются. В качестве функции пороговой обработки, с помощью которой производится обнуление достаточно маленьких коэффициентов, могут применяться различные функции, например, функция жесткой и мягкой пороговой обработки, пороговая функция с двумя пороговыми значениями и их модификации [4-7]. Рассмотрим особенности указанных функций:

- функция жесткой пороговой обработки:

$$p_h(y, Thr) = \begin{cases} y & |y| > Thr \\ 0 & |y| \leq Thr \end{cases} \quad (4)$$

Такая пороговая функция из-за своей разрывности приводит к отсутствию устойчивости, оценкам, имеющим большую дисперсию, а также смещенной оценке риска.

- функция мягкой пороговой обработки:

$$p_s(y, Thr) = \begin{cases} y - Thr & y > Thr \\ y + Thr & y < -Thr \\ 0 & |y| \leq Thr \end{cases} \quad (5)$$

В процессе обработки с функцией мягкого порога участвуют все коэффициенты, что приводит к появлению дополнительного смещения в оценке функции сигнала.

- пороговая функция с двумя пороговыми значениями:

$$p_f(y, Thr_0, Thr_1) = \begin{cases} y & |y| \geq Thr_1 \\ \operatorname{sgn}(y) \frac{Thr_1(|y| - Thr_0)}{Thr_1 - Thr_0} & Thr_0 < |y| < Thr_1, \operatorname{sgn}(y) = \begin{cases} 1 & y > 0 \\ 0 & y = 0 \\ -1 & y < 0 \end{cases} \\ 0 & |y| \leq Thr_0 \end{cases} \quad (6)$$

Недостатки функций (4) и (5) убираются с помощью функции с двумя порогами. Когда значения $|y| \leq Thr_0$, то функция (6) ведет себя как функция (5), а когда значения $|y| \geq Thr_1$ – функция (6) принимает значения функции y [8, 9].

Помимо указанных выше функций существует и блочная пороговая обработка коэффициентов [10]. Такой вид обработки предпочтителен, когда у обрабатываемого сигнала имеется сильная статистическая связь.

Принцип блочной пороговой обработки заключается в следующем. На каждом j -ом уровне преобразования разбиваем вейвлет-коэффициенты на не пересекающиеся блоки длины L , при этом, для удобства, предполагается, что 2^j делится на L . Набор индексов коэффициентов в блоке с номером m на j -ом уровне обозначим (jm) , т.е. получим $(jm) = \{(j, k): (m-1)L + 1 \leq k \leq mL\}$. Пусть также энергия зашумленного сигнала в блоке (jm) равна $S_{jm}^2 = \sum_m Y_{jk}^2$. Тогда оценку вейвлет-коэффициентов вектора значений функции s можно выполнить по следующему правилу:

$$\hat{\mu}_{jk} = \left[1 - \frac{ThrL\sigma_\varepsilon^2}{S_{jm}^2} \right]_+ \cdot Y_{jk}, \quad j=0, \dots, J-1, jk \in (jm), [w]_+ = \begin{cases} w, & w \geq 0 \\ 0, & w < 0 \end{cases} \quad (7)$$

Данный вид обработки применяется к группам соседних коэффициентов, т.е. обнуление коэффициентов принимается сразу для всей группы коэффициентов. Как видно из формулы (7) на величину оценки влияют L и Thr . При получении значения энергии зашумленного сигнала меньше порогового $ThrL\sigma_\varepsilon^2$ все коэффициенты в рассматриваемой группе обнуляются.

Полученная оценка будет обладать оптимальным (в минимаксном смысле) порядком среднеквадратичной погрешности для различных классов функций, что делает блочную пороговую обработку более предпочтительной для использования в практических задачах [10-12].

Таким образом, для вышеперечисленных функций обработки происходит сравнение абсолютной величины каждого обрабатываемого коэффициента, либо абсолютной величины группы обрабатываемых коэффициентов с некоторым порогом. Но в случае групповой обработки коэффициентов, в отличие от функций (5) и (6), также используется информация о соседних коэффициентах.

Выбор значения порога

Выбор оптимального порогового значения является одной из важных задач при шумоподавлении. И если порог выбран слишком маленьким, то в сигнале останется значительный шум, а если пороговое значение слишком велико, то некоторые важные характеристики сигнала могут быть удалены вместе с шумом. Значение порога Thr для функций пороговой обработки зачастую вычисляется экспериментально для каждой конкретной задачи отдельно. Вычисления основываются на значениях параметров полученных вейвлет-коэффициентов, и, как правило, решение выносится на основе на минимизации оценки среднеквадратичной погрешности, полученной по методу Стейна [13].

При этом, пороговое значение может быть вычислено независимо для всех уровней разложений, а также отдельно для каждого набора коэффициентов.

Универсальный порог.

Одно из наиболее часто используемых значений порога вычисляется следующим образом:

$$Thr = \sigma_{\xi} \sqrt{2 \log N} \quad (8)$$

где N – количество коэффициентов в разложении.

С учетом того, что в канале связи предполагается действие «белого» гауссовского шума, то при выборе порога (8) с большой вероятностью шумовые составляющие будут удалены, а вероятность обнаружить шум в восстановленном сигнале экспоненциально убывает.

Обычно для расчета среднеквадратичного значения шума σ_{ξ} используется следующая величина медианного абсолютного отклонения:

$$\hat{\sigma}_{\xi} = \frac{\text{median} \left\{ Y \left[\frac{N}{2} + 1 \right], \dots, Y[N] \right\}}{0.6745} \quad (9)$$

То есть оценка получается на основе отношения выборочной медианы, рассчитываемой на основе детализирующих коэффициентов, получаемых на последнем уровне разложения, к постоянной стандартного нормального распределения.

Минимаксный порог.

Формула вычисления минимаксного порога следующая:

$$Thr = \hat{\sigma}_{\xi} (0.3936 + 0.1829 \log_2 N) \quad (10)$$

Минимаксный порог также учитывает среднеквадратичное отклонение шума σ_{ξ} , определяемое как и для универсального порога с помощью медианного абсолютного отклонения по формуле (9).

SURE-порог.

В основе такого порога лежит минимизация несмещенной оценки риска Стейна (*SURE* – *Stein's Unbiased Risk Estimation*), так как истинные значения коэффициентов разложения обычно неизвестны.

SURE-порог \widehat{Thr} является решением задачи минимизации *SURE*(Thr) по $Thr > 0$:

$$\widehat{Thr} = \arg \min_{Thr > 0} SURE(Thr) \quad (11)$$

Вид функции *SURE*(Thr) зависит от выбора пороговой функции. Например, можно воспользоваться следующей оценкой риска для функции мягкой пороговой обработки:

$$SURE(Thr) = \sigma_{\xi}^2 + \frac{1}{N} \sum_{k=0}^{2^j-1} \left[\min(|Y_{jk}|, Thr) \right]^2 - 2 \frac{\sigma_{\xi}^2}{N} \sum_{k=0}^{2^j-1} \text{Cond} \left[|Y_{jk}| \leq Thr \right] \quad (12)$$

$$\text{Cond} \left[|Y_{jk}| \leq Thr \right] = \begin{cases} 1, & |Y_{jk}| \leq Thr \\ 0, & |Y_{jk}| > Thr \end{cases}$$

На практике может использоваться объединение универсального порога и *SURE*-порога, т.к. значение \widehat{Thr} может оказаться слишком маленьким, и шумовая составляющая эффективно удалиться не будет.

Так как пороговой обработке подвергаются все вейвлет-коэффициенты, то в процессе обработки сигнала может теряться полезная информация при достаточно большом уровне разложения J . Но если уровень J окажется небольшим, то в результате обработки в сигнале может остаться шум.

Таким образом, необходимо определить оптимальный уровень разложения J , при котором после обработки вейвлет-коэффициентов с помощью пороговой функции, можно по полученным обработанным коэффициентам восстановить сигнал, и при этом получить минимальную среднеквадратичную ошибку между исходным сигналом и восстановленным.

Оценка восстановленного сигнала после удаления шума

В общем случае, целью пороговой обработки является уменьшение среднеквадратичной погрешности, которая для пороговых функций определяется следующим образом:

$$R = \sum_{j=0}^{J-1} \sum_{k=0}^{2^j-1} M \left(\mu_{jk} - \hat{Y}_{jk} \right)^2 \quad (13)$$

где \hat{Y}_{jk} – это оценка вейвлет-коэффициентов, которая получается с помощью пороговой обработки, задаваемой для порога Thr некоторой функцией $p_{Thr}(x) : \hat{Y}_{jk} = p_{Thr}(Y_{jk})$.

Выбор порогового значения Thr , как правило, ориентирован на минимизацию риска среднеквадратичной погрешности. При этом, в выражении (13) присутствуют величины μ_{jk} , которые являются неизвестными, т.к. на приеме нет «чистых» коэффициентов разложения μ_{jk} , и вычислить значение среднеквадратичной погрешности на практике нельзя. Поэтому пороговое значение Thr вычисляется одним из приведенных выше способом. Либо в качестве несмещенной оценки риска можно использовать следующую величину:

$$\hat{R} = \sum_{j=0}^{J-1} \sum_{k=0}^{2^j-1} F(Y_{jk}, Thr), F(y, Thr) = \begin{cases} y^2 - \sigma_{\xi}^2 & |y| \leq Thr \\ h^2(y, Thr) + \sigma_{\xi}^2 - 2\sigma_{\xi}^2 h'_y(y, Thr) & |y| > Thr \end{cases} \quad (14)$$

$$p_h(y, Thr) = \begin{cases} y - h(y, Thr) & |y| > Thr \\ 0 & |y| \leq Thr \end{cases}$$

Функция $h(y, Thr)$ является обобщающей функцией пороговой обработки со свойствами: непрерывности, нечетности и ограниченности.

Оценить получаемые оценки риска относительно теоретического риска (13) можно следующим образом:

$$\frac{\hat{R} - R}{\sigma_{\hat{R}}^2 \sqrt{2^{J+1}}} \rightarrow N(0, \phi) \quad (15)$$

где $\phi = 1$ – если использовалась оценка дисперсии шума на основе среднеквадратического значения; $\phi = 1,36$ – если использовалась оценка дисперсии шума на основе медианного абсолютного отклонения [14].

При этом формулу для оценки теоретического риска можно преобразовать к более удобному виду [15]:

$$R = \sum_{i=1}^{2^J} (\mu_i)^2 \{F_{\sigma}(Thr - \mu_i) - F_{\sigma}(-Thr - \mu_i)\} - \\ - \sum_{i=1}^{2^J} \sigma^2 \{ (Thr + \mu_i \varphi_{\sigma}(Thr - \mu_i)) + (Thr - \mu_i \varphi_{\sigma}(Thr + \mu_i)) \} + \\ + \sum_{i=1}^{2^J} (\sigma^2 + Thr^2) \{2 - F_{\sigma}(Thr - \mu_i) - F_{\sigma}(Thr + \mu_i)\}$$

Определение параметров и оценка пороговой обработки частотно-модулированного сигнала

Оценка метода пороговой обработки коэффициентов разложения сигнала получается за счет выполнения следующих действий:

1. Вычисление дискретного вейвлет-преобразования принятого сигнала.
2. Определение значения порога.
3. Применение пороговой функции $p(y, Thr)$ к вейвлет-коэффициентам для получения оценки обработанных вейвлет-коэффициентов.
4. Выполнение обратного вейвлет-преобразования.
5. Оценка эффективности работы пороговой обработки.

В качестве исходного информационного сигнала был взят частотно-модулированный сигнал (рис. 1), часто используемый для передачи информации в системах связи. Для моделирования передачи сигнала по гауссовскому каналу связи к сигналу был добавлен «белый» гауссовский шум, который суммируется с исходным сигналом (рис. 2).

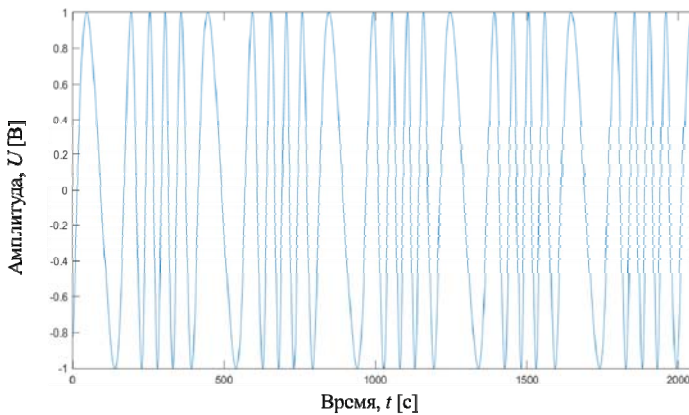


Рис. 1. Исходный частотно-модулированный сигнал

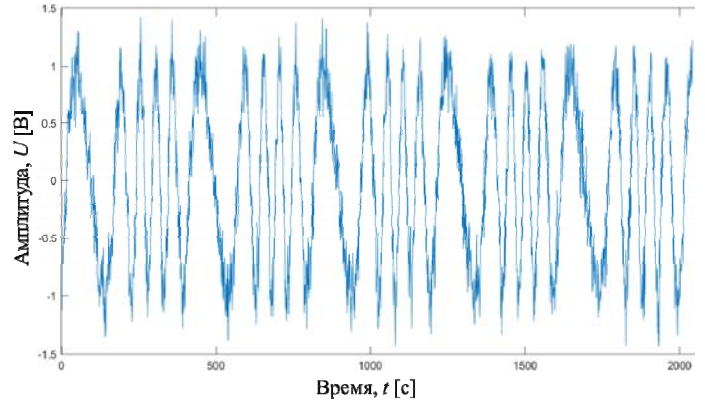


Рис. 2. Исходный частотно-модулированный сигнал + «белый» гауссовский шум

Отношение сигнал/шум у полученного зашумленного сигнала имеет значение $h_{in}^2 = 12$ дБ. Произведем пороговую обработку зашумленного сигнала по вышеописанному алгоритму.

Произведем определение оптимального уровня разложения для исследуемого сигнала, используя при этом несколько параметров, влияющих на результат обработки. К таким параметрам относятся: тип используемых вейвлетов – симлеты, вейвлеты Койфмана, Добеши, Хаара; тип пороговой обработки – мягкая, жесткая. Оценивание качества обработки производится с помощью среднеквадратического отклонения и отношения сигнал/шум после обработки. Результаты вычислений представлены в таблице 1.

Среднеквадратическое отклонение (17) и отношение сигнал/шум (ОСШ) после обработки (18) рассчитываются по формулам:

$$S_{err}(\hat{X}) = \frac{1}{N} \sum_{i=1}^N (\mu_w[i] - \hat{\mu}_w[i])^2 \quad (17)$$

$$h_{out}^2 = 10 \lg \frac{\sum_{i=1}^N (\mu_w[i])^2}{\sum_{i=1}^N (\mu_w[i] - \hat{\mu}_w[i])^2} \quad (18)$$

где N – объем выборки вейвлет-коэффициентов; μ_w – вейвлет-коэффициенты исходного сигнала; $\hat{\mu}_w$ – вейвлет-коэффициенты восстановленного сигнала.

ОСШ является одним из важнейших параметров сигнала. Чем больше ОСШ, тем меньше шум влияет на сигнал. И если после пороговой обработки сигнала ОСШ увеличивается, то увеличивается и точность восстановления исходного сигнала.

Увеличение ОСШ после обработки относительно исходного значения можно оценить следующей разницей:

$$\Delta h^2 = h_{out}^2 - h_{in}^2 \quad (19)$$

С возрастанием ОСШ уменьшается среднеквадратическое отклонение восстановленного сигнала после обработки от исходного сигнала.

Таблица 1

Оптимальные уровни разложения для разных вейвлетов для ЧМ сигнала

Вейвлет	Мягкий порог				Жесткий порог			
	Уровень	$S_{err}(\ddot{x})$	I_{err}^2	Δt^2	Уровень	$S_{err}(\ddot{x})$	I_{err}^2	Δt^2
Хаар	2	0.0123	16,039	4,04	2	0.0216	14,083	2,08
Добешн db2	3	0.0056	18,863	6,86	8	0.0166	16,069	4,07
Добешн db3	3	0.0051	19,949	7,95	7	0.0166	16,253	4,25
Добешн db8	4	0.0046	20,466	8,47	8	0.0132	19,543	7,54
Добешн db11	4	0.0036	21,537	9,54	8	0.0157	18,850	6,85
Добешн db18	4	0.0033	22,112	10,11	8	0.0141	18,939	6,94
Добешн db24	4	0.0036	22,099	10,10	8	0.0157	19,805	7,81
Добешн db31	4	0.0036	22,616	10,62	8	0.0135	22,477	10,48
Симлет sym3	3	0.0043	20,641	8,64	8	0.0177	16,739	4,74
Симлет sym7	4	0.0041	21,237	9,24	8	0.0182	18,917	6,92
Симлет sym8	4	0.0045	20,859	8,86	7	0.0161	18,209	6,21
Симлет sym15	4	0.0043	21,162	9,16	8	0.0148	20,938	8,94
Симлет sym24	4	0.0040	21,439	9,44	8	0.0171	19,895	7,90
Койфлет кой3	4	0.0046	20,746	8,75	8	0.0172	19,525	7,53
Койфлет кой4	3	0.0047	20,367	8,37	7	0.0122	19,569	7,57
Койфлет кой5	4	0.0037	21,665	9,67	7	0.0136	19,055	7,06

При мягкой пороговой обработке для большинства исследуемых вейвлетов оптимальный уровень разложения оказался равным 4. При жесткой пороговой обработке для большинства исследуемых вейвлетов оптимальный уровень разложения равен 8. Для вейвлета Хаара оптимальный уровень разложения оказался равен 2 (при мягкой и при жесткой пороговой обработке).

Анализ приведенных значений показывает, что при фиксированном сигнале и мягком типе пороговой обработки оптимальные уровни разложения для большинства вейвлетов совпадают, а ошибки соизмеримы. При жестком типе пороговой обработки оптимальные уровни разложения также не сильно отличаются, но при этом оптимальный уровень разложения больше, чем для мягкой обработки, а ошибки восстановления – на порядок больше. Кроме того, для мягкого типа пороговой обработки наблюдается большее увеличение ОСШ после обработки относительно исходного значения.

Рассмотрим зависимость среднеквадратичной ошибки от уровня вейвлет разложения (рис. 3), и зависимость ОСШ от уровня разложения (рис. 4), выбрав в качестве базисного вейвлета – вейвлет Добешн.

Графики на рисунке 3 показывают отсутствие монотонной зависимости между уровнем вейвлет-разложения и среднеквадратичной ошибкой. При этом при мягком типе пороговой обработки ошибка начинает сильно расти, когда уровень разложения становится больше оптимального.

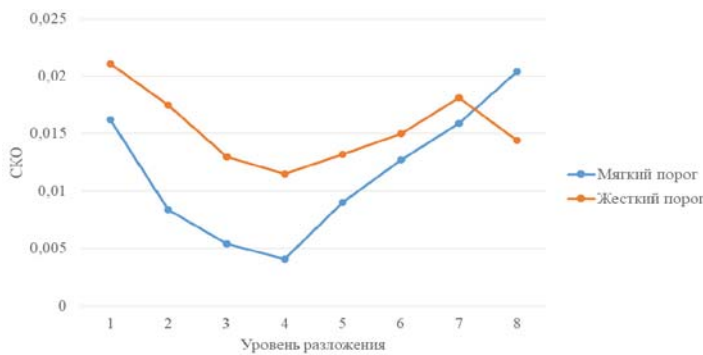


Рис. 3. Зависимость среднеквадратичной ошибки от уровня разложения для ЧМ сигнала

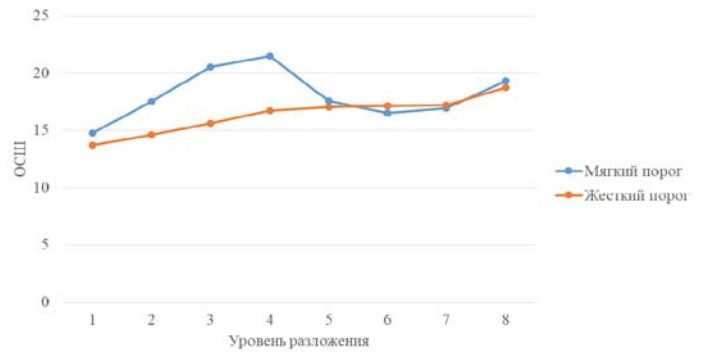


Рис. 4. Зависимость отношения сигнал/шум от уровня разложения для ЧМ сигнала

На рисунке 5 показаны восстановленные после обработки сигналы, полученные с использованием вейвлета Добешн при разных уровнях разложения и мягком типе пороговой обработки.

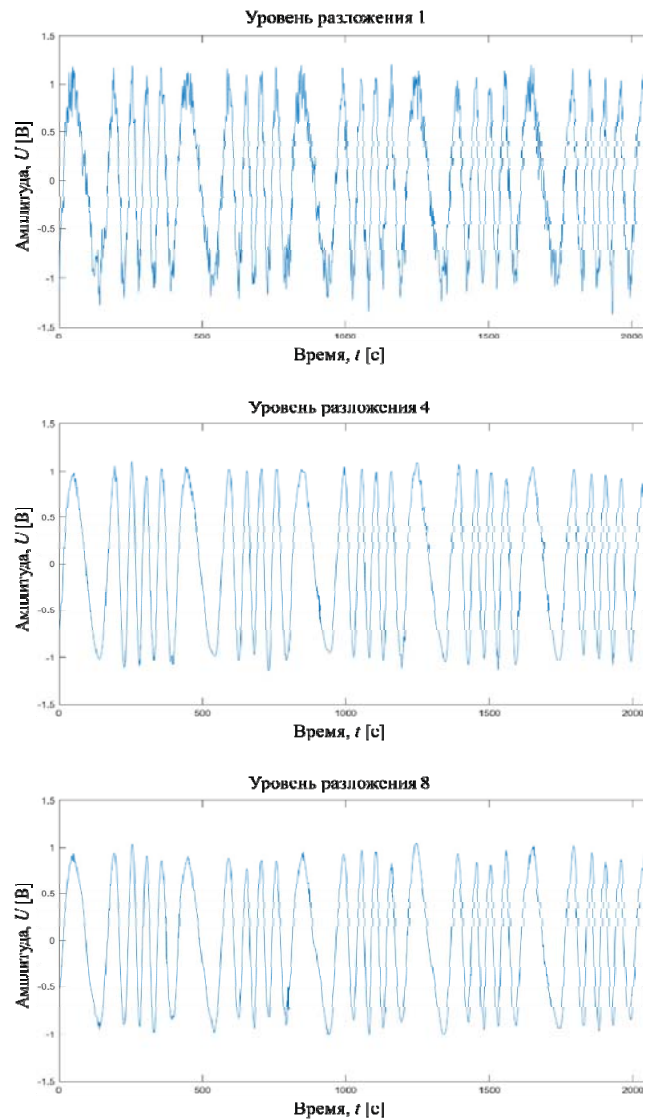


Рис. 5. Восстановленные после обработки сигналы при уровне разложения 1, 4 и 8

Как видно из рисунка 5, если уровень разложения слишком маленький, то в восстановленном сигнале остается шумовая составляющая, а при слишком большом уровне разложения из сигнала удаляется информационная часть.

Дальше проведем ДВП зашумленного сигнала. Уровень разложения, используемый для ДВП определен выше и равен 4. Используемый метод пороговой обработки выбран – мягкий, так как показал более высокие результаты. А значения порога определяются с помощью универсального метода (8), рассчитанного с помощью (9) (y_{MAO}) и на основе среднеквадратичного отклонения (y_{CKO}), минимаксный (10) и *SURE*-порог (11, 12). Для оценки эффективности работы представленного алгоритма производится оценка среднеквадратичного отклонения (17), оценки риска относительно теоретического риска (15), и оценка выходного отношения сигнал/шум (18, 19).

Результаты усредненных вычисления указаны в таблице 2.

Таблица 2

Результаты эксперимента

Вейвлет	Пороговое значение		Оценка СКО	Оценка риска	h_{out}^2	Δh^2
Добеши db11	y_{MAO}	0,4750	0,0039	0,51	21,18	9,49
	y_{CKO}	0,4732	0,0039	0,29	21,18	9,49
	минимаксный	0,4448	0,0039	0,53	21,22	9,53
	<i>SURE</i> -порог	0,6367	0,0043	0,06	20,82	9,13
Добеши db18	y_{MAO}	0,4714	0,0028	0,32	22,87	11,16
	y_{CKO}	0,4675	0,0028	0,12	22,86	11,16
	минимаксный	0,4418	0,0028	0,36	22,83	11,13
	<i>SURE</i> -порог	0,5771	0,0027	0,07	22,92	11,22
Добеши db24	y_{MAO}	0,4563	0,0028	0,99	23,23	11,40
	y_{CKO}	0,4602	0,0028	0,48	23,23	11,41
	минимаксный	0,4281	0,0028	1,07	23,18	11,35
	<i>SURE</i> -порог	0,5540	0,0028	0,25	23,28	11,45
Добеши db31	y_{MAO}	0,4149	0,0042	4,93	21,95	10,01
	y_{CKO}	0,4387	0,0042	1,83	21,98	10,05
	минимаксный	0,3897	0,0043	4,94	21,89	9,95
	<i>SURE</i> -порог	0,5451	0,0041	2,03	22,06	10,12
Симлет sym7	y_{MAO}	0,4581	0,0045	1,29	20,80	8,75
	y_{CKO}	0,4463	0,0045	0,18	20,81	8,77
	минимаксный	0,4286	0,0044	1,21	20,84	8,79
	<i>SURE</i> -порог	0,5050	0,0046	0,12	20,73	8,69
Симлет sym8	y_{MAO}	0,4832	0,0043	0,13	21,08	9,14
	y_{CKO}	0,4636	0,0043	0,82	21,08	9,15
	минимаксный	0,4522	0,0043	0,02	21,09	9,16
	<i>SURE</i> -порог	0,6318	0,0044	0,70	21,00	9,07
Симлет sym15	y_{MAO}	0,4459	0,0045	1,84	20,99	9,10
	y_{CKO}	0,4589	0,0045	0,29	20,96	9,07
	минимаксный	0,4177	0,0044	1,71	21,04	9,15
	<i>SURE</i> -порог	0,5766	0,0049	0,61	20,61	8,73
Симлет sym24	y_{MAO}	0,4500	0,0042	1,37	21,30	9,35
	y_{CKO}	0,4614	0,0042	0,16	21,30	9,35
	минимаксный	0,4222	0,0042	1,24	21,29	9,34
	<i>SURE</i> -порог	0,5720	0,0042	0,28	21,29	9,34
Койфлет coif3	y_{MAO}	0,4666	0,0045	0,16	20,81	9,05
	y_{CKO}	0,4691	0,0045	0,15	20,80	9,04
	минимаксный	0,4367	0,0044	0,01	20,94	9,19
	<i>SURE</i> -порог	0,6284	0,0053	0,90	20,10	8,34
Койфлет coif5	y_{MAO}	0,4578	0,0039	1,00	21,44	9,71
	y_{CKO}	0,4664	0,0040	0,04	21,42	9,68
	минимаксный	0,4289	0,0039	0,93	21,51	9,77
	<i>SURE</i> -порог	0,5939	0,0043	0,34	21,01	9,28

С учетом того, что шум является случайной величиной, то для получения более корректных значений оценки риска 1000 раз был создан зашумленный сигнал, проведена пороговая обработки и произведено восстановление сигнала, а все полученные показатели усреднялись. Результаты вейвлет-обработки жестким методом пороговой обработки не приводятся, так как для исследуемого сигнала данный тип обработки показал значения на порядок хуже, чем при мягкой обработке.

После анализа таблицы 2, а также сравнения графиков восстановленных сигналов были выбраны наилучшие параметры пороговой обработки: тип вейвлета – Добеши db18 и db24; мягкий метод пороговой обработки; универсальный и *SURE*-порог; оптимальный уровень разложения – 4.

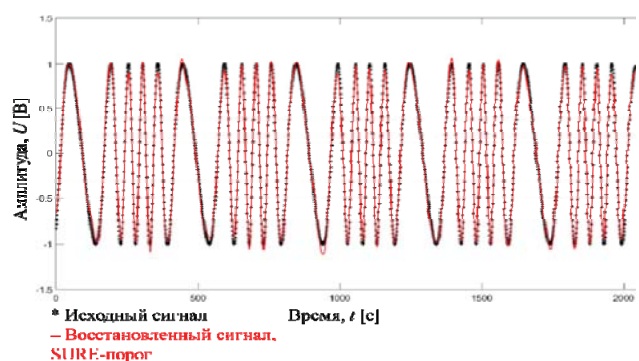
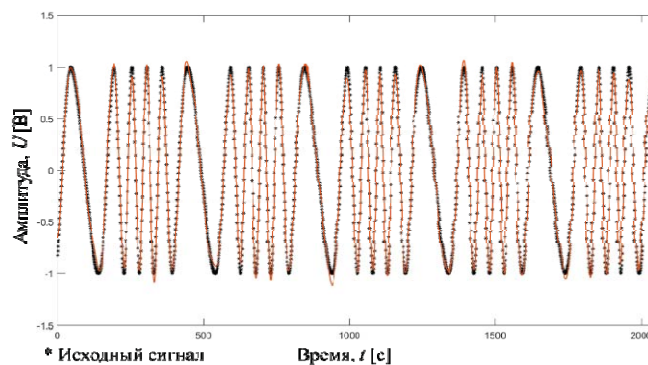
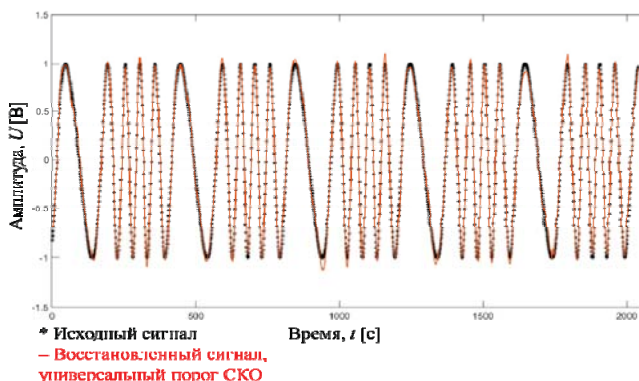


Рис. 6. Исходный и восстановленный сигнал при использовании вейвлета Добеши db18

На рисунках 6 и 7 показаны исходный и восстановленный сигнал после пороговой обработки с выявленными параметрами.



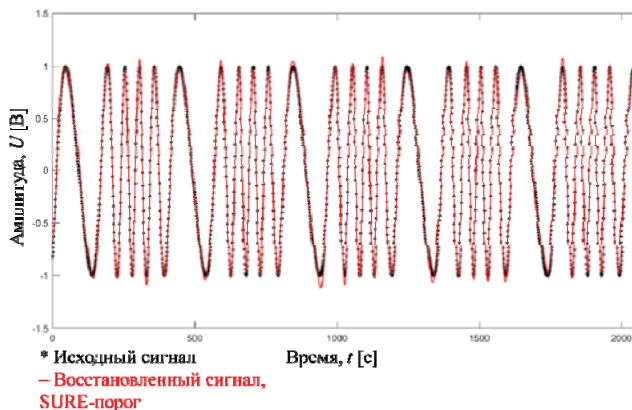


Рис. 7. Исходный и восстановленный сигнал при использовании вейвлета Добеши db24

Как видно из рисунка 6 – оба восстановленных сигнала близки к исходному сигналу, а разница между двумя восстановленными сигналами – минимальна. Аналогичные выводы можно сделать после анализа рисунка 7.

Заключение

При пороговой обработке сигналов с помощью вейвлет-преобразования с целью удаления шумовой составляющей на качество восстановления сигнала влияют многие факторы. А именно: уровень вейвлет-разложения зашумленного сигнала – результаты показали, что между уровнем разложения и ошибкой восстановления отсутствует монотонная зависимость и до определенного уровня значение СКО уменьшается, а затем начинает увеличиваться. И при уровне большем, чем оптимальное значение, жесткая обработка дает значения СКО соизмеримые с наименьшим значением ошибки, а при мягкой обработке наблюдается резкое увеличение СКО. Помимо этого, влияет метод пороговой обработки и для исследуемого сигнала наилучшие результаты были получены при мягкой пороговой обработке. На качество восстановления влияет и способ определения порогового значения. Универсальный способ показал наилучшие результаты, при этом вычисление порога оценивалось для каждого набора коэффициентов.

Помимо метода пороговой обработки большое влияние на качество оказывает выбор базисного вейвлета. И чем вейвлет-функция более гладкая, тем более сглаженным будет восстановленный сигнал. Например, применение методов обработки с использованием вейвлетов Добеши высоких порядков позволяет получать более гладкие функции при восстановлении, что зачастую улучшает эффективность удаления шума.

Несмотря на активное развитие исследований, направленных на пороговую вейвлет-обработку сигналов, многие проблемы остаются неразрешенными. Использование методов мягкой и жесткой пороговой обработки приводят к скачкам в

восстановленном сигнале и оценки получаются смещенными, что может привести к большому СКО от значений исходного сигнала. Решение может быть получено с использованием методов, зависящих от набора параметров, которых получают после оптимизации некоторых функционалов.

Но данные методы обладают существенным преимуществом – они хорошо изучены и для них возможно получить оценки риска, предсказывающие поведение методов для тех или иных сигналов. Поэтому дальнейшее развитие данных методов, а также изучение свойств новых методов позволит улучшить экспериментальные показатели и найти условия, при которых модифицированные методы смогут превзойти классические методы по качеству обработки.

Литература

1. Быстров К.С., Грызлов Г.Ю., Дворкович А.В., Дворкович В.П. Использование видеокодека на основе многоканального вейвлет-разложения в телекоммуникационных системах потокового телевидения // Распределенные компьютерные и телекоммуникационные сети: управление, вычисление, связь (DCCN-2017). М.: Рекламно-издательский центр "ТЕХНОСФЕРА", 2017. С. 68-75.
2. Шестаков О.В. Пороговые функции в методах подавления шума, основанных на вейвлет-разложении сигнала // Информатика и ее применения. 2021. Т. 15, № 3. С. 51-56. DOI 10.14357/19922264210307.
3. Mallat S. A wavelet tour of signal processing. New York, NY: Academic Press. 1999.
4. Donoho D., Johnstone I.M. Ideal spatial adaptation via wavelet shrinkage // Biometrika. No. 81(3), pp. 425-455. 1994.
5. Donoho D., Johnstone I.M. Adapting to unknown smoothness via wavelet shrinkage // J. Am. Stat. Assoc. no. 90, pp. 1200-1224. 1995.
6. Donoho D., Johnstone I.M. Minimax estimation via wavelet shrinkage // Ann. Stat., no. 26(3), pp. 879-921. 1998.
7. Zhao R.-M., Cui H.-M. Improved threshold denoising method based on wavelet transform // 7th Conference (International) on Modelling, Identification and Control Proceedings. Piscataway, NJ: IEEE. Art. ID: 7409352. 2015. 4 p. DOI: 10.1109/ICMIC.2015.7409352.
8. Кудрявцев А.А., Шестаков О.В. Минимаксные оценки функции потерь, основанной на интегральных вероятностях ошибок при пороговой обработке вейвлет-коэффициентов // Информатика и ее применения. 2021. Т. 15, № 4. С. 12-19. DOI 10.14357/19922264210402.
9. Шестаков О.В. Несмещенная оценка риска пороговой обработки с двумя пороговыми значениями // Информатика и ее применения. 2022. Т. 16, № 4. С. 14-19. DOI 10.14357/19922264220403.
10. Cai T. Adaptive wavelet estimation: A block thresholding and oracle inequality approach // Ann. Stat., no. 28(3), pp. 898-924. 1999.
11. Шестаков О.В. Анализ несмещенной оценки среднеквадратичного риска метода блочной пороговой обработки // Информатика и ее применения. 2021. Т. 15, № 2. С. 30-35. DOI 10.14357/19922264210205.
12. Zhao R.-M., Cui H.-M. Improved threshold denoising method based on wavelet transform // 7th Conference (International) on Modelling, Identification and Control Proceedings. Piscataway, NJ, USA: IEEE, 2015. Art. 7409352. 4 p. DOI: 10.1109/ICMIC.2015.7409352.
13. Stein C. Estimation of the mean of a multivariate normal distribution // Ann. Stat., no. 9(6), pp. 1135-1151. 1981.
14. Кудрявцев А.А., Шестаков О.В. Оценка усредненной вероятности ошибки при вычислении вейвлет-коэффициентов в методе гибридной пороговой обработки // Вестник Московского университета. Серия 15: Вычислительная математика и кибернетика. 2021. № 1. С. 19-24.
15. Манонина И.В. Использование вейвлет-анализа для оценки качества рефлектограмм // Т-Comm: Телекоммуникации и транспорт 2014. № 9. С. 54-59.

DECISION SUPPORT CONCEPT FOR LIFECYCLE SUPPORT PROBLEMS OF COMPLEX TECHNICAL SYSTEMS

IRINA V. MANONINA,
Moscow, Russia, ivm@mtuci.ru

VLADIMIR V. SHESTAKOV,
Moscow, Russia, shvvov@mtuci.ru

KEYWORDS: *wavelet analysis, threshold processing method, risk assessment, noise component; threshold functions.*

ABSTRACT

Introduction: Currently, the use of wavelet analysis makes it possible to solve various problems in the formation and processing of information, perform measurement tasks, and perform compression and restoration of signals with low distortion. **Purpose:** is to study and analyze the possibilities of using the wavelet transform for processing and analyzing signals in information transmission systems. **Methods:** with the help of wavelet processing it is possible to carry out effective pattern recognition with better performance than with multivariate statistical analysis; for digital information processing systems allows you to develop modern methods and algorithms for processing signals received from various radars and hydroacoustic sensors, allowing you to improve the resolution and accuracy of object identification; for infocommunication systems, it is widely used in processing data transmitted over the net-

work to improve the quality of data transmission and reduce the consumed network bandwidth, especially where effective processing of signals and data in real time is required; performing basic algorithms for spectral analysis, filtering and signal synthesis, which allows for more economical use of technical resources; obtain more efficient methods of processing, compression and restoration of signals transmitted over digital communication channels with low distortion. **Results:** as a result, methods of threshold wavelet signal processing using various threshold functions were considered. The optimal level of wavelet decomposition was determined with subsequent assessment of the quality of processing. A subsequent comparative analysis was also carried out for the selected communication signal by determining the risk assessment relative to the theoretical risk, estimating the standard deviation and estimating the output signal-to-noise ratio.

REFERENCES

1. K.S. Bystrov, G.Ju. Gryzov, A.V. Dvorkovich, V.P. Dvorkovich, "Using a video codec based on multichannel wavelet decomposition in telecommunication systems for live TV broadcasting," *Distributed computer and telecommunication networks: control, computing, communication (DCCN-2017)*. Moscow: Advertising and publishing center "TECHNOSPHERE", 2017, pp. 68-75. (In Rus)
2. O.V. Shestakov, "Threshold functions in noise reduction methods based on wavelet decomposition of the signal," *Informatika i ee primeneniya*. 2021. vol. 15, no. 3, pp. 51-56. (In Rus)
3. S. Mallat, "A wavelet tour of signal processing," New York, NY: Academic Press. 1999.
4. D. Donoho, I.M. Johnstone, "Ideal spatial adaptation via wavelet shrinkage," *Biometrika*, no. 81(3), pp. 425-455. 1994.
5. D. Donoho, I.M. Johnstone, "Adapting to unknown smoothness via wavelet shrinkage," *J. Am. Stat. Assoc.*, no. 90, pp. 1200-1224. 1995.
6. D. Donoho, I.M. Johnstone, "Minimax estimation via wavelet shrinkage," *Ann. Stat.*, no. 26(3), pp. 879-921. 1998.
7. R.-M. Zhao, H.-M. Cui, "Improved threshold denoising method based on wavelet transform," *7th Conference (International) on Modeling, Identification and Control Proceedings*. Piscataway, NJ: IEEE. Art. ID: 7409352. 2015. 4 p.
8. A.A. Kudrjavcev, O.V. Shestakov, "Minimax estimates of the loss function based on the integral probabilities of errors during thresholding of wavelet coefficients," *Informatika i ee primeneniya*. 2021. Vol. 15, no. 4, pp. 12-19. (In Rus)
9. O.V. Shestakov, "Unbiased risk assessment of thresholding with two threshold values," *Informatika i ee primeneniya*. 2022. Vol. 16, № 4. Pp. 14-19. (In Rus)
10. T. Cai, "Adaptive wavelet estimation: A block thresholding and oracle inequality approach." *Ann. Stat.*, no. 28(3), pp. 898-924. 1999.
11. O.V. Shestakov, "Analysis of the unbiased estimate of the root mean square risk of the block thresholding method," *Informatika i ee primeneniya*. 2021. Vol. 15, no. 2, pp. 30-35. (In Rus)
12. R.-M. Zhao, H.-M. Cui, "Improved threshold denoising method based on wavelet transform," *7th Conference (International) on Modeling, Identification and Control Proceedings*. Piscataway, NJ, USA: IEEE, 2015. Art. 7409352. 4 p.
13. C. Stein, "Estimation of the mean of a multivariate normal distribution," *Ann. Stat.*, no. 9(6), pp. 1135-1151. 1981.
14. A.A. Kudrjavcev, O.V. Shestakov, "Estimation of the average error probability when calculating wavelet coefficients in the hybrid thresholding method," *Bulletin of Moscow University. Episode 15: Computational Mathematics and Cybernetics*. 2021, no. 1, pp. 19-24. (In Rus)
15. I.V. Manonina, "Using wavelet analysis to assess the quality of reflectograms," *T-Comm*. 2014, no. 9, pp. 54-59. (In Rus)

INFORMATION ABOUT AUTHORS:

Irina V. Manonina, PhD, Associate Professor, MTUCI, Moscow, Russia

Vladimir V. Shestakov, PhD, Associate Professor, MTUCI, Moscow, Russia

For citation: Manonina I.V., Shestakov V.V. Application of wavelet analysis for signal processing of information transmission systems. *H&ES Reserch*. 2024. Vol. 16. No 3. P. 30-38. doi: 10.36724/2409-5419-2024-16-3-30-38 (In Rus)



doi: 10.36724/2409-5419-2024-16-3-39-45

РЕАЛИЗАЦИЯ СЕТЕВЫХ ФУНКЦИЙ В IP-ФАБРИКЕ ЦЕНТРА ОБРАБОТКИ ДАННЫХ

БУЖИН
Игорь Геннадьевич¹

АНТОНОВА
Вероника Михайловна²

ГНЕЗДИЛОВ
Владислав Станиславович³

МИРОНОВ
Юрий Борисович⁴

Сведения об авторах:

¹ к.т.н., доцент кафедры "Сети и системы фиксированной связи", Московский Технический Университет Связи и Информатики, Москва, Россия, i.g.buzhin@mtuci.ru

² к.т.н., доцент, зав. кафедры "Сети и системы фиксированной связи", Московский Технический Университет Связи и Информатики, Москва, Россия, v.m.antonova@mtuci.ru

³ ассистент кафедры "Сети и системы фиксированной связи", Московский Технический Университет Связи и Информатики, Москва, Россия, v.s.gnezdilov@mtuci.ru

⁴ к.т.н., декан факультета "Сети и системы связи", Московский Технический Университет Связи и Информатики, Москва, Россия, i.b.mironov@mtuci.ru

АННОТАЦИЯ

Введение: в современных дата-центрах часто применяют IP-фабрики, которые являются системой объединенных сетевых устройств с высокой степенью взаимосвязи, благодаря чему минимизируется расстояние между конечными узлами, сокращаются задержки, и устройства функционируют более эффективно. При этом многие процедуры переносятся в наложенную (оверлейную) сеть с помощью технологии виртуализации сетевых функций. В связи с этим возникает проблема эффективной реализации сетевых функций в IP-фабрике центра обработки данных. **Цель исследования:** нахождение эффективного способа реализации виртуализации сетевых функций в IP-фабрике центра обработки данных. **Обоснованность** данного подхода доказана экспериментально. Данный подход работает для обработки различного типа трафика. **Результаты:** Предложен подход к реализации сетевых функций в IP-фабрике центра обработки данных. Выбран способ обработки трафика на сервере общего пользования на основе технологии VPP и FRR. Показаны результаты тестовых измерений обработки различного трафика на уровне передачи данных (data plane). Результаты экспериментальных тестов показывают, что на 1 ядре Xeon Cascade Lake технология VPP выдает производительность порядка 20 Mpps при IPv4 трафике. Комбинации обработки IPv4-lookup, VxLAN, Encap/Decap, ACL-lookup показывают более низкую производительность. Предложен способ доставки трафика до сетевых функций IP-фабрики на основе технологий VxLAN, EVPN и ECMP.

КЛЮЧЕВЫЕ СЛОВА: IP-фабрика, FRR, Виртуализация Сетевых Функций (ВСФ), VPP, VxLAN.

Для цитирования: Бужин И.Г., Антонова В.М., Гнездилов В.С., Миронов Ю.Б. Реализация сетевых функций в IP-фабрике центра обработки данных // Научные исследования в космических исследованиях Земли. 2024. Т. 16. № 3. С. 39-45. doi: 10.36724/2409-5419-2024-16-3-39-45

Введение

В современных центрах обработки данных используются IP-фабрики – это объединенная система сетевых устройств с высокой степенью взаимосвязи в центре обработки данных, развернутая на двух или трех уровнях. Благодаря этому значительно упрощается сетевая архитектура: минимизируется расстояние между конечными узлами, сокращаются задержки, и устройства функционируют более эффективно. Многие процедуры, необходимые для организации сетевого взаимодействия, переносятся в оверлейную сеть: сегментация, виртуализация и прочие взаимосвязанные сервисы сдвигаются в наложенную (оверлейную) сеть, функционирующую поверх IP-фабрики. При этом осуществляется поддержка стандартных протоколов динамической маршрутизации.

IP-фабрика – это сетевая архитектура, обеспечивающая высокий уровень связности, резервирования, гарантированную полосу взаимодействия, QoS для сетей с одноранговым обменом. IP-фабрика предоставляет транспортный сервис для различных наложенных (оверлейных) IP-сетей. Эта топология опирается на структуру дерева (fat-tree) и стебля с листьями (spine-leaf) – последняя также известна как «сеть Клоза» и представляет собой многокаскадную коммутационную сеть. Во многих современных центрах обработки данных архитектура сети Клоза реализуется в виде схемы "leaf-spine", где уровень "spine" представляет коммутаторы на магистральном уровне, а уровень "leaf" – пограничные коммутаторы на входе и выходе. Такую схему также иногда называют топологией утолщенного дерева (fat-tree).

Цель данной топологии в уменьшении общего количества требуемых коммутаторов и портов. Архитектура IP-фабрики (рис. 1) подразумевает наличие большого количества высокоскоростных прямых каналов связи, которые позволяют избежать замедления скорости в сети, вызванного появлением «бутылочных горлышек», и поддерживать высокую эффективность перенаправления трафика и низкую задержку. Использование такой архитектуры в дата-центре дает ряд преимуществ по сравнению с классической двухуровневой архитектурой со «свернутым» ядром сети (collapsed core):

- увеличивается отказоустойчивость. В сети collapsed core независимых ядер может быть только два – это ограничение технологий агрегации MLAG (Multi-Chassis Link Aggregation), которые позволяют объединять интерфейсы в группы максимум между двумя коммутаторами. Коммутаторов же Spine может быть гораздо больше.
- облегчается увеличение пропускной способности – для этого нужно просто добавить необходимое число коммутаторов Spine.
- сбои затрагивают меньше устройств – коммутаторы полностью независимы, отказоустойчивость достигается без использования стекирования или MLAG.
- задержка становится предсказуемой – на пути любого потока внутреннего трафика находится только один коммутатор Spine.
- повышается уровень утилизации сетевых интерфейсов – трафик между Leaf и Spine прозрачно и эффективно распределяется с помощью механизмов ECMP (Equal Cost Multipath).

Однако, при реализации архитектуры IP-фабрики используется сетевое оборудование центров обработки данных, которое не позволяет, в случае необходимости, организовать сервисы по дополнительной обработке трафика – применение функций NAT (трансляции адресов), особая фильтрация трафика L3/L4, применение систем обнаружения и предотвращения вторжений (IPS/IDS), асимметричная отдача трафика с сервиса (Direct Server Return). При этом при такой реализации IP-фабрики нет возможности модифицировать сетевой стек.

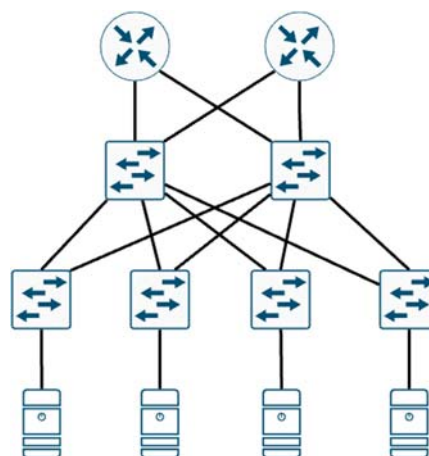


Рис. 1. Архитектура IP-фабрики

Таким образом, при организации дополнительных сервисов по обработке трафика на IP-фабрике необходимо решить несколько задач: выбрать способ обработки трафика, как организовать доставку трафика до места обработки, как выполнить требования по архитектуре сети (отсутствие возможности модификации сетевого стека) и как обеспечить масштабирование и резервирование.

Способы обработки трафика на сервере общего пользования

Для реализации обработки сетевого трафика на серверах общего пользования применяется подход виртуализации сетевых функций (NFV).

В соответствии с эталонной архитектурой NFV [8], систему, состоящую из программно-аппаратных средств для реализации NFV, можно представить из следующих элементов (рис. 2):

- виртуальные сетевые функции (VNF(s));
- виртуальная сетевая инфраструктура (NFVI);
- ПО управления и оркестрации NFV.

Примерами такого функционала могут быть протоколы маршрутизации, трансляция сетевых адресов, реализация списков доступа и межсетевого экранирования, реализация механизмов QoS и т.д. Инфраструктура NFV представляет собой абстракцию аппаратных средств сетей связи, фактически является набором программных средств для реализации виртуализации аппаратных ресурсов, включая память и вычислительные ресурсы.

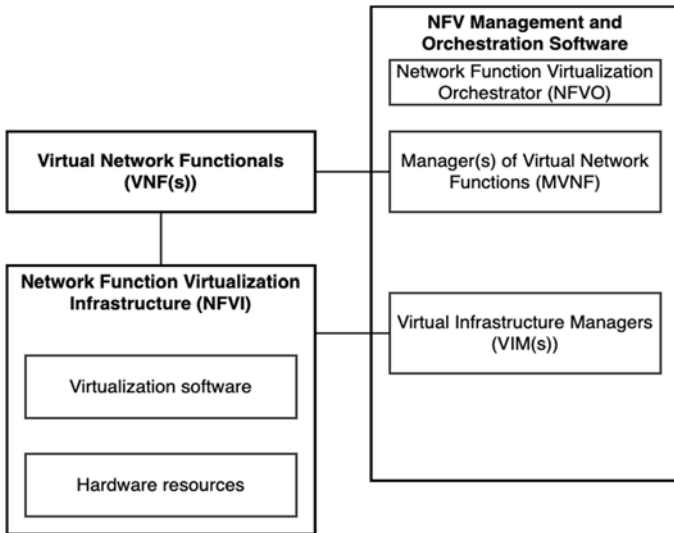


Рис. 2. Упрощенная архитектура виртуализации сетевых функций аппаратных средств связи (коммутаторов, маршрутизаторов и т.д.)

Для правильного и скоординированного функционирования инфраструктуры и функций NFV используется оркестратор NFVO. Его главными функциями являются подключение и создание экземпляров VNF и сетевых служб, изменение ресурсов инфраструктуры. Оркестратор постоянно взаимодействует с менеджером VNF, который следит и обеспечивает жизненный цикл всех сетевых функций. Менеджер VIM управляет и контролирует инфраструктурой. Его ключевыми функциями являются идентификация средств инфраструктуры (аппаратные и программные), перераспределение ресурсов между виртуальными сущностями (виртуальными машинами или контейнерами), мониторинг параметров функционирования виртуальных сущностей и их взаимодействий.

Концепция NFV позволяет заменить функции устройств BNG/BRAS – шлюзы-сервера для подключения абонентов в глобальную сеть. В качестве сетевых функций BRAS выступают протоколы установления сессий PPPoE, DHCP/IPoE, реализация сервера RADIUS для управления абонентскими сессиями, автоматическое создание VLAN для каждого отдельного сервиса (S-VLAN), реализация протокола GRE для HTTP Redirect сервера, реализация QoS на уровне VLAN. В классическом аппаратном исполнении BRAS имеют высокую стоимость и проприетарные реализации вышеперечисленных функций, которые привязаны к аппаратной части. Инфраструктура NFV позволяет реализовать такой функционал на группе серверов общего пользования с возможностью масштабирования функционала.

Помимо этого, NFV позволяет реализовать без специализированных аппаратных средств DPI – глубокая инспекция пакетов – функция, позволяющая оператору связи ограничивать или определять уровень сервиса (квоту, скорость) для определённого типа приложения или содержимого.

Таким образом, концепция NFV позволяет повысить производительности сети, оптимизировать загрузку ресурсов аппаратных устройств, сократить расходы на приобретение и техническое обслуживание специфических аппаратных и аппаратно-программных телекоммуникационных устройств,

уменьшить энергопотребление сети, а также унифицировать реализацию сетевых функций на аппаратных средствах.

Для реализации данного подхода необходимо выбрать реализацию для уровня передачи данных (data plane) и для уровня управления (control plane). Сервер сетевых функций показан на рисунке 3.

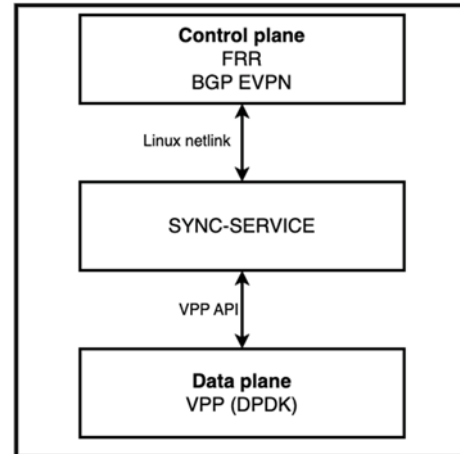


Рис. 3. Сервер сетевых функций

Для обеспечения необходимого уровня производительности Data Plane было выбрана реализация VPP [9] на основе DPDK [10]. Платформа VPP [9] – одна из новейших платформ для высокоскоростной обработки пакетов. Она полностью выполняется в пространстве пользователя и реализует методы обхода ядра для доступа к оборудованию. Ее дизайн не зависит от оборудования, ядра и развертывания. В отличие от старых методов обработки «пакет за пакетом», VPP обрабатывает сразу вектор пакетов. Таким образом, это обработка "вектор за вектором". VPP использует сервисы DPDK [10] для обхода ядра и доступа к аппаратному обеспечению. Пакет DPDK является интегрированной частью пакета VPP. Сетевой ввод-вывод реализован DPDK, а обработка пакетов реализована приложением VPP. VPP использует DPDK для получения вектора пакетов с сетевой карты, а затем обрабатывает все пакеты в векторе. Вектор – это группа пакетов, которые обрабатываются одновременно. Текущий размер вектора равен 256 пакетов.

Как только буфер пакетов (один вектор) становится доступен, VPP начинает обработку всех пакетов в векторе. Обработка VPP реализована в виде графа пересылки. Каждый узел представляет собой сетевую функцию. Существует четыре типа узлов: 1) Предварительный ввод 2) Входной сигнал 3) Внутренний 4) Процесс. Узлы предварительного ввода – это функции, которые обрабатывают выборку пакетов с аппаратного обеспечения и делают буфер индексов доступным для VPP. Узел ввода может находиться в двух состояниях: прерывание или опрос. Входные узлы находятся в режиме прерывания, когда количество пакетов, доступных в буфере, меньше пяти. Когда доступно более 10 пакетов, узел переходит из режима прерывания в режим опроса. В режиме опроса узел непрерывно продолжает проверять, есть ли какие-либо пакеты, доступные для заполнения вектора и обработки.

Узлы процесса – это отдельные узлы, которые не подключены к графу. Они выполняются отдельно как потоки. Каждый узел предсказывает следующий узел после обработки вектора и отправляет пакеты различным следующим узлам на основе своего решения. Это называется предсказанием ветвления.

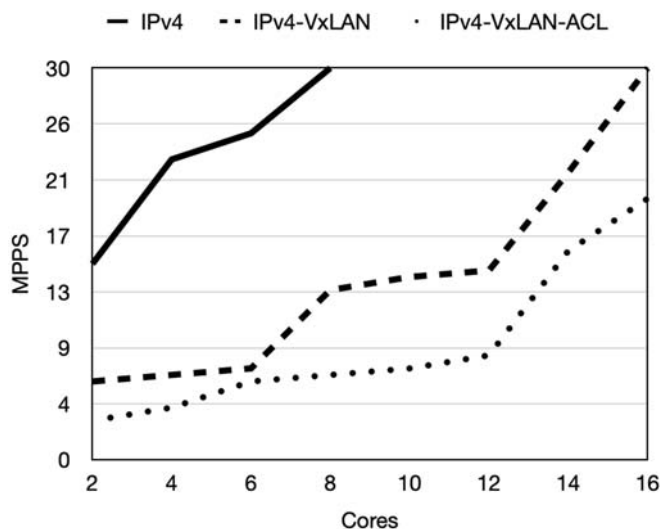


Рис. 4. Производительность VPP

Результаты тестов (рис. 4) показывают, что на 1 ядре Xeon Cascade Lake технология VPP выдает производительность порядка 20 Mpps при IPv4 трафике. Комбинации обработки IPv4-lookup, VxLAN, Енсар/Decap, ACL-lookup показывают более низкую производительность. Также, из результатов тестов видно, что производительность обработки трафика при добавлении ядер процессора растет нелинейно. Сервер с Intel Xeon 6238 2.2GHz с сетевой картой Intel x710, RAM 512 Gb показал производительность 20 Mpps на 16 ядрах при обработке трафика IPv4-VxLAN-ACL.

В качестве Control plane выбрана открытая реализация BGP – FRR [11]. FRR предоставляет услуги IP-маршрутизации. Его роль в сетевом стеке заключается в обмене информацией о маршрутизации с другими маршрутизаторами, принятии решений о маршрутизации и политике и информировании других уровней об этих решениях. В наиболее распространенном сценарии FRR устанавливает решения о маршрутизации в ядро операционной системы, позволяя сетевому стеку ядра принимать соответствующие решения о переадресации. В дополнение к динамической маршрутизации FRR поддерживает полный спектр конфигураций L3, включая статические маршруты, адреса, рекламные объявления маршрутизаторов и т.д. Он также обладает некоторыми облегченными функциями L2, но это в основном зависит от платформы. Помимо этого, FRR поддерживает EVPN VxLAN и сравнительно легко интегрируется с выбранным Data plane. Для реализации FRR используется программный пакет FRRouting [11], который позволяет реализовать помимо BGP такие протоколы как OSPF, IS-IS, EIGRP, VRRP и т.д. Для конфигурирования используется Cisco-like команды. FRRouting возможно устанавливать и использовать на виртуальных сущностях с NIX системами.

Доставка трафика до сетевых функций IP-фабрики

В работе [1] анализируется проблема растущего спроса на виртуализацию ресурсов в центрах обработки данных. Виртуализация аппаратных средств обеспечивает такие преимущества, как более высокая загрузка аппаратных средств (за счет реализации нескольких виртуальных сущностей на аппаратном средстве), уменьшение времени ожидания пользователя, эффективное энергопотребление. Однако сеть передачи данных центров обработки данных также должна поддерживать повышенный спрос на виртуализацию. Согласно [1], этот растущий спрос возможно преодолеть за счет применения NFV, применяя изоляцию трафика, изоляцию адресного пространства (использование одного и того же адресного пространства в изолированных виртуальных сетях).

Для доставки трафика до сетевых функций IP-фабрики используется технология VxLAN [12]. Данная технология разработана для решения проблем масштабируемости VLAN. VxLAN с его 24-разрядным идентификатором сегмента может поддерживать до 16 миллионов виртуальных сетей. VxLAN инкапсулирует фреймы Ethernet в UDP-пакеты, позволяя создавать виртуализированные подсети L2 уровня L3. Таким образом, организуется VxLAN-туннель с коммутатора IP-фабрики непосредственно на сервер сетевых функций.

В данном сценарии нет необходимости перенаправлять трафик на сетевые функции On-Demand (т.е. устанавливать соединения только в случае активности определенного типа трафика), сервисы которым требуется специфическая обработка трафика определены заранее. Группа сервисов определяется одним VRF с доступом в глобальную таблицу через ACL.

Таким образом, VxLAN позволяет делать изоляцию L3. Также для безопасности L2 используется Switched Virtual Interface (SVI) [13] для скрытия MAC-адреса. SVI работает как шлюз по умолчанию. Также для безопасности VxLAN может использовать отдельную таблицу VRF для изоляции адресного пространства, что также позволяет использовать одни и те же IP-адреса разными клиентами в разных адресных пространствах.

Для построения overlay предлагается использовать EVPN VXLAN Type5 IP-PREFIX-ROUTE (RFC9136 [14]), модель IP-VRF-to-IP-VRF, без ESI/GW Overlay Index.

В [2] описывается технология EVPN для уровня управления NFV при использовании в мультитенантных центрах обработки данных. Одной из функций уровня управления NFV является управления потоками трафика между конечными точками NFV. Для реализации потоков данных трафика необходима плоскость данных, которая реализует переадресацию (маршрутизацию) трафика в сети на основе уровня управления. В [2] рассматривают возможность EVPN для изоляции сетевого трафика для каждого клиента, расширение возможностей подключения на L2 за счет мобильности MAC и возможности масштабирования уровня управления.

EVPN является расширением сообщества Multi Protocol-BGP (MP-BGP) [15], который является новой основой для вычисления достижимости сетевого уровня BGP (NLRI). EVPN NLRI используется расширение MP-BGP под названием Ad-



dress Family Identifier (AFI) и Subsequent Address Family Identifier (SAFI). For EVPN the AFI is 25 (i.e. L2 VPN) and the SAFI is 70 (i.e. EVPN) [4]. В [5] описываются типы маршрутов для EVPN, которые представлены в таблице 1.

Таблица 1

Типы маршрутов EVPN

Type	Description
RT-1	Ethernet Auto-discovery Route
RT-2	MAC/IP Advertisement Route
RT-3	Inclusive Multicast Ethernet Tag Route
RT-4	Ethernet Segment Route
RT-5	IP Prefix Route

Для балансировки трафика между серверами сетевых функций (решение проблемы масштабирования и резервирования) используется ECMP (Equal-Cost Multi-Path routing) [6]. ECMP определяет стоимость (вес) путей до точки доставки, допускает наличие одинаковых путей по весу и может осуществлять балансировку нагрузки трафика между путями с одинаковым весом. Применение ECMP для балансировки нагрузки между одинаковыми по стоимости маршрутами повышает эффективность использования сетевых ресурсов, а также отказоустойчивость сети. ECMP рекомендуется использовать совместно с EVPN [24].

Так как в центрах обработки данных присутствует большое количество трафика север-юг, то он может быть обслужен (передан по назначению) на основе сопоставления таблицы VRF клиента и таблицы маршрутизации VRF на border leaf switches, которые подключены непосредственно к граничным маршрутизаторам. Border leaf switches помещают информацию о маршрутах в глобальную таблицу маршрутизации для взаимодействия с внешним миром. Помещение информации о маршрутах из VRF клиентов в глобальную таблицу маршрутизации возможно за использования VRF на border leaf switches [7].

Также EVPN допускает многозадачность сегментов Ethernet (ES) (устройство или сеть устройств, подключенные к одному или нескольким каналам связи), в отличие от VxLAN. Полностью активное многозвенное соединение позволяет распределять нагрузку трафика по потокам для эффективного использования каналов. Однако такой режим работы имеет недостаток – могут возникать циклы. Для избегания таких ситуаций в EVPN подход расщепления горизонта, который не допускает обратную отправку пакета, пришедшего по многоадресному соединению. Метка MPLS использует EVPN для фильтрации на основе расщепления горизонта. Когда устройство получает кадр с мультиадресной рассылкой и пытается его переслать, оно проверяет метку, и, в случае совпадения исходящего и входящего интерфейса, кадр не пересылается. Помимо этого, EVPN позволяет выбирать пересыльного таким образом, чтобы трафик многоадресной рассылки можно было отправлять только одному каналу. Это позволяет предотвратить передачу дублированного многоадресного трафика и образования лавинного трафика.

Развертывание EVPN-VxLAN обеспечивает такие преимущества, как наличие архитектуры на основе открытых стандартов, эффективное подключение на L2/L3 на основе

плоскости управления, сегментирование внутренней сети и адресного пространства, мобильность MAC-адресов позволяет эффективно масштабировать и развертывать сеть.

Таким образом, реализация сетевых функций в IP-фабрике центра обработки данных может быть представлена как на рисунке 5.

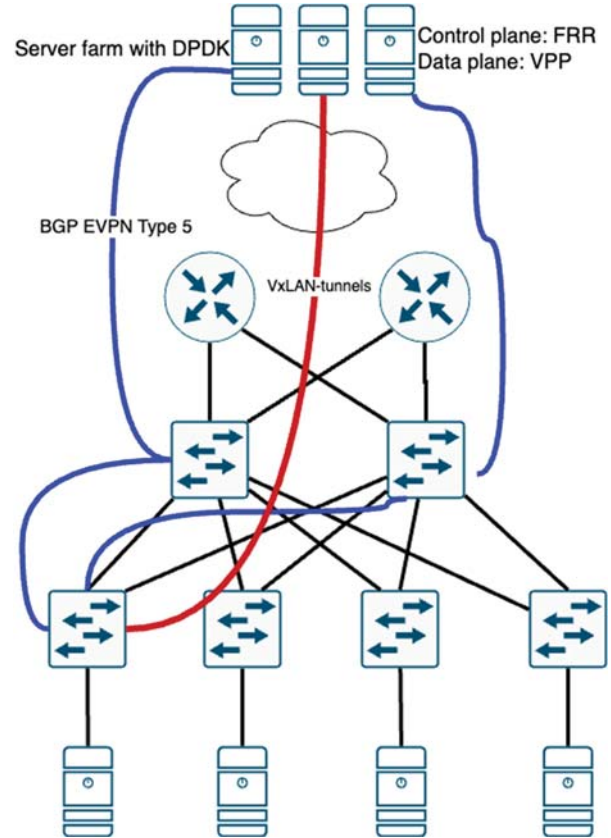


Рис. 5. Архитектура реализации сетевых функций в IP-фабрике

Заключение

В данной статье осуществлен поиск эффективный способ реализации виртуализации сетевых функций в IP-фабрике центра обработки данных. Способ основан на технологиях VPP и FRR. Технология VPP использует сервисы DPDK для обхода ядра и доступа к аппаратному обеспечению.

Проведены экспериментальные измерения обработки различного сетевого трафика с использованием предложенного способа реализации NFV. Результаты экспериментальных тестов показывают, что на 1 ядре Xeon Cascade Lake технология VPP выдает производительность порядка 20 Mpps при IPv4 трафике.

Комбинации обработки IPv4-lookup, VxLAN, Encap/Decap, ACL-lookup показывают более низкую производительность. Таким образом, обоснованность данного подхода доказана экспериментально. Также предложена архитектура для доставки различного пакетного трафика до сетевых функций IP-фабрики на основе VxLAN. Для построения overlay предлагается использовать EVPN VXLAN Type5 IP-PREFIX-ROUTE, модель IP-VRF-to-IP-VRF, без ESI/GW Overlay In-

дех. Предложенная архитектура позволяет эффективно обрабатывать трафик в направлении север-юг в центре обработки данных, изолировать адресные пространства и осуществлять балансировку нагрузки по маршрутам с одинаковым весом.

Литература

1. Narten T., Ed., Gray E., Ed., Black D., Fang L., Kreeger L., Napierala M. Problem Statement: Overlays for Network Virtualization. RFC 7364. 2014, pp. 1-23. URL: <http://www.hjp.at/doc/rfc/rfc7364.html> (дата обращения 23.01. 2024).
2. Sajassi A., Drake J., Bitar N., Shekhar R., Uttaro J., Henderickx W. A Network Virtualization Overlay Solution Using Ethernet VPN (EVPN), tech. rep., IETF, 2018. URL: <https://tools.ietf.org/html/rfc8365> (дата обращения 23.01. 2024).
3. Nadeau T., Drake J., Schlisser B., Rekhter Y., Shekhar R., Bitar N., Isaac A., Uttaro J., Hendrix W. A Control Plane for Network Virtualized Overlays, tech. rep., IETF, 2012. URL: <https://tools.ietf.org/html/draft-drake-nvo3-evpn-control-plane-00> (дата обращения 23.01. 2024).
4. Sajassi A., Aggarwal R., Bitar N., Isaac A., Uttaro J., Drake J., Henderickx W. BGP MPLS-Based Ethernet VPN, RFC 7432 (2015). URL: <https://tools.ietf.org/html/rfc7432#section-7> (дата обращения 23.01. 2024).
5. Rabadan E. J., Henderickx W., Drake J., Lin W., Sajassi A. IP Prefix Advertisement in EVPN, tech. rep., IETF, 2018. URL: <https://tools.ietf.org/html/draft-ietf-bess-evpn-prefix-advertisement-11> (дата обращения 23.01. 2024).
6. Sajassi A., Aggarwal R., Uttaro J., Bitar N., Henderickx W., Isaac A. Requirements for Ethernet VPN (EVPN), tech. rep., IETF, 2014. URL: <https://tools.ietf.org/html/rfc7209> (дата обращения 23.01. 2024).
7. Isaac A. Building blocks in evpn for multi-service fabrics. 2019. URL: https://pc.nanog.org/static/published/meetings/NANOG75/1903/20190219_Isaac_Building_Blocks_In_v1.pdf (дата обращения 23.01. 2024).
8. Herrera J.G., Botero J.F. Resource allocation in NFV: A comprehensive survey // IEEE Transactions on Network and Service Management, 2016. Vol. 13. No.3. C. 518-532.

9. Saboori H., Mohammadi M., Taghe R. Virtual power plant (VPP), definition, concept, components and types // 2011 Asia-Pacific power and energy engineering conference. IEEE, 2011. c. 1-4.

10. Kourtis M.A. et al. Enhancing VNF performance by exploiting SR-IOV and DPDK packet processing acceleration // 2015 IEEE Conference on Network Function Virtualization and Software Defined Network (NFV-SDN). IEEE, 2015. c. 74-78.

11. Jain V., Edgeworth B. Troubleshooting BGP: A practical guide to understanding and troubleshooting BGP. Cisco Press, 2016.

12. Mahalingam M. et al. Virtual extensible local area network (VXLAN): A framework for overlaying virtualized layer 2 networks over layer 3 networks. 2014. No. rfc7348.

13. Sans F. et al. Analytical performance evaluation of different switch solutions // Journal of Computer Networks and Communications. 2013. Vol. 2013.

14. Rabadan J. et al. RFC 9136 IP Prefix Advertisement in Ethernet VPN (EVPN). 2021.

15. Pei D., Van der Merwe J. BGP convergence in virtual private networks // Proceedings of the 6th ACM SIGCOMM Conference on Internet Measurement. 2006. c. 283-288.

16. Hiryanto L. et al. Multi-path routing in green multi-stage upgrade for bundled-links SDN/OSPF-ECMP networks // IEEE Access. 2021. Vol. 9. c. 99073-99091.

17. George D.A.S., George A.S.H. A Brief Overview of VXLAN EVPN // Ijireeice International Journal of Innovative Research in Electrical, Electronics, Instrumentation and Control Engineering. 2021. Vol. 9. No. 7. C. 1-12.

18. Salazar-Chacon G., Marrone L. Open Networking for Modern Data Centers Infrastructures: VXLAN Proof-of-Concept Emulation using LNV and EVPN under Cumulus Linux // 2022 IEEE Sixth Ecuador Technical Chapters Meeting (ETCM). IEEE, 2022. c. 1-6.

19. Cardona R. VXLAN BGP EVPN Fabric Configuration Templates // The Fast-Track Guide to VXLAN BGP EVPN Fabrics: Implement Today's Multi-Tenant Software-Defined Networks. Berkeley, CA: Apress, 2021. C. 209-242.

20. Previdi S., Aries E., Afanasiev D. RFC 9087: Segment Routing Centralized BGP Egress Peer Engineering. 2021.

21. Pucci D., Casoni G. Monitoring an EVPN-VxLAN fabric with BGP Monitoring Protocol. 2020.

IMPLEMENTING NETWORK FUNCTIONS IN A DATA CENTER IP FABRIC

IGOR G. BUZHIN

Moscow, Russia, i.g.buzhin@mtuci.ru

VERONIKA M. ANTONOVA

Moscow, Russia, v.m.antonova@mtuci.ru

VLADISLAV S. GNEZDILOV

Moscow, Russia, v.s.gnezdilov@mtuci.ru

YURIY B. MIRONOV

Moscow, Russia, i.b.mironov@mtuci.ru

ABSTRACT

Introduction: In modern data centers, IP fabrics are often used, which are a system of interconnected network devices with a high degree of interconnection, thereby minimizing the distance between end nodes, reducing delays, and devices function more efficiently. At the same time, many procedures are transferred to an overlay network using network function virtualization technology. In this regard, there is a problem of effective implementation of network functions in the IP fabric of the data center. **The purpose of the study** is to find an effective way to implement virtualization of network functions in the IP fabric of a data center. **The validity of this approach** has been proved experimentally. This approach works to handle different types of traffic.

KEYWORDS: IP fabric, FRR, Network Function Virtualization (NFV), VPP, VxLAN.

Results: An approach to the implementation of network functions in the IP fabric of a data processing center is proposed. The method of processing traffic on a public server based on VPN and FRR technology has been selected. The results of test measurements of processing various traffic on the data plane are shown. The results of experimental tests show that on 1 core of Xeon Cascade Lake, VPP technology produces a performance of about 20 Mpps with IPv4 traffic. Combinations of IPv4 lookup, VxLAN, Encap/Decap, and ACL lookup processing show lower performance. A method for delivering traffic to the network functions of an IP fabric based on VxLAN, EVPN and ECMP technologies is proposed.



REFERENCES

1. T. Narten, E. Gray, D. Black, L. Fang, L. Kreeger, M. Napierala, "Problem Statement: Overlays for Network Virtualization," *RFC 7364* 2014, pp. 1-23. URL: <http://www.hjp.at/doc/rfc/rfc7364.html> (date of access Accessed 23.08. 2019).
2. A. Sajassi, J. Drake, N. Bitar, R. Shekhar, J. Uttaro, W. Henderickx, "A Network Virtualization Overlay Solution Using Ethernet VPN (EVPN)," *tech. rep., IETF*, 2018. URL: <https://tools.ietf.org/html/rfc8365>.
3. T. Nadeau, J. Drake, B. Schlisser, Y. Rekhter, R. Shekhar, N. Bitar, A. Isaac, J. Uttaro, W. Hendrix, "A Control Plane for Network Virtualized Overlays," *tech. rep., IETF*, 2012. URL: <https://tools.ietf.org/html/draft-drake-nvo3-evpn-control-plane-00>.
4. A. Sajassi, R. Aggarwal, N. Bitar, A. Isaac, J. Uttaro, J. Drake, "Henderickx W. BGP MPLS-Based Ethernet VPN," *RFC 7432*. 2015. URL: <https://tools.ietf.org/html/rfc7432#section-7> (date of access 4.10.2019).
5. E.J. Rabadan, W. Henderickx, J. Drake, W. Lin, A. Sajassi, "IP Prefix Advertisement in EVPN," *tech. rep., IETF*, 2018. URL: <https://tools.ietf.org/html/draft-ietf-bess-evpn-prefix-advertisement-11>.
6. A. Sajassi, R. Aggarwal, J. Uttaro, N. Bitar, W. Henderickx, A. Isaac, "Requirements for Ethernet VPN (EVPN)," *tech. rep., IETF*, 2014. URL: <https://tools.ietf.org/html/rfc7209>.
7. A. Isaac, "Building blocks in evpn for multi-service fabrics," 2019. URL: https://pc.nanog.org/static/published/meetings/NANOG75/1903/20190219_Isaac_Building_Blocks_In_v1.pdf.
8. J.G. Herrera, J.F. Botero, "Resource allocation in NFV: A comprehensive survey," *IEEE Transactions on Network and Service Management*, 2016. Vol. 13. No.3, pp. 518-532.
9. H. Saboori, M. Mohammadi, R. Taghe, "Virtual power plant (VPP), definition, concept, components and types," *2011 Asia-Pacific power and energy engineering conference*. IEEE, 2011, pp. 1-4.
10. M.A. Kourtis et al., "Enhancing VNF performance by exploiting SR-IOV and DPDK packet processing acceleration," *2015 IEEE Conference on Network Function Virtualization and Software Defined Network (NFV-SDN)*. IEEE, 2015, pp. 74-78.
11. V. Jain, B. Edgeworth, "Troubleshooting BGP: A practical guide to understanding and troubleshooting BGP," Cisco Press, 2016.
12. M. Mahalingam et al., "Virtual extensible local area network (VXLAN): A framework for overlaying virtualized layer 2 networks over layer 3 networks," 2014. No. rfc7348.
13. F. Sans et al., "Analytical performance evaluation of different switch solutions," *Journal of Computer Networks and Communications*. 2013. Vol. 2013.
14. J. Rabadan et al., "RFC 9136 IP Prefix Advertisement in Ethernet VPN (EVPN)," 2021.
15. D. Pei, J. Van der Merwe, "BGP convergence in virtual private networks," *Proceedings of the 6th ACM SIGCOMM Conference on Internet Measurement*. 2006, pp. 283-288.
16. L. Hiryanto et al., "Multi-path routing in green multi-stage upgrade for bundled-links SDN/OSPF-ECMP networks," *IEEE Access*. 2021. Vol. 9, pp. 99073-99091.
17. D.A.S. George, A.S.H. George, "A Brief Overview of VXLAN EVPN," *Ijireice International Journal of Innovative Research in Electrical, Electronics, Instrumentation and Control Engineering*. 2021. Vol. 9. No. 7, pp. 1-12.
18. G. Salazar-Chacon, L. Marrone, "Open Networking for Modern Data Centers Infrastructures: VXLAN Proof-of-Concept Emulation using LNV and EVPN under Cumulus Linux," *2022 IEEE Sixth Ecuador Technical Chapters Meeting (ETCM)*. IEEE, 2022, pp. 1-6.
19. R. Cardona, "VXLAN BGP EVPN Fabric Configuration Templates," *The Fast-Track Guide to VXLAN BGP EVPN Fabrics: Implement Today's Multi-Tenant Software-Defined Networks*. Berkeley, CA: Apress, 2021, pp. 209-242.
20. S. Previdi, E. Aries, D. Afanasiev, "RFC 9087: Segment Routing Centralized BGP Egress Peer Engineering," 2021.
21. D. Pucci, G. Casoni, "Monitoring an EVPN-VxLAN fabric with BGP Monitoring Protocol," 2020.

INFORMATION ABOUT AUTHORS:

Igor G. Buzhin, PhD, Associate Professor of the Department "Fixed-line networks and Systems", Moscow Technical University of Communications and Informatics, Moscow, Russia

Veronika M. Antonova, PhD, docent, Head of the Department "Fixed-line networks and Systems", Moscow Technical University of Communications and Informatics, Moscow, Russia

Vladislav S. Gnezdilov, assistant of the Department "Fixed-line networks and Systems", Moscow Technical University of Communications and Informatics, Moscow, Russia

Yuriy B. Mironov, PhD, Dean of the Faculty of "Networks and Communication Systems", Moscow Technical University of Communications and Informatics, Moscow, Russia

For citation: Buzhin I.G., Antonova V.M., Gnezdilov V.S., Mironov Yu.B. Implementing network functions in a data center IP fabric. H&ES Reserch. 2024. Vol. 16. No 3. P. 39-45 doi: 10.36724/2409-5419-2024-16-3-39-45 (In Rus)

ОДНОВРЕМЕННАЯ ПЕРЕДАЧА ЗАЩИЩЕННОГО СООБЩЕНИЯ И ГАММА-КЛЮЧА К НЕМУ В ОДНОМ ЧАСТОТНОМ КАНАЛЕ С ПРИЕМОМ НА АНТЕННУЮ РЕШЕТКУ С УПРАВЛЯЕМОЙ ПОЛЯРИЗАЦИОННОЙ ХАРАКТЕРИСТИКОЙ

БЕЛОВ

Никита Вадимович¹

РЕПИНСКИЙ

Владимир Николаевич²

АННОТАЦИЯ

Введение: представлены результаты анализа и моделирования приема двух независимых последовательностей, передаваемых на одной частоте, но с противоположными эллиптическими поляризациями. **Методы:** При вращении антенны в том числе и электрическом путем поочередного переключения диполей, в простейшем случае двух перпендикулярных полуволновых вибраторов, спектр волны с круговой поляризацией, совпадающей по направлению с вращением антенны, смещается по частоте вверх, а волны противоположного направления вращения электрического вектора, соответственно вниз. Вращение возможно для антенн различного типа, как традиционных, так и магнитных, представляющих собой взаимно перпендикулярные катушки. Принципиальным здесь является только вращение вектора поляризации, что обеспечивает лучшее разделение каналов, чем перпендикулярные линейные поляризации. Показано, что выделение этих смещенных спектров возможно с помощью частотной фильтрации после преобразования в управляемой антенной решетке. **Результаты:** проанализированы переходные помехи между ортогональными поляризационными каналами и показано, что максимальный уровень мощности переходной помехи не превышает 15% от суммарного уровня сигнала вблизи приемной антенны, а в случае небольшой эллипсности траектории вектора E составляет от долей до единиц процентов. Вследствие этого появление переходных помех, обусловленных отличием поляризации волн от круговой, практически не влияет на процесс обнаружения, то есть описываемы здесь способ одночастотной передачи кодированного сообщения и ключа актуален. В силу того, что для обнаружения ортогональных поляризационных составляющих необходимо техническое решение, не связанное с ориентацией антенны, делается вывод об удовлетворительной защищенности сообщения, передаваемого в оперативной обстановке.

Сведения об авторах:

¹старший преподаватель кафедры ИСУиА МТУСИ, Москва, Россия, n.v.belov@mtuci.ru

²доцент кафедры ИСУиА МТУСИ, Москва, Россия, repinski@rambler.ru

КЛЮЧЕВЫЕ СЛОВА: круговая поляризация, управляемая поляризационная характеристика, переходные искажения, спектральная плотность, гамма-последовательность.

Для цитирования: Белов Н.В., Репинский В.Н. Одновременная передача защищенного сообщения и гамма-ключа к нему в одном частотном канале с приемом на антенную решетку с управляемой поляризационной характеристикой // Научно-технические исследования в космических исследованиях Земли. 2024. Т. 16. № 3. С. 46-54. doi: 10.36724/2409-5419-2024-16-3-46-54



Введение

Авторы считают необходимым почтить добрую память д.т.н., профессора С.С. Аджемова с участием и под руководством которого были начаты эти исследования.

Гаммирование передаваемых дискретных сообщений стало фактически методическим примером для курса информационной безопасности и вытесняется из практики гораздо более эффективными методами шифрования, в частности, системами с открытыми ключами. Однако, сочетание физических и математических методов защиты может быть весьма эффективным и при использовании простейших алгоритмов криптозащиты, к которым относится и метод гаммирования дискретных сообщений.

Использование поляризационной модуляции при передаче дискретной информации известно достаточно давно и осуществляется в радиорелейной связи [1], околоземном космическом пространстве [2] или при решении задач радиолокации [3]. Из всех видов поляризации волн как правило используются ортогональные волны с линейной поляризацией, однако в последние годы появляются работы, описывающие системы связи с круговой поляризацией волн [4, 5].

Прием волны, в которой дискретные посылки передаются на одной частоте и отличаются только поляризацией, с наибольшей эффективностью возможен лишь на соответственно расположенные антенны. При приеме на изотропную антенну (или близкую к таковой) различие посылок становится затрудненным, особенно при деполяризации волн, возникающей из-за неблагоприятных условий распространения, таких как многолучевость, замирания и различные процессы в электромагнитном поле ионосферы.

Но тем не менее, ионосферный механизм распространения волн по-прежнему привлекателен из-за огромных расстояний и высокой защищенности канала ионосферной радиосвязи. Это дает возможность осуществить дважды защищенную передачу – кодированное сообщение и аппаратную защиту.

Переходные искажения

Круговая (или эллиптическая) поляризация [6] чаще всего рассматривается либо как средство для передачи на изотропную приемную антенну, либо как побочный продукт при ионосферном распространении высокочастотных волн вдоль магнитно-силовых линий поля Земли [7]. Однако, определенный интерес представляет и осуществление модуляции волны, путем формирования двух волн одной частоты, но с противоположными вращениями электрического вектора, что в простейшем случае может быть осуществлено путем применения переключаемых спиральных антенн с противоположным ходом спиралей [8] (рис. 1).

В [9] показано, что использование вращающейся приемной антенны, позволяет разнести на разные частоты колебания с правой и левой круговыми или эллиптическими поляризациями. В последнем случае возникают переходные искажения, которые тем меньше, чем ближе поляризация к круговой.

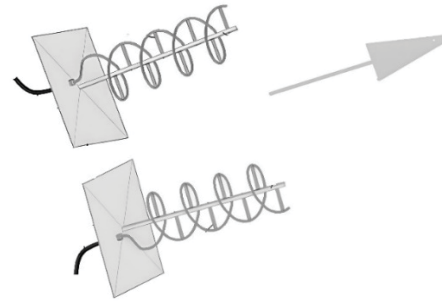


Рис. 1. Система спиральных антенн для манипуляции круговой поляризацией противоположного направления

Реализовать прием вращающейся антенной можно с помощью триортогональной антенны с соответственно переключаемыми вибраторами, то есть вращение имитируется поочередным подключением вибраторов (рис. 2).



Рис. 2. Активная малогабаритная приемная антенна (АМП) с триортогональными вибраторами

Воздействие волны на вращающуюся антенну приводит к проявлению стробоскопического эффекта (можно интерпретировать как эффект Доплера) [10], при котором на выходе антенны наблюдаются колебания с разностной (суммарной) частотами [11]. Если на антенну одновременно действуют две волны с противоположными направлениями вращения электрических векторов, происходит разделение их по частоте с возможностью дальнейшей фильтрации.

Вращать поляризационную характеристику антенны, придавая ей необходимую конфигурацию огибающей, можно меняя эквивалентную длину вибраторов, что реализуется путем управления уровнем поступающего от антенны напряжения [12-13].

Меняющаяся длина вибратора рассчитывается по формуле:

$$\rho = \frac{b}{\sqrt{1 - e_a^2 (\cos(2\pi\Omega_a t))}} \quad (1)$$

где b – физическая длина вибратора антенны, Ω_a – угловая частота вращения поляризационной характеристики антенны, e_a – эксцентриситет эллипса, описываемого огибающей вращающейся антенны. Антенне, вращающейся по кругу, соответствует значение $e_a = 0$.

Координаты мгновенного значения огибающей вращающейся антенны имеют вид:

$$\begin{aligned} \rho y_t &= \frac{b}{\sqrt{1-e_a^2(\cos(2\pi\Omega_a t))}} \cdot \sin(2\pi\Omega_a t) \\ \rho x_t &= \frac{b}{\sqrt{1-e_a^2(\cos(2\pi\Omega_a t))}} \cdot \cos(2\pi\Omega_a t) \end{aligned} \quad (2)$$

Разделенные по частоте колебания встречно вращающихся электрических векторов можно использовать как для образования дополнительного канала приема (поляризационное разнесение) так и для передачи дополнительной информации. В последнем случае в суммарную волну можно вложить как закодированное сообщение, так и ключ для его прочтения. Прием такого колебания на обычную неподвижную антенну не позволяет разделить два канала передачи.

Таким образом может быть осуществлена двойная защита передаваемой информации – физическая и криптографическая. При этом следует учитывать, что при поляризации волн, отличных от круговой, между разнесенными по частоте составляющими возможно появление переходных помех. Эти переходные помехи (рис. 3), наряду с обычными помехами при распространении волны, снижают помехозащищенность системы и в худшем случае недопустимо снижают качество приема, что в данном случае может фатально отразиться на процессе декодирования принятого сообщения (для лучшего разрешения волны показаны с амплитудной модуляцией разными частотами).

В данной статье приводится оценка влияния уровня переходных искажений при передаче гаммированного сообщения и его гамма-последовательности в разнесенных каналах с противоположной круговой поляризацией и эфирными шумами. Особенность описываемого метода разделения колебаний с помощью виртуального вращения поляризационной характеристики фазированной антенной решетки заключается в исключительно электрически переключаемых антенных элементах, полном отсутствии механических вращающихся частей, вследствие чего достижима высокая надежность системы и возможность установки ее на высоко вибрационных платформах типа беспилотных летательных аппаратов.

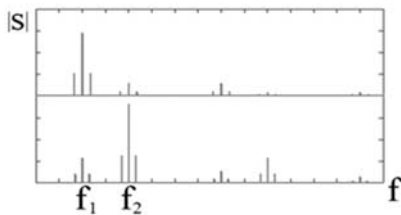


Рис. 3. Перенос спектров двух колебаний одной частоты, но противоположно направленными эллиптическими поляризациями с взаимными переходными помехами

Рассмотрим в качестве примера случай передачи кодированного сообщения последовательностью 010. Используемая при кодировании гамма-последовательность имеет вид 001, следовательно исходная комбинация будет 011. Ошибка при декодировании определяется вероятностью ошибки в

приеме символа, которая, в свою очередь, определяется и внешними шумами и переходными помехами. Так в рассматриваемом примере при вероятности ошибки в приеме символа $P_1 = 10^{-3}$, вероятность ошибки декодирования комбинации из трех разрядов равна (при независимости посылок и помех) $P_2 = 1 - 0.999^3 = 2.997 \cdot 10^{-3}$. При более длинных гамма-последовательностях вероятность неправильной расшифровки почти пропорционально увеличивается.

Мощность помехи, действующей на передаваемый символ, определяется выражением:

$$N_i = N_1 + N_2 \quad (3)$$

где N_1 – мощность эфирных шумов (помех распространения), N_2 – мощность переходных помех.

Расчет мощности переходных помех позволит определить степень помехоустойчивости такого способа передачи информации. Для расчета модифицируем математическую модель, предложенную в [4]. Координаты конца вектора волны, несущей информационное сообщение эллипс которой повернут на угол ψ относительно вектора волны, несущей гамма-последовательность:

Если посылка (элемент сигнала) представляет собой отрезок гармонического колебания:

$$\begin{aligned} \rho x_i &= \frac{U_i}{\sqrt{1-e_i^2(\cos(2\pi\Omega_i t))}} \cdot \cos(2\pi\Omega_i t) \\ \rho y_i &= \frac{U_i}{\sqrt{1-e_i^2(\cos(2\pi\Omega_i t))}} \cdot \sin(2\pi\Omega_i t) \end{aligned} \quad (4)$$

где e_i – эксцентриситет эллипса информационной волны, Ω_i – угловая частота колебания информационной волны, U_i – максимальное значение электрического вектора информационной волны.

Аналогичные выражения справедливы и для волны, несущей гамма-последовательность:

$$\begin{aligned} \rho x_\gamma &= \frac{U_\gamma}{\sqrt{1-e_\gamma^2(\cos(2\pi\Omega_\gamma t))}} \cdot \cos(2\pi\Omega_\gamma t) \\ \rho y_\gamma &= \frac{U_\gamma}{\sqrt{1-e_\gamma^2(\cos(2\pi\Omega_\gamma t))}} \cdot \sin(2\pi\Omega_\gamma t) \end{aligned} \quad (5)$$

$$\begin{aligned} (\rho x_i)_\psi &= \rho x_i \cos(\psi) - \rho y_i \sin(\psi) \\ (\rho y_i)_\psi &= \rho x_i \sin(\psi) + \rho y_i \cos(\psi) \end{aligned} \quad (6)$$

где $\rho x_i, \rho y_i$ проекции конца вектора информационной волны на произвольно выбранную систему координат.

Координаты конца вектора наведенного напряжения от информационной волны во вращающейся антенне:

$$\begin{aligned} \rho X_i &= (\rho x_i)_\psi \rho x_t - (\rho y_i)_\psi \rho y_t \\ \rho Y_i &= (\rho x_i)_\psi \rho y_t + (\rho y_i)_\psi \rho x_t \end{aligned} \quad (7)$$



Координаты конца вектора волны, несущей гамма-последовательность:

$$(\rho x \gamma_t), (\rho y \gamma_t) \quad (8)$$

Координаты конца вектора наведенного напряжения от гамма-волны во вращающейся антенне:

$$\begin{aligned} \rho X \Gamma_t &= (\rho x \gamma_t)_{\psi} \rho x_t - (\rho y i \gamma_t)_{\psi} \rho y_t \\ \rho Y \Gamma_t &= (\rho x \gamma_t)_{\psi} \rho y_t - (\rho y \gamma_t)_{\psi} \rho x_t \end{aligned} \quad (9)$$

В качестве выходного сигнала приемной антенны в случае круговой (эллиптической) поляризации можно использовать колебание с любого из виртуально вращающихся вибраторов, например:

$$\{\rho X \Gamma_t + \rho X U_i\} \quad (10)$$

Для расчета уровня переходных искажений в зависимости от степени вытянутости эллипса поляризации (отношения большой и малой полуосей эллипса) найдем спектральную плотность преобразованного колебания и по ней определим его энергию:

$$|S(\Omega)|^2 = \left| \int_0^T (\rho X \Gamma_t + \rho X U_i) e^{-j\Omega t} dt \right|^2 \quad (11)$$

Аналитическое решение (11) в общем виде весьма громоздко, поэтому было проведено численное моделирование с помощью пакета Mathcad14 [14] и выявлена зависимость доли энергии волны, переходящей в виде помехи в другой канал, в виде простой формулы:

$$\Delta \mathcal{E} = \frac{2}{3} 10^{-6} e^{10\varepsilon} \quad (12)$$

Эта зависимость приведена на рисунке 4.

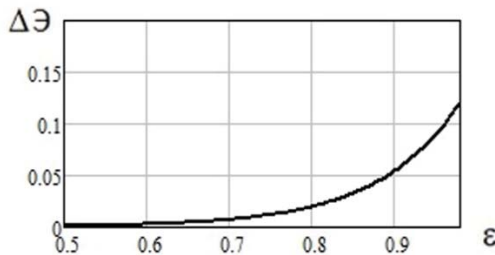


Рис. 4. Доля энергии волны, переходящая на частоту соседнего канала в зависимости от величины эксцентриситета эллипса поляризации

Как видно, максимальная доля энергии переходной помехи составляет примерно 15% от энергии порождающей ее волны, при этом соответственно уменьшается и ее энергия. Так как по обоим каналам передается независимая информация, помеху в приближении можно считать некогерентной и рассматривать ее мощность аддитивно по отношению к эфирным помехам.

Реализация приема на вращающуюся антенну возможна и в рое беспилотных летающих аппаратов (БПЛА), когда антенна состоит из нескольких линейных антенн отдельных

БПЛА, в силу динамики роя, оказавшихся на одной линии определенного азимута (рис. 5), выбранного системой управления, как элемента решетки с управляемой поляризационной характеристикой.

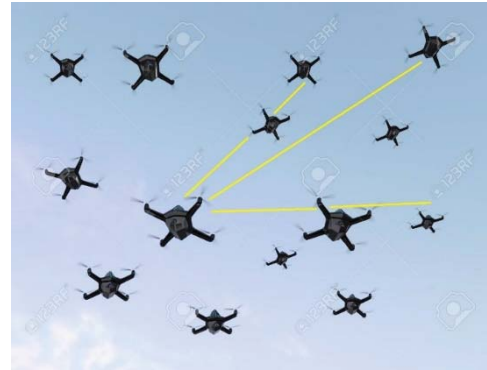


Рис. 5. Переключения антенн в рое БПЛА для реализации антенной решетки с управляемой поляризационной характеристикой

Для обеспечения виртуального вращения антенны в следующий момент для образования повернутого антенного луча выбирается другое сочетание дронов, образующих другой антенный луч, повернутый на угол $\Delta \psi$, определяемый рабочей частотой обрабатываемого сигнала, и характеристиками фильтров постобработки (рис. 11).

Разумеется, строго соосное размещение летательных аппаратов возможно не всегда, поэтому приходится мириться с неточностью построения, то есть рассматривать в качестве элементов фазированной антенной решетки антенны аппаратов, расположенные неточно по лучу предполагаемого виртуального вращения, так и под углом, неравным $\Delta \psi$. Однако влияние этих неточностей положения предположительно не уничтожает саму идею такого построения фазированной антенной решетки, но определяет направление дополнительного исследования влияния такого фактора на эффективность системы.

При проектировании системы следует помнить, что использование некоторых видов сигналов, в частности шумоподобных, в диапазоне дециметровых волн, обеспечивающих не только дальнейшее распространение (до 2500–3000) км, но и дополнительную защиту от прослушивания возможно лишь в полосе частот до 50 кГц [15]. В силу этого значительная доля решений, принимаемых системой управления, должны быть отдана искусственному интеллекту. Отметим важные преимущества, предоставляемые настоящей системой:

1. Скрытность передачи сигналов управления роём БПЛА за счет использования шумоподобных сигналов с полосой до 50 кГц.
2. Скрытность передачи сигналов управления роём БПЛА за счет использования шифрования сигнала по методу гаммирования.
3. Скрытность передачи гамма-последовательности за счет использования одного частотного канала и поляризационного разнесения.

Необходимые условия для реализации системы

1. Значительная доля использования искусственного интеллекта в алгоритме системы управления в силу малой пропускной способности декаметрового радиоканала с шумоподобным сигналом.

Влияние переходных помех на ошибку обнаружения

Помеха, действующая в информационном канале и в канале с гамма-последовательностью в полосе частот, определяемой преселектором приемника и, в небольшой степени антенны, может считаться случайным колебанием с гауссовым распределением, определяющим вероятность ошибки в приеме символа. Как известно [16], вероятность ошибки в этом случае может быть рассчитана по формуле:

$$P_{ош} = 1 - F(H) \tag{13}$$

где $F(H)$ – интеграл вероятности, а аргумент.

$$H = \sqrt{\frac{(E_0 + E_1)}{2N_0(1 - \lambda)}} \tag{14}$$

в выражении которого E_0 и E_1 энергии посылок, N_0 – соответственно шума, а коэффициент λ в случае фазовой манипуляции на π при равенстве энергий посылок равен 0, следовательно:

$$H = \sqrt{\frac{E_0}{N_0}} \tag{15}$$

Для оценки влияния на вероятность ошибки степени эллиптичности поляризации волны воспользуемся выражением (15), добавляя к знаменателю долю энергии, переходящую из канала с противоположным направлением вращения электрического вектора:

$$P_{эош} = 1 - F(H_1) \tag{16}$$

где

$$H = \sqrt{\frac{E_0}{N_0 + \Delta N_э}} \tag{17}$$

$\Delta N_э$ – доля энергии, поступающая в канал из-за переходных помех, вызванных эллиптичностью волны.

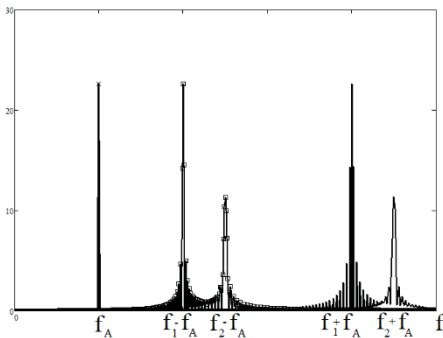


Рис. 6. Модуль спектральной плотности колебаний волн, вращающейся с частотой f_a , с круговой поляризацией, принятой антенной с вращающейся поляризационной характеристикой

Спектр информационного колебания $(f_1 - f_A; f_2 - f_A)$ переносится «вниз» на частоту вращения поляризационной характеристики антенны, а спектр сигнала с гамма-информацией $(f_1 + f_A; f_2 + f_A)$ на частоту выше. Если вращать антенную характеристику в противоположную сторону, спектры поменяются местами [17].

Разница в уровне спектральных составляющих на выходе антенны на рисунке 5 объясняется особенностью рассматриваемого примера, когда из трех посылок две одной частоты. На рисунке 5 не видны переходные помехи, возникающие из-за эллиптичности поляризации волн, они показаны отдельно на рисунке 7.

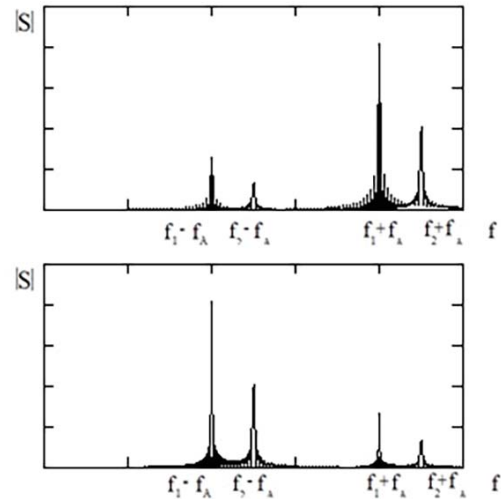


Рис. 7. Образование переходных помех между каналами с противоположным вращением электрического вектора

Если волны поляризованы по кругу, переходных помех нет, они в этом случае появляются, когда огибающая поляризационной характеристики вращающейся антенны эллипс.

Из этого следует, что при организации канала связи в пределах прямой видимости и без подстилающих поверхностей (например, в космосе) переходных помех нет и передача гамма-шифрования не снижает пропускной способности по сравнению с традиционным каналом связи без такой передачи. Если изобразить это колебание в виде фазового портрета, то это динамически меняющаяся в зависимости от расстановки битов в сообщении фигура с огибающей в виде круга (рис. 8). Если же одного из каналов нет, то просто круг.

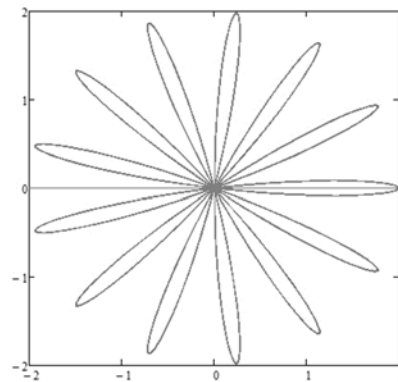


Рис. 8. Фазовый портрет двухканального одночастотного поляризованного колебания



Рассчитав энергию переходной помехи с помощью (11) и вероятность ошибки по (13-17), построим кривую зависимости вероятности ошибки от смеси отношения уровней сигнала к суммарной энергии переходной помехи и аддитивных гауссовых шумов (рис. 9).

Как видно, при малом уровне входного колебания антенны превалируют каналные помехи, уровень переходных помех между поляризационными каналами мал и на вероятность ошибки влияет мало. А при относительно большом уровне переходных искажений, возникающих при сильной эллиптичности волновой поляризации ($\epsilon > 0.8$) и высоком уровне энергии волны возле антенны, вероятность ошибки может возрастать в десятки и даже сотни раз по сравнению с неподвижной антенной. Однако эллипсы поляризации с эксцентриситетом более 0.7 в свободном пространстве редки (рис. 9), поэтому можно сделать вывод о пренебрежимо малом влиянии переходных помех на помехоустойчивость двухканальной системы связи с круговой поляризацией противоположного вращения.

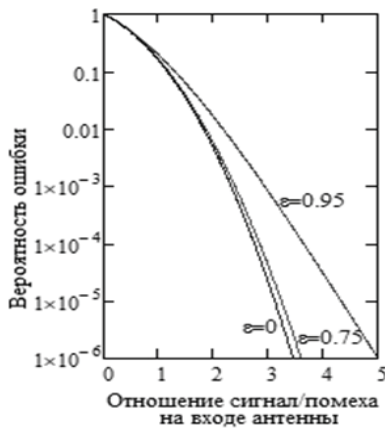


Рис. 9. Зависимость вероятности ошибки при приеме символа от суммарного уровня шумовых и переходных помех

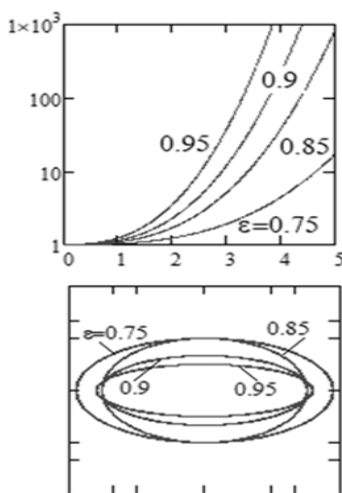


Рис. 10. Кратность увеличения вероятности ошибки в зависимости от отношения сигнал-помеха и эксцентриситета эллипса поляризации

Моделирование

Для более ясного представления приведем результаты моделирования преселекции и детектирования эллиптически поляризованного двухканального сигнала с последующей иллюстрацией порогового решения (рис. 11) [18].

Искажения принятой и преобразованной последовательностей определяются эфирными помехами и переходными шумами между поляризационными каналами передачи.

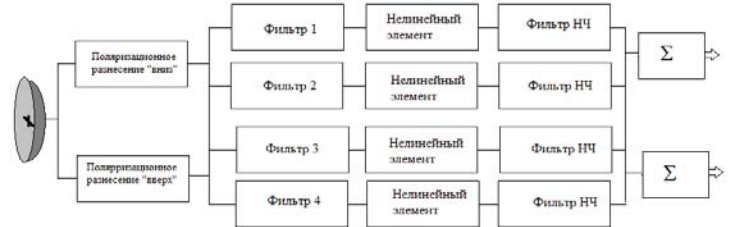


Рис. 11. Структурная схема процесса детектирования двух ЧМ колебаний, передаваемых с поляризационным разнесением

При значении эксцентриситета эллипса поляризации, не превышающем 0.75, на временной диаграмме входного и выходного сигналов демодулятора влияние переходных искажений на фоне эфирных помех практически неразличимо (рис. 12).

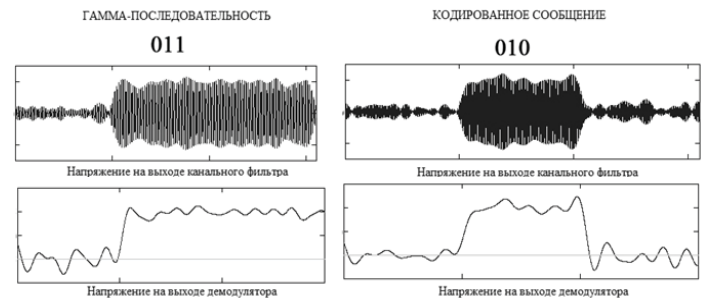


Рис. 12. Колебания на входе и выходе демодулятора в двух поляризационных каналах с круговой поляризацией

Колебание на выходе антенны в случае сильной эллипсидности поляризации (рис. 13), хотя и происходит в условиях действия тех же эфирных шумов, парадоксальным образом выглядит лучше, чем при круговой поляризации и отсутствии переходных помех.

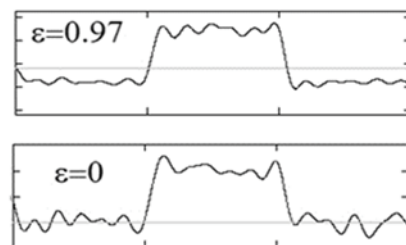


Рис. 13. Колебания на выходе демодулятора при эллиптической и круговой поляризациях

Если взглянуть на спектр выходного колебания антенны (рис. 14), то напрашивается объяснение, что энергия волн переходит не только на суммарные и разностные, но теперь и на комбинационные частоты, не попадающие в полосу пропускания канальных фильтров. Появление большого числа частотных переходов создает условия для проявления параметрических преобразований, подобных описываемым уравнениями Мэнли-Роу, поскольку в информационном и гамма-каналах помехи сильно коррелированы (одно и то же неполяризованное колебание).

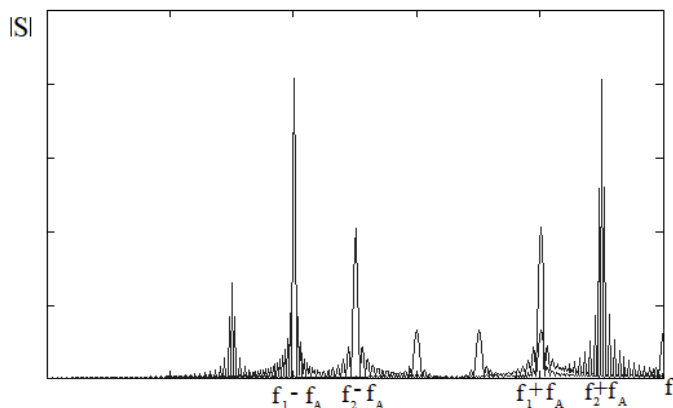


Рис. 14. Спектр колебания на выходе антенны при эксцентриситете эллипса поляризации волны 0.97

Колебание, в котором информационная часть заключается в правосторонней круговой составляющей поляризации волны, а ключ в виде гамма-последовательности в левосторонней составляющей, на приемнике-анализаторе спектра выглядит как простое одноканальное двухчастотное колебание (ЧТ) и в этом аспекте обеспечивает определенную скрытность (рис. 15).

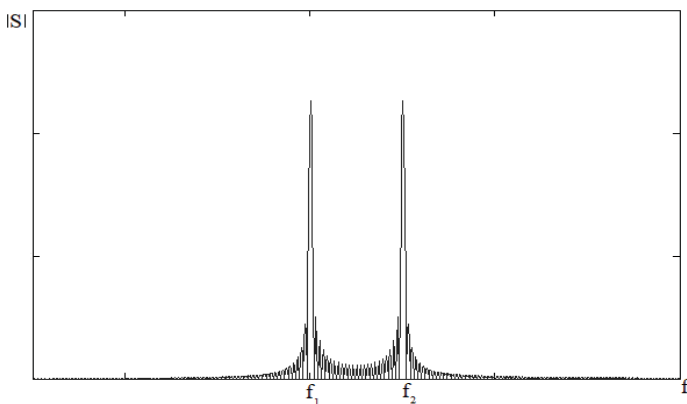


Рис. 15. Спектр колебания ЧМ с двумя поляризационными составляющими

Заключение

Прием волн с круговой поляризацией на вращающуюся антенну позволяет осуществить эффективное частотное разделение двух колебаний с противоположными направлениями вращения электрического вектора.

Помехоустойчивость каналов передачи информации с противоположными направлениями вращения электрических векторов по крайней мере не хуже, чем при частотной разделении.

Использование одного из круговых поляризационных каналов для передачи информационного кодированного сообщения, а второго канала для передачи ключевой гамма-последовательности, позволяет осуществлять устойчивый обмен защищенной информацией при простом способе кодирования.

Существенным является то обстоятельство, что осуществить разделение информационного и ключевого сообщений возможно лишь при наличии приемной антенны с управляемой поляризационной характеристикой. Улучшение формы колебания на выходе демодулятора при эллиптической поляризации волны упрощает алгоритм его работы.

Литература

1. Томаси У. Электронные системы связи. Litres, 2022.
2. Гульельми А.В., Потапов А.С. Частотно-модулированные ультранизкочастотные волны в околоземном космическом пространстве // Успехи физических наук. 2021. Т. 191. №5. С. 475-491.
3. Елисеев Б.П. и др. Радиолокация. Распространение радиоволн. Аэрорадионавигация. М.: Дашков и К, 2022. 196 с. ISBN 978-5-394-04693-3. URL: <https://www.iprbookshop.ru/120752.html>
4. Аджемов С.С., Репинский В.Н. Прием обыкновенной и необыкновенной волн антенной решеткой с управляемой поляризационной характеристикой. М: Радиотехника и электроника, 2019. Т. 64. №5. С. 455-461.
5. Adzhemov S.S., Repinsky V.N. Selection of a splitted ionospheric wave using the rotation of polarization of the receiving antenna // T-Comm: Телекоммуникации и транспорт, 2018. Т. 12. № 1. С. 4-8.
6. Буняк Г.А., Дмитриева В.В. Исследование антенн с круговой поляризацией // Актуальные проблемы инфотелекоммуникаций в науке и образовании (АПИНО 2022). Сборник научных трудов XI Международной научно-технической и научно-методической конференции. В 4-х томах, Санкт-Петербург, 15-16 февраля 2022 года / Под. редакцией А.В. Шестакова, сост. В.С. Елагин, Е.А. Аникевич. Том 3. Санкт-Петербург: Санкт-Петербургский государственный университет телекоммуникаций им. проф. М.А. Бонч-Бруевича, 2022. С. 61-65. EDN YTSOPS.
7. Adzhemov S.S., Repinsky V.N. Increasing the efficiency of separation of single-frequency signals with elliptic polarization by using a phased antenna array control // Scientific aspect, 2018, Vol. 7. No. 4, pp. 763-770.
8. Huang Y. Antennas: from theory to practice. John Wiley & Sons, 2021.
9. Adzhemov S.S., Belov N.V., Repinsky V.N., Shmelev I.A. Intelligent Location of a Multi-beam Ionospheric Wave by Isolating the Polarization Characteristics of Partial Channels // 2020 International Conference on Engineering Management of Communication and Technology (EMCTECH), Vienna, Austria, 2020, pp. 1-7, doi: 10.1109/EMCTECH49634.2020.9261552.
10. Поворознюк М.В., Бондарь С.В. Использование эффекта Доплера в науке и технике // Естественные и математические науки в современном мире. Сборник материалов студенческой конференции на базе Республиканского РУМО. Сост. Л.А. Полякова, А.И. Бакарюка, Н.С. Сидаш. ГПОУ «ХТТ ДОННТУ», 2022. С. 112.
11. Repinsky V.N., Belov N.V. Minimization of Transient Distortions in the Ionospheric Wave Reception System by a Phased Array Antenna with Controlled Polarization Characteristic // 2022 Systems of Signals Generating and Processing in the Field of on Board Communications, SOSG 2022 - Conference Proceedings, Moscow, 2022. DOI 10.1109/IEEECONF53456.2022.9744269. EDN SKAKBU.



12. Kryukovsky A.S., Lukin D.S., Rastyagaev D.V., Bova Y.I. The method of mathematical modeling of wave fields and caustic structures in the process of propagation of electromagnetic radiation in the ionospheric plasma // 2021 XXXIVth General Assembly and Scientific Symposium of the International Union of Radio Science (URSI GASS), 2021. Rome, 28 August – 4 September Publisher: IEEE, pp. 1-4.

13. Иценко Е.А., Пастернак Ю.Г., Пендюрин В.А., Федоров С.М. Применение технологии виртуальных антенных решеток для минимизации погрешности пеленгации Антенны и распространение радиоволн // Сб. докладов Всероссийской научно-технической конференции. СПб.: СПбГЭТУ «ЛЭТИ». 2021. 120 с.

14. Бурьков Д.В. Mathcad, Matlab, Matlab Simulink, Scilab в электротехнике: учебное пособие. Ростов-на-Дону, Таганрог: Издательство Южного федерального университета, 2021. 171 с. ISBN 978-5-9275-3961-1. URL: <https://www.iprbookshop.ru/121901.html>

15. Ivanov D.V., Ivanov V.A., Ryabova N.V., Elsukov A.A., Ryabova M.I., Chernov A.A. Software-defined radio technology in the problem concerning with the successive sounding of HF ionospheric communication channels // Journal of Communications Technology and Electronics. 2016. 7(61), pp. 767-775.

16. Контев Д. Теория радиотехнических сигналов. Litres, 2023.

17. Аджемов С.С., Репинский В.Н. Повышение эффективности разделения одночастотных сигналов с эллиптической поляризацией с помощью управления фазированной антенной решеткой. Научный аспект. 2018. Т. 7. № 4. С. 763-770.

18. Корнеев П.Е. Обработка эллиптически поляризованного сигнала в радиолокационных станциях с цифровым синтезированием апертуры антенны // Научный вестник Московского государственного технического университета гражданской авиации. Т. 22, № 1, 2019. С. 83-92.

SIMULTANEOUS TRANSMISSION OF A SECURED MESSAGE AND A GAMMA KEY TO IT IN ONE FREQUENCY CHANNEL WITH RECEPTION ON AN ANTENNA ARRAY WITH CONTROLLED POLARIZATION CHARACTERISTICS

NIKITA V. BELOV

Moscow, Russia, n.v.belov@mtuci.ru

VLADIMIR N. REPINSKY

Moscow, Russia, repinski@rambler.ru

KEYWORDS: *Circular polarization, controlled polarization response, transient distortion, spectral density, gamma sequence.*

ABSTRACT

Introduction: The results of analysis and simulation of the reception of two independent sequences transmitted at the same frequency, but with opposite elliptical polarizations, are presented.

Methods: when the antenna rotates, including electrically, by alternately switching dipoles, in the simplest case, two perpendicular half-wave vibrators, the spectrum of a wave with circular polarization, coinciding in direction with the rotation of the antenna, shifts upward in frequency, and waves in the opposite direction of rotation of the electric vector, respectively, downward. Rotation is possible for antennas of various types, both traditional and magnetic, which are mutually perpendicular coils. The only principle here is the rotation of the polarization vector, which provides better channel separation than perpendicular linear polarizations. **Results:** It is shown that the

selection of these shifted spectra is possible using frequency filtering after conversion in a controlled antenna array. Transient interference between orthogonal polarization channels is analyzed and it is shown that the maximum level of transient interference power does not exceed 15% of the total signal level near the receiving antenna, and in the case of a small ellipse of the vector E trajectory it ranges from fractions to a few percent. As a result, the appearance of transient interference due to the difference in wave polarization from circular polarization has practically no effect on the detection process, that is, the method of single-frequency transmission of an encoded message and key described here is relevant. Due to the fact that detection of orthogonal polarization components requires a technical solution that is not related to the orientation of the antenna, it is concluded that the message transmitted in an operational environment is sufficiently secure.

REFERENCES

1. U. Tomasi, "Electronic communication systems," *Litres*, 2022.
2. A.V. Guglielmi, A.S. Potapov, "Frequency-modulated ultra-low-frequency waves in near-Earth space," *Advances in Physical Sciences*. 2021. Vol. 191. No. 5, pp. 475-491.
3. B.P. Eliseev et al. Radar. Propagation of radio waves. Aeroradionavigation. Moscow: Dashkov and K, 2022. 196 p. ISBN 978-5-394-04693-3. URL: <https://www.iprbookshop.ru/120752.html>
4. S.S. Adzhemov, V.N. Repinsky, "Reception of ordinary and extraordinary waves by an antenna array with a controlled polarization characteristic," Moscow: Radio engineering and electronics, 2019. Vol. 64. No. 5, pp. 455-461.
5. S.S. Adzhemov, V.N. Repinsky, "Selection of a splitted ionospheric wave using the rotation of polarization of the receiving antenna," *T-Comm*, 2018, Vol. 12.No. 1, pp. 4-8.
6. G.A. Bunyak, V.V. Dmitrieva, "Research on antennas with circular polarization," *Current problems of information telecommunications in science and education (APINO 2022): Collection of scientific papers of the XI International Scientific-Technical and Scientific-methodological conference*. In 4 volumes, St. Petersburg, February 15-16, 2022. Under. edited by A.V. Shestakova, comp. V.S. Elagin, E.A. Anikevich. Volume 3. St. Petersburg: St. Petersburg State University of Telecommunications. prof. M.A. Bonch-Bruevich, 2022, pp. 61-65.
7. S.S. Adzhemov, V.N. Repinsky, "Increasing the efficiency of separation of single-frequency signals with elliptic polarization by using a phased antenna array control," *Scientific aspect*, 2018, Vol. 7.No. 4, pp. 763-770.
8. Y. Huang, "Antennas: from theory to practice," John Wiley & Sons, 2021.
9. S.S. Adjemov, N.V. Belov, V.N. Repinsky and I.A. Shmelev, "Intelligent Location of a Multi-beam Ionospheric Wave by Isolating the Polarization Characteristics of Partial Channels," *2020 International Conference on Engineering Management of Communication and Technology (EMCTECH)*, Vienna, Austria, 2020, pp. 1-7, doi: 10.1109/EMCTECH49634.2020.9261552.
10. M.V. Povoroznyuk, S.V. Bondar, "Use of the Doppler effect in science and technology," *Natural and mathematical sciences in the modern world. Collection of materials from the student conference on the basis of the Republican Department of Education and Science*. Comp. L.A. Polyakova, A.I. Bakaryuk, N.S. Sidash - GPOU "HTT DON-NTU", 2022, p. 112.
11. V.N. Repinsky, N.V. Belov, "Minimization of Transient Distortions in the Ionospheric Wave Reception System by a Phased Array Antenna with Controlled Polarization Characteristic," *2022 Systems of Signals Generating and Processing in the Field of on Board Communications, SOSG 2022 - Conference Proceedings*, Moscow, March 15-17, 2022. Moscow, 2022. DOI 10.1109/IEEECONF53456.2022.9744269.
12. A.S. Kryukovsky, D.S. Lukin, D.V. Rastyagaev, Y.I. Bova, "The method of mathematical modeling of wave fields and caustic structures in the process of propagation of electromagnetic radiation in the ionospheric plasma," *2021 XXXIVth General Assembly and Scientific Symposium of the International Union of Radio Science (URSI GASS)*, 2021. Rome, 28 August – 4 September Publisher: IEEE, pp. 1-4.
13. E.A. Ishchenko, Yu.G. Pasternak, V.A. Pendyurin, S.M. Fedorov, "Application of virtual antenna array technology to minimize direction finding error Antennas and radio wave propagation," *Collection. reports of the All-Russian Scientific and Technical Conference*. SPb.: SPbSETU "LETI". 2021. 120 p.
14. D.V. Burkov, "Mathcad, Matlab, Matlab Simulink, Scilab in electrical engineering," Rostov-on-Don, Taganrog: Southern Federal University Publishing House, 2021. 171 p. ISBN 978-5-9275-3961-1. URL: <https://www.iprbookshop.ru/121901.html>
15. D.V. Ivanov, V.A. Ivanov, N.V. Ryabova, A.A. Elsukov, M.I. Ryabova, A.A. Chernov, "Software-defined radio technology in the problem concerning with the successive sounding of HF ionospheric communication channels," *Journal of Communications Technology and Electronics*. 2016. 7(61), pp. 767-775.
16. D. Koptev, "Theory of radio signals," *Litres*, 2023.
17. S.S. Adzhemov, V.N. Repinsky, "Improving the separation efficiency of single-frequency signals with elliptical polarization using phased array antenna control," *Scientific aspect*. 2018. Vol. 7. No. 4, pp. 763-770.
18. Pavel E. Korneev, "Processing of an elliptically polarized signal in radar stations with digital synthesis of the antenna aperture," *Scientific Bulletin of the Moscow State Technical University of Civil Aviation*, vol. 22, no. 1, 2019, pp. 83-92.

INFORMATION ABOUT AUTHORS:

Nikita V. Belov, Senior Lecturer, Department of ISUIA MTUCI, Moscow, Russia

Vladimir N. Repinsky, Associate Professor at the Department of ISUIA MTUCI, Moscow, Russia

For citation: Belov N.V., Repinsky V.N. Simultaneous transmission of a secured message and a gamma key to it in one frequency channel with reception on an antenna array with controlled polarization characteristics. *H&ES Reserch*. 2024. Vol. 16. No 3. P. 46-54. doi: 10.36724/2409-5419-2024-16-3-46-54 (In Rus)



ПРИМЕНЕНИЕ ТЕХНОЛОГИИ MIMO ДЛЯ УЛУЧШЕНИЯ ХАРАКТЕРИСТИК ФИЗИЧЕСКОГО УРОВНЯ БЕСПРОВОДНЫХ СЕТЕЙ WI-FI

ПАНКРАТОВ

Денис Юрьевич¹

ПАХОМОВА

Александра Валерьевна²

АННОТАЦИЯ

Введение: Развитие компьютерной техники дало резкий скачок в появлении новых технологий практически во всех областях жизни людей. Это не обошло стороной системы связи, в том числе и беспроводные. Для передачи данных с каждым годом нарастает потребность в увеличении емкости системы и пропускной способности систем связи при заданном качестве. Добиться увеличения скорости передачи возможно применяя все более многопозиционные квадратурные виды модуляции, расширением частотного спектра за счет более высоких несущих частот, и также поддержкой сравнительно новой технологии MIMO (Multiple-Input-Multiple-Output). В представленной работе показано, что применение различных конфигураций MIMO в системах беспроводной связи WiFi обеспечивает значительное увеличение скорости передачи данных. На пропускную способность влияет конфигурация MIMO - с увеличением числа антенн на передающей и приемной стороне пропускная способность увеличивается. Цель работы: Целью работы является анализ таких характеристик физического уровня систем WiFi, как помехоустойчивость и пропускная способность, в зависимости от количества антенн, используемых в технологии MIMO, а также от используемой ширины полосы частот. **Методы:** Для анализа физического уровня систем WiFi были использованы методы статистического имитационного моделирования в графической среде MATLAB. **Результаты:** В результате компьютерного моделирования были получены зависимости пропускной способности, а также зависимости вероятности ошибки от отношения сигнал/шум при различной конфигурации MIMO для систем Wi-Fi. Результаты показали, что с увеличением числа антенн вероятность ошибки уменьшается при одинаковом отношении сигнал/шум, а пропускная способность существенно возрастает. **Практическая значимость:** Исследование показало, что в разработках новых беспроводных систем связи, таких как Wi-Fi, весьма перспективным является применение технологии MIMO с большим количеством антенн, позволяющей обеспечить одновременную передачу большого числа пространственных потоков данных абонентам.

Сведения об авторах:

¹ МТУСИ, к.т.н. доцент каф. СиСРТ,
Москва, Россия, dpankr@mail.ru

² МТУСИ, Москва, Россия,
aleks.pahomova@yandex.ru

КЛЮЧЕВЫЕ СЛОВА: MIMO, Wi-Fi, беспроводные сети связи,
моделирование физического уровня, пропускная способность, BER.

Для цитирования: Панкратов Д.Ю., Пахомова А.В. Применение технологии MIMO для улучшения характеристик физического уровня беспроводных сетей Wi-Fi // Научные исследования в космических исследованиях Земли. 2024. Т. 16. № 3. С. 55-61. doi: 10.36724/2409-5419-2024-16-3-55-61

Введение

В последних стандартах систем беспроводной связи (WiFi) применяется технология MIMO. Это стандарты IEEE 802.11n (Wi-Fi 4), 802.11ac (Wi-Fi 5), 802.11ax (Wi-Fi 6), 802.11be (Wi-Fi 7) [1-4].

Технология MIMO с N передающими и N приемными антеннами теоретически способна увеличить максимальную пропускную способность в N раз. По сравнению с традиционными системами связи, имеющими по одной антенне, как на передаче, так и на приеме. Это происходит потому, что одновременно с каждой передающей антенны передается свой символ, то есть N символов передается в один момент времени и на одной несущей частоте [2].

Беспроводные сети, использующие технологию Wi-Fi с каждым годом, находят более широкое применение [3]. Эта технология применяется в беспроводных локальных сетях (WLAN), быстро распространяющихся в последнее время, поскольку в них не требуется проводных линий связи, то есть абонент может передвигаться в зоне действия сети. За это преимущество приходится платить меньшей скоростью передачи, чем в проводных линиях связи, меньшим расстоянием, на которое возможна передача данных [3, 4].

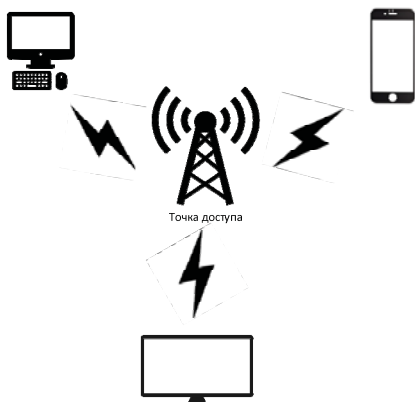


Рис. 1. Структурная системы Wi-Fi

Структурная схема системы Wi-Fi показана на рисунке 1 [4]. В рассматриваемой конфигурации система Wi-Fi включает точку доступа и множество клиентских станций. В типичной конфигурации Wi-Fi, приложения включают доступ в Интернет и потоковое аудио и видео. Кроме того, пользовательский опыт работы с такими приложениями, как внутри-сетевое взаимодействие для локальной передачи файлов, резервное копирование и печать улучшаются за счет более высоких скоростей передачи данных [5].

С развитием технологии Wi-Fi различие в пропускной способности по сравнению с проводными сетями уменьшается. Это привело к тому, что стало возможным объединение сетей Wi-Fi с проводными линиями связи и с сетью Интернет [6].

Технология MIMO

Для расчёта пропускной способности беспроводного канала связи для системы с одной передающей и одной приемной антенны, используется формула Шеннона [5]:

$$C = \Delta F \log_2 \left(1 + \frac{P_s}{2\sigma_\eta^2} \right), \text{ бит/с}, \quad (1)$$

где ΔF – ширина канала связи, Гц; P_s – мощность сигнала; $2\sigma_\eta^2$ – мощность шума. Из формулы (1) видно, что пропускную способность можно увеличить за счет увеличения полосы частот канала связи, увеличения мощности сигнала или уменьшения мощности помех [5].

Увеличение полосы частот затруднительно, так как радиочастотный спектр является ограниченным природным ресурсом. При увеличении мощности сигнала требуются более мощные передатчики, что приводит к их усложнению из-за соблюдения требований электромагнитной совместимости, что в свою очередь приводит к удорожанию системы связи. Уменьшение мощности помех возможно только в некоторых случаях (например, применение маломощных усилителей). Кроме того, согласно формуле (1), пропускная способность с улучшением этих параметров растет по логарифмическому закону. Таким образом, для систем с одной антенной как на передаче, так и на приеме повышение пропускной способности весьма ограничено [6].

Выход из создавшегося положения возможен, применяя системы со многими передающими и многими приемными антеннами (MIMO). Принцип работы системы связи, использующей технологию MIMO показан на рисунке 1.

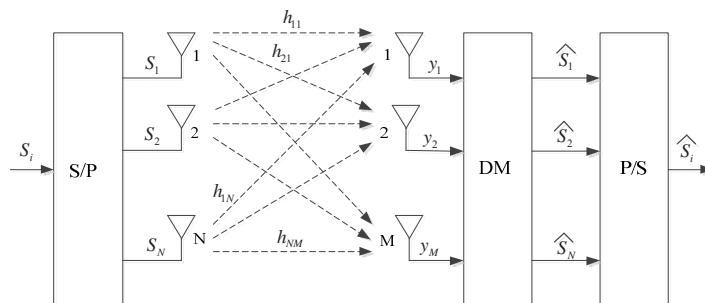


Рис. 2. Принцип работы системы радиосвязи с технологией MIMO: S/P – последовательно-параллельный преобразователь; DM – демодулятор; P/S – параллельно-последовательный преобразователь

Система связи, изображенная на рисунке 2, работает следующим образом [6]. В блоке S/P входная последовательность преобразовывается в N параллельных последовательностей, где N равно количеству передающих антенн. Одновременно все символы блока излучаются с помощью соответствующей антенны, при этом длительность каждого излучаемого символа в N раз длиннее, чем символа на входе преобразователя S/P.

Таким образом, N символов передаются в полосе частот в N раз меньшей, чем исходная последовательность символов, и тем самым система MIMO обеспечивает большую спектральную эффективность.

В системе радиосвязи, использующей технологию MIMO, математическая модель принимаемого сигнала выражается следующей формулой [6]:

$$\mathbf{Y} = \mathbf{H}\mathbf{s} + \boldsymbol{\eta}, \quad (2)$$

где \mathbf{Y} – вектор-столбец принимаемых сигналов размерности $M \times 1$; \mathbf{H} – матрица канала связи, размерности $M \times N$; $\boldsymbol{\eta}$ – случайный гауссовский вектор размерности $M \times 1$; \mathbf{s} – вектор-столбец информационных символов;

Согласно формуле (2), принимаемый сигнал в системе с несколькими передающими и приемными антеннами (MIMO), описывается системой линейных уравнений. Пропускная способность системы радиосвязи с технологией MIMO, описывается следующей формулой [5]:

$$C = \Delta F \log_2 \det \left(\mathbf{I} + \frac{P_s}{N \cdot 2\sigma_\eta^2} \mathbf{H}\mathbf{H}' \right), \text{ бит/с} \quad (3)$$

где ΔF – ширина канала связи, Гц; P_s – мощность сигнала; $2\sigma_\eta^2$ – мощность шума; \mathbf{I} – единичная матрица; \mathbf{H} – матрица канала связи MIMO; \mathbf{H}' – эрмитово-сопряженная матрица канала связи MIMO; N – количество передающих антенн.

Когда число передающих и приемных антенн совпадают и матрица \mathbf{H} ортогональная, достигается максимальная пропускная способность канала связи системы MIMO. Условие ортогональности матрицы канала \mathbf{H} :

$$\mathbf{H}\mathbf{H}' = |\lambda|^2 \mathbf{1} = M \cdot \mathbf{1} \quad (4)$$

где M – количество приемных антенн; λ – собственные числа матрицы канала связи \mathbf{H} . При этом выражение для канала радиосвязи с MIMO принимает следующий вид:

$$C = M \cdot \Delta F \log_2 \det \left(\mathbf{I} + \frac{P_s}{2\sigma_\eta^2} \right), \text{ бит/с} \quad (5)$$

где $M = N$ – количество приемных и передающих антенн.

Из формулы (5) видно, что в вышеприведенном частном случае пропускная способность канала MIMO растет прямо пропорционально количеству антенн. Следовательно, есть потенциальные возможности увеличения пропускной способности беспроводных систем связи, применяющих технологию MIMO [7].

Обзор стандартов WiFi

После появления первого стандарта Wi-Fi очевидным стало то, что максимальная скорость передачи данных в 2 Мбит/с недостаточна для замены проводной сети Ethernet со скоростью 100 Мбит/с. Вот почему довольно скоро сообщество разработчиков Wi-Fi предложило палитру дополнительных стандартов, а именно 802.11a/b/g, которые позволили увеличить скорость передачи до 54 Мбит/с за счет использования новых технологий физического уровня: новых схем модуляции и кодирования, а также новых частотных диапазонов и каналов. В стандарте 802.11a появилась технология мультиплексирования OFDM (Orthogonal Frequency Division Multiplexing) с каналами шириной 20 МГц, что заложило основу для следующих поколений Wi-Fi [8].

По мере развития стандартов IEEE 802.11, начиная с версии IEEE 802.11n (WiFi 4) применяется технология MIMO. Благодаря использованию нескольких антенн возможна одновременная передача до четырех пространственных потоков. Это добавление наряду с расширением ширины частотных каналов и новых видов модуляции приводит к существенному увеличению пропускной способности. Далее кратко рассмотрим системы Wi-Fi различных стандартов, использующих технологию MIMO [8].

Первым стандартом, в котором для повышения пропускной способности системы связи предусмотрено применение технологии MIMO является стандарт IEEE 802.11n. Стандарт 802.11n поддерживает четыре антенны и технологию физического уровня OFDM с 64 поднесущими. На каждой поднесущей могут использоваться модуляции BPSK (Binary Phase-Shift Keying), QPSK (Quadrature Phase-Shift Keying), 16-QAM (Quadrature Amplitude Modulation) и 64-QAM. Возможны четыре скорости помехоустойчивого кодирования 1/2, 2/3, 3/4, 5/6. Теоретически максимальная скорость передачи достигает 600 Мбит/с при применении четырех антенн, модуляции 64-QAM и скорости кодирования 5/6 [9].

Устройства, поддерживающие стандарт 802.11n могут работать как в канале шириной 20 МГц, так и в расширенном канале шириной 40 МГц [9, 10].

Теоретическую скорость в реальных условиях достичь невозможно. На уменьшение пропускной способности влияют: число абонентов, одновременно работающих в одном канале связи, помехи, создаваемые близкорасположенными к точке доступа радиотелефонами, устройствами Bluetooth, микроволновыми печами и другими высокочастотными устройствами, создающими дополнительные помехи [8].

Для поддержки новых возможностей физического уровня появились новые функции уровня MAC (Media Access Control, управление доступом к среде), к наиболее существенным из которых следует отнести технологии агрегации блоков данных для сокращения накладных расходов на передачу заголовков [9].

Следующим стандартом, использующим технологию MIMO, является 802.11ac (IEEE Std. 802.11ac), в нем расширяются возможности MIMO до 8 пространственных потоков вместо 4 как в предыдущей версии [9, 10]. Добавлен новый вид модуляции 256-QAM, то есть один символ передает 8 бит данных. Для реализации модуляции 256-QAM необходим более мощный сигнал на передающей стороне, для того чтобы на приеме отношение сигнал/шум было не менее 30 дБ. Так же, как и в стандарте 802.11n, поддерживается четыре скорости кодирования. Ширина полосы частот каналов может быть 20 МГц и 40 МГц как в стандарте 802.11n, а также введены новые каналы 80 МГц и 160 МГц. Это стало возможным за счет использования нового частотного диапазона 5 ГГц. При использовании полосы частот 160 МГц, модуляции 256-QAM, скорости кодирования 5/6 теоретически скорость передачи приблизительно может достигать 7 Гбит/с [9].

Существенным преимуществом стандарта 802.11ac является возможность применения технологии формирования диаграммы направленности Beamforming, которая позволяет сконцентрировать передачу в нужном направлении и дает возможность обеспечения большей скорости.

В данной технологии существуют режимы: однопользовательский и многопользовательский, которые применяются на нисходящей линии (Downlink) [10].

Если применяется режим SU-MIMO (однопользовательский режим), то диаграммы направленности всех антенн направлены на одну абонентскую станцию. При применении режима MU-MIMO (многопользовательский режим) диаграммы направленности антенн не пересекаются и отсюда следует, что прием производится различными абонентскими станциями.

Изменения в стандарте IEEE 802.11ac, по сравнению со стандартом 802.11n, позволили увеличить пропускную способность, емкость системы WiFi, а также при применении технологии направленной передачи работать в энергетически более экономичном режиме. Чтобы уменьшить накладные расходы, связанные с заголовками при таких высоких скоростях передачи данных, добавляется возможность увеличения длины агрегированного кадра.

Следующим стандартом на пути развития Wi-Fi является стандарт 802.11ax (IEEE Std. 802.11ax-2021). Возможное количество антенн в технологии MIMO составляет 8. При этом как на нисходящей линии (DL), так и на восходящей линии (UL) используется множественный доступ с ортогональным частотным разделением (OFDMA). Используются типы модуляции BPSK, QPSK, 16-QAM, 64-QAM, 256-QAM и 1024-QAM. Используются следующие скорости кодирования: 1/2, 2/3, 3/4 и 5/6. Максимальная теоретическая скорость передачи данных составляет более 8 Гбит/с. Применяются каналы шириной 20, 40, 80 и 160 МГц, а также канал 20 МГц для Интернета вещей (IoT). Станции рассматриваемого стандарта работают в частотных диапазонах 2,4 ГГц и 5 ГГц, также возможно использование новых диапазонов (от 1 до 7 ГГц) [11].

Резюмируя отмеченное выше, ряд новых возможностей и преимуществ технологии 802.11ax следующие:

1. Технология OFDMA используется как в восходящих каналах, так и в нисходящих каналах;
2. Режим MU-MIMO используется как в восходящих каналах, так и в нисходящих каналах;
3. Модуляция 1024-QAM;
4. Увеличена длина символа OFDM, в 4 раза больше поднесущих;
5. Снижено энергопотребление;
6. Технология формирования лучей диаграммы направленности Beamforming (которая также уже используется в 802.11ac) с расширенными возможностями, перераспределение пространственных потоков.

Последнее поколение Wi-Fi – проект 802.11be – включает в себя очень амбициозные цели, связанные с более высокими скоростями передачи данных, более высокой эффективностью использования спектра, снижением влияния помех и обеспечением поддержки приложений реального времени (RTA). Применение технологии RTA требуют гарантированно низкой задержки и высокой надежности [10, 11].

Основными нововведениями Wi-Fi7 являются следующие:

- 1) Применение на физическом уровне технологии экстремально высокой пропускной способности (EHT). В системе Wi-Fi 7 предусмотрено удвоения как используемой полосы частот, так и количества антенн в режиме MU-MIMO, что

увеличивает пропускную способность в 4 раза. За счет использования модуляции 4096-QAM, добавляется еще 20% к пропускной способности. Таким образом, Wi-Fi 7 обеспечит номинальную скорость передачи данных более чем в 4 раза выше по сравнению с Wi-Fi 6. Оценивается, что теоретически максимальная скорость передачи данных в системе Wi-Fi 7 составит 46 Гбит/с [14]. Кроме того, ожидается существенное изменение в уровне MAC, которое связано с обобщением заголовков кадров и разработкой формата кадров, совместимого с прямой передачей.

- 2) Усовершенствованный доступ OFDMA.

Технология OFDMA, применяемая в предыдущих версиях WiFi, позволяет весьма эффективно распределять ресурсы системы WiFi, однако эта технология не очень гибкая, что приводит к снижению производительности и увеличению задержки. Усовершенствованная в Wi-Fi 7 технология OFDMA позволяет более гибко использовать ресурсы [11].

- 3) Работа по нескольким каналам связи.

Одним из одобренных изменений Wi-Fi 7 является поддержка работы по нескольким каналам связи, которая обеспечивает как высокую скорость передачи данных, так и чрезвычайно низкую задержку. Хотя современные чипсеты в настоящее время могут использовать несколько каналов связи одновременно, эти каналы независимы, что ограничивает эффективность такой работы.

Разработчики стандарта 802.11be (Status of Project IEEE P802.11be, https://ieee802.org/11/Reports/tgbe_update.htm) стремятся найти такой уровень синхронизации между каналами, который позволит более эффективно использовать ресурсы и минимизировать помехи при плотном развертывании систем WiFi [12].

- 4) Усовершенствованные технологии физического уровня, повышающие эффективность использования спектра.

Применение технологии неортогонального множественного доступа (NOMA) обеспечит значительное повышение эффективности использования спектра в случае повторных попыток передачи и одновременных передач в одном и том же или противоположных направлениях с

- 5) Совместная передача с помощью нескольких точек доступа.

Еще одним важным нововведением в стандарте 802.11be является использование нескольких точек доступа для совместной передачи абонентским станциям с целью повышения надежности и скорости передачи данных определенным абонентам [13, 14].

По результатам рассмотренных поколений систем WiFi в таблице 1 представлены основные характеристики физического уровня стандартов IEEE 802.11. В таблицу 1 также добавлен стандарт 802.11a в котором не используется технология MIMO, для сравнения характеристик. Видно, что с каждым внедрением нового стандарта повышается пропускная способность канала и скорость передачи системы WiFi. Это достигается внедрением новых технологий, которые позволяют увеличить полосу частот, внедрить многопозиционные виды квадратурной модуляции, внедрить технологию MIMO с большим числом антенн [8-11].



Таблица 1

Сравнение стандартов IEEE 802.11

Стандарты	Модуляция	Диапазон, ГГц	Скорость кодирования	Количество антенн	Ширина канала, МГц	Скорость
802.11a	BPSK QPSK 16-QAM	5 и 8	1/2, 2/3, 3/4, 5/6	1	20	1,5 Мбит/с – 54 Мбит/с
802.11n	Доп. - 64-QAM	2.4 и 5	1/2, 2/3, 3/4, 5/6	4	20 40	150 Мбит/с – 600 Мбит/с
802.11ac	Доп. - 256-QAM	5	1/2, 2/3, 3/4, 5/6	8	20 40 80	433 Мбит/с – 6933 Мбит/с
802.11ax	Доп. - 1024-QAM	2.4 и 5	1/2, 2/3, 3/4, 5/6	8	20 40 80 160	600 Мбит/с – 9608 Мбит/с
802.11be	Доп. - 4096-QAM	2.4; 5 и 6	1/2, 2/3, 3/4, 5/6	16	20 40 80 160 320	До 46 Гбит/с

Результаты моделирования системы беспроводной связи с технологией MIMO

Для анализа характеристик физического уровня систем WiFi в настоящей работе было проведено статистическое компьютерное моделирование для анализа пропускной способности каналов беспроводной связи WiFi. Моделирование проводилось в графической среде MATLAB [14] с применением технологии MIMO с различным числом антенн. В моделях с различной конфигурацией MIMO остальные условия были равнозначны, в частности, при анализе помехоустойчивости использовался релейский канал связи, применялся алгоритм демодуляции, оптимальный по критерию максимального правдоподобия. Также возможно применение других алгоритмов демодуляции, например, итерационных [15, 16].

Демодулятор, оптимальный по критерию максимального правдоподобия (ML), является наиболее эффективным алгоритмом демодуляции, в нем оценка информационных символов $\hat{\mathbf{S}}$ модели (2) находится по формуле

$$\hat{\mathbf{S}}_{ML} = \arg \min_{\theta \in S^N} \{(\mathbf{Y} - \mathbf{H}\mathbf{s})'(\mathbf{Y} - \mathbf{H}\mathbf{s})\}, \quad (6)$$

где $\hat{\mathbf{S}}_{ML}$ – вектор оценок принятого сигнала; \mathbf{Y} – вектор принятого сигнала; \mathbf{H} – матрица канала MIMO; \mathbf{s} – вектор возможной комбинации принятого сигнала, S^N – множество перебираемых комбинаций.

Для нахождения вектора оценок $\hat{\mathbf{S}}$, нужно осуществить перебор всех возможных комбинаций информационных символов в результате цифровой обработки принятого сигнала. Сложность такой обработки зависит от числа антенн N кратности модуляции QAM.

Результаты анализа пропускной способности канала MIMO приведены в графическом виде на рисунке 3. На графике показаны зависимости пропускной способности от отношения сигнал/шум (SNR) в дБ. Моделирование проводилось для системы WiFi с одной антенной на передаче и

приеме с технологией SISO (Single-Input Single-Output) и системы WiFi со многими антеннами с технологиями MIMO с конфигурациями 2x2, 4x4, 8x8 и 12x12 [17, 18].

В таблице 2 представлены результаты оценки скорости передачи данных систем WiFi с разной конфигурацией MIMO для разной ширины канала.

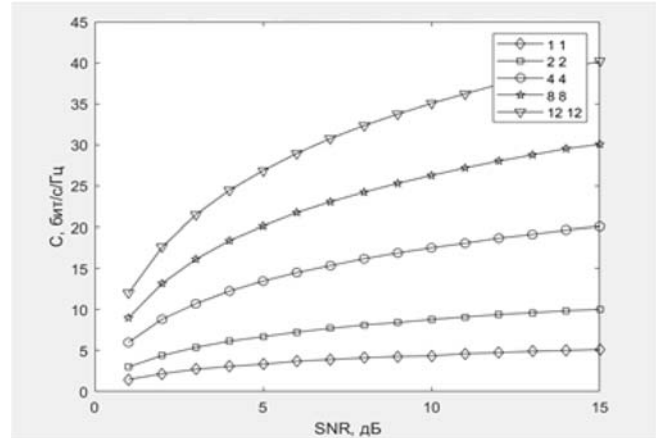


Рис. 3. Зависимость пропускной способности канала системы WiFi от отношения сигнал/шум (SNR) в дБ для различных конфигураций технологии MIMO

Таблица 2

Оценка максимальной скорости R передачи данных системы Wi-Fi с разной конфигурацией MIMO для разной ширины канала W

R Мбит/с	Конфигурация MIMO					
	1x1	2x2	4x4	8x8	12x12	
Ширина канала W, МГц	20	80	160	320	500	700
	80	320	640	1280	2000	2800
	160	640	1280	2560	4000	5600
	320	1280	2560	5120	8000	11200

Из таблицы 2 видно, что с увеличением количества антенн в технологии MIMO (при ОСШ = 9 дБ) скорость передачи увеличивается, причем при конфигурации 12x12 скорость передачи на порядок больше, чем при конфигурации 1x1. Увеличение числа антенн в совокупности с увеличением ширины полосы с 20 МГц до 320 МГц позволяет достигнуть увеличения скорости передачи до 11200 Мбит/с.

Перейдем к оценке помехоустойчивости системы WiFi при разных конфигурациях MIMO. Для моделирования системы MIMO будем использовать следующий алгоритм, по которому составлена программа и проведено моделирование в среде MATLAB для случая с использованием методов компьютерного моделирования систем радиосвязи [6, 19].

1. од исходных данных.
2. Циклы по отношению сигнал/шум (SNR) и по числу испытаний:
 - диапазон SNR от 0 дБ до 15 дБ с шагом 1 дБ;
 - число испытаний 10 000.
4. Формирование случайных битовых последовательностей и модуляция.
6. Формирование комплексной матрицы канала для различных конфигураций системы MIMO.

7. Формирование наблюдаемого вектора на входе демодулятора.
 8. Вычисление оценки вектора переданных символов с использованием алгоритма ML, отображение оценки вектора символов в биты.
 9. Завершение цикла по числу испытаний
 10. Вычисление коэффициента битовых ошибок (BER).
 11. Завершение цикла по SNR
 12. Вывод кривых помехоустойчивости $BER = f(SNR)$ в графической среде MATLAB для разного числа антенн.
- В результате моделирования по указанному алгоритму в среде MATLAB был получен график помехоустойчивости для системы WiFi с технологией MIMO с различной конфигурацией антенн (зависимости BER от параметра SNR в дБ).

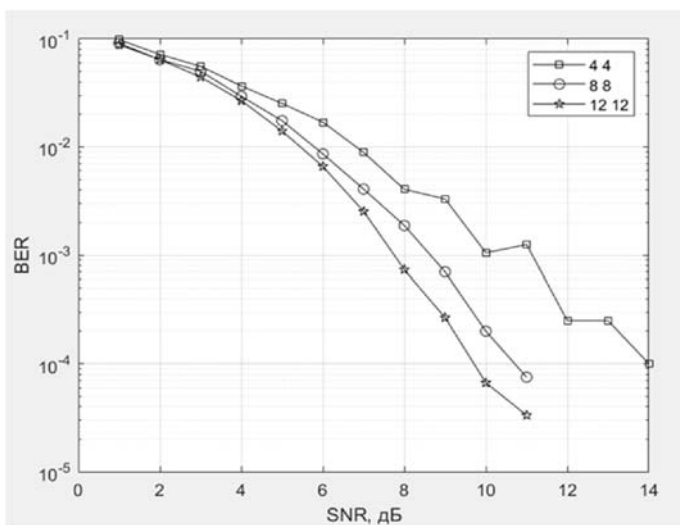


Рис. 4. Зависимость коэффициента ошибок (BER) от отношения сигнал/шум (SNR) в дБ для различных конфигураций технологии MIMO в системе WiFi

Из графика, показанного на рисунке 4, видно, что с увеличением числа антенн в технологии MIMO, при прочих равных условиях, вероятность ошибки уменьшается. Так по уровню $BER=10^{-4}$ для конфигурации MIMO 12x12 значение SNR=9,5 дБ, а для конфигурации MIMO 4x4 значение SNR=14 дБ, то есть выигрыш составляет 4,5 дБ. Очевидно, что данный выигрыш достигается за счет увеличения сложности обработки.

Заключение

Применение технологии MIMO в беспроводных сетях WiFi увеличивает их пропускную способность. При усложнении конфигурации, то есть при увеличении числа передающих и приемных антенн, скорость передачи значительно увеличивается, естественно при этом возрастает вычислительная сложность. Вычислительная сложность в основном связана со сложностью цифровой обработки сигналов на приемной стороне. Применяя алгоритм демодуляции, оптимальный по критерию максимального правдоподобия, вычислительная сложность возрастает по экспоненциальному закону с увеличением количества антенн. Отсюда следует, что применение этого метода демодуляции затруднительно для сетей

беспроводной связи с большим числом параллельно передаваемых потоков данных. Следует применять другие методы демодуляции, проигрывая в энергетической эффективности, для систем WiFi, в которых используется большое число антенн и высокая кратность модуляции.

Литература

1. Вишневецкий В.М., Ляхов А.И., Портной С.Л., Шахнович И.В. Широкополосные беспроводные сети передачи информации Москва: Техносфера, 2005. 592 с.
2. Korolev N., Levitsky I., Khorov E. Analytical Model of Multi-link Operation in Saturated Heterogeneous Wi-Fi 7 Networks. IEEE Wireless Communications Letters, 2022.
3. Evgeny Khorov, Andrey Lyakhov, Alexander Krotov, Andrey Guschin. A survey on IEEE 802.11ah: An enabling networking technology for smart cities // Computer Communications. 2015. №58. С. 53-69.
4. Gordon Jeffrey. Wi-Fi Technology: Wireless Networking. Amazon, 2022. 129 p.
5. Бакулин М.Г., Крейнделин В.Б. и др. Неортогональный множественный доступ (NOMA) как основа систем связи 5G и 6G. М.: Горячая Линия – Телеком, 2024. 264 с.
6. Бакулин М.Г., Крейнделин В.Б., Панкратов Д.Ю. Технологии в системах радиосвязи на пути к 5G. М.: Горячая линия – Телеком, 2021. 280 с.
7. Korolev G., Kureev A., Khorov E., Lyakhov A. Enabling Synchronous Uplink NOMA in Wi-Fi Networks // 2021 International Conference Engineering and Telecommunication (En&T), Dolgoprudny, Russian Federation, 2021, pp. 1-5.
8. Krasilov A., Lebedeva I., Yusupov R., Khorov E. Efficient Multiplexing of Downlink eMBB and URLLC Traffic with Massive MU-MIMO // 2022 IEEE International Black Sea Conference on Communications and Networking (BlackSeaCom), Sofia, Bulgaria, 2022, pp. 185-190.
9. Eldad Perahia, Robert Stacey. Next Generation Wireless LAN's 802.11n and 802.11ac. Cambridge University Press, 2015. 478 p.
10. Gordon Colbach. The WiFi Networking Book: WLAN Standards: IEEE 802.11 bgn, 802.11n, 802.11ac and 802.11ax. Amazon, 2023. 108 p.
11. Khorov E., Kiryanov A., Lyakhov A., Bianchi G. A tutorial on IEEE 802.11ax high efficiency WLANs // IEEE Commun. Surveys Tuts., vol. 21, no. 1, pp. 197-216, 1st Quart., 2019.
12. Khorov E., Levitsky I., Akyildiz I.F. Current Status and Directions of IEEE 802.11be, the Future Wi-Fi 7 // IEEE Access, vol. 8, pp. 88664-88688, 2021.
13. Reshef E., Cordeiro C. Future Directions for Wi-Fi 8 and Beyond // IEEE Communications Magazine, vol. 60, no. 10, pp. 50-55, October 2022.
14. Bakulin M., Ben Rejeb T., Kreyndelin V., Pankratov D., Smirnov A. Analysis of the MU-MIMO System from the Perspective of Orthogonal and Non-Orthogonal Access // 2023 Systems of Signal Synchronization, Generating and Processing in Telecommunications (SYNCHROINFO), Pskov, Russian Federation, 2023, pp. 1-4.
15. Bakulin M.G., Kreyndelin V.B., Pankratov D.Y., Stepanova A.G. Iterative massive mimo demodulation method with non-gaussian approximation // Journal of Communications Technology and Electronics. 2022. Т. 67. № 6. С. 740-746.
16. Бакулин М.Г., Крейнделин В.Б., Панкратов Д.Ю., Степанова А.Г. Анализ эффективности и сложности демодуляции с использованием негауссовской аппроксимации в системах massive MIMO // Информационные процессы. 2022. Т. 22. № 2. С. 77-92.
17. Daniel T. Valentine, Brian H. Hahn. Essential MATLAB for Engineers and Scientists. 8th Edition. Academic Press, 2022. 428 p.
18. Jennifer Minella. Wireless Security Architecture: Designing and Maintaining Secure Wireless for Enterprise. 1st Edition. Wiley, 2022. 624 p.
19. Benny Bing. Wi-Fi Technologies and Applications: From 802.11ax (Wi-Fi 6) to 802.11be. First Edition. Amazon, 2023. 220 p.



THE USE OF MIMO TECHNOLOGY TO IMPROVE THE PHYSICAL LAYER CHARACTERISTICS OF WI-FI WIRELESS NETWORKS

DENIS Y. PANKRATOV

Moscow, Russia, dpankr@mail.ru

ALEXANDRA V. PAKHOMOVA

Moscow, Russia, aleks.pahom0wa@yandex.ru

KEYWORDS: MIMO, Wi-Fi, physical layer simulation, wireless networks, capacity, BER.

ABSTRACT

Introduction. The development of computer technology has given a sharp leap in the emergence of new technologies in almost all areas of people's lives. This has not spared communication systems, including wireless ones. For data transmission, the need to increase the capacity and the bandwidth of communication systems at a given quality is increasing every year. It is possible to achieve an increase in transmission bitrate by using increasingly multi-position quadrature types of modulation, expanding the frequency spectrum due to higher carrier frequencies, and also supporting the relatively new MIMO (Multiple-Input-Multiple-Output) technology. In the presented article, the authors showed that when using various MIMO configurations in wireless communication systems, it is possible to significantly increase the data transfer rate. The bandwidth is

affected by the MIMO configuration – with an increase in the number of antennas on the transmitting and receiving sides, the data transmission rate increases. **The purpose of the work:** To determine the noise immunity of MIMO technology with a different number of spatial streams in Wi-Fi systems. **Methods:** Using mathematical simulation methods in MATLAB graphical environment. **Results:** The dependence of bit error ration on the signal-to-noise ratio was obtained for different configurations of the MIMO system used in Wi-Fi. The results showed that with an increase in spatial flows, the probability of error decreases with the same signal-to-noise ratio. **Practical significance:** The study showed that the use of MIMO technology with a large number of spatial streams is promising in the development of new wireless communication systems such as Wi-Fi, mobile communications, etc., but more complex digital signal processing algorithms are needed.

REFERENCES

1. E.V. Smirnov, A.V. Proletarsky, "Technologies of modern wireless Wi-Fi networks," Moscow: MSTU im. N.E. Bauman, 2017. 446 p.
2. V.M. Vishnevsky, A.I. Lyakhov, S.L. Portnoy, I.V. Shakhnovich, "Broadband wireless information transmission networks," Moscow: Tekhnosphere. 2005. 592 p.
3. Eldad Perahia, Robert Stacey, "Next generation wireless LANs: 802.11n, 802.11ac, and Wi-Fi direct," Second edition. 2013.
4. Gordon Jeffrey, "WiFi technology: wireless networking," September 10, 2022.
5. M.G. Bakulin, V.B. Kreindelin, D.Yu. Pankratov, "Technologies in radio communication systems on the way to 5G," Moscow: Hotline – Telecom, 2018. 280 p.
6. M.G. Bakulin, L.A. Varukina, V.B. Kreindelin, "MIMO technology: principles and algorithms," Moscow: Hotline – Telecom, 2014. 244 p.
7. MIMO System Technology for Wireless Communication. Edited by George Tsoulos. USA, FL, Boca Raton, CRC Press, 2006. 378 p.
8. Eldad Perahia, Robert Stacey, "Next generation wireless LANs : 802.11n, 802.11ac, and Wi-Fi direct," Second edition. 2013.
9. Gordon Colbach, "The WiFi Networking Book: WLAN Standards: IEEE 802.11 bgn, 802.11n , 802.11ac and 802.11ax," June 30, 2023.
10. IEEE Std 802.11ac™ - 2013. IEEE Standard for Information

technology - Telecommunications and information exchange between systems Local and metropolitan area networks – Specific requirements. Part 11: Wireless LAN Medium Access Control (MAC) and Physical Layer (PHY) Specifications. Amendment 4: Enhancements for Very High Throughput for Operation in Bands below 6 GHz.

11. IEEE Std 802.11ax™?2021.
12. E. Khorov, A. Kiryanov, A. Lyakhov, and G. Bianchi, "A tutorial on IEEE 802.11ax high efficiency WLANs," *IEEE Commun. Surveys Tuts.*, vol. 21, no. 1, pp. 197-216, 1st Quart., 2019.
13. IEEE, "Status of Project IEEE P802.11be," IEEE P802.11-TASK GROUP BE (EHT) MEETING UPDATE, 2019.
14. E. Khorov, I. Levitsky and I. F. Akyildiz, "Current Status and Directions of IEEE 802.11be, the Future Wi-Fi 7," *IEEE Access*, vol. 8, pp. 88664-88688, 2020, doi: 10.1109/ACCESS.2020.2993448.
15. William Palm Iii, "MATLAB for Engineering Applications," McGraw-Hill Education, 4th edition, April 10, 2018.
16. T.E. Krenkel, E.S. Kurashov, "Modeling of the MIMO-T-Comm system, 2015, pp. 21-25. Replace, recent paper on MIMO modeling.

INFORMATION ABOUT AUTHORS:

Denis Y. Pankratov, MTUSI, Ph.D., Associate Professor, Department of SiSRT, Moscow, Russia

Alexandra V. Pakhomova, MTUCI, Moscow, Russia

For citation: Pankratov D.Y., Pakhomova A.V. The use of MIMO technology to improve the physical layer characteristics of Wi-Fi wireless networks. *H&ES Reserch*. 2024. Vol. 16. No. 3. P. 55-61. doi: 10.36724/2409-5419-2024-16-3-55-61 (In Rus)

Звуковые технологии на страже порядка и безопасности.

Оповещение на решениях от компании ОТЗВУК.

Типовая точка оповещения объектовой системы оповещения.

- Соответствует ГОСТ Р 42.3.01-2021;
- интерфейс приема звуковых программ: Ethernet, аналоговый;
- номинальная выходная мощность—200/300/400/500/600 Вт;
- электропитание ~220В;
- ИБП;
- шкаф 9 U.



Таксофонная точка оповещения.

трансляционный усилитель (мощность 200 Вт, с питанием от аккумуляторов, аналоговый вход);
аккумуляторы, антивандальный шкаф;
наружные громкоговорители 50/100 Вт;
блок АТС с IP интерфейсом, (устанавливаемый на АТС для сопряжения с управляющими станциями оповещения верхнего уровня и таксофоном).

Переносной автономный усилительный комплекс – ПАУК

интерфейс приема звуковых программ: микрофон, SD-карта, аналоговый;
номинальная выходная мощность—150 Вт;
электропитание встроенная АКБ 12В;
время работы от батареи – 8 часов (речь);
разборчивость речи на удалении до 1 км



Компетенции компании.

Компания ОТЗВУК является разработчиком и производителем оборудования семейства «ОТЗВУК» позволяющего транслировать программы оповещения, звукового вещания, по магистральным сетям передачи данных (Eth/SDH) до точки и далее по проводным сетям до конечных громкоговорителей;

- оказывает услуги по поддержке и послегарантийному сопровождению произведенного оборудования;
- выполняет работы по НИОКР в соответствии с техническими заданиями в сфере звукового вещания и сопряжением локальных, ведомственных и объектовых систем оповещения с другими видами оборудования;
- программное обеспечение собственной разработки ПАК АСУ «ОТЗВУК» позволяет осуществлять мониторинг, контроль и управление сетями цифрового оповещения, радиовещания, а также управлять устройствами сторонних производителей. Работа в ПАК АСУ отлично масштабируется от одного узла до управления сетями оповещения и вещания масштаба мегаполиса;
- проектирование ЛСО, слаботочных систем в зданиях и сооружениях.

Оборудование точек оповещения:

Пульт – ПАК АСУ «ОТЗВУК»



Средство речевого оповещения «ОТЗВУК – СРО»

- интерфейс приема звуковых программ: Ethernet, микрофон (аналоговый);
- номинальная выходная мощность – 200/400/500/600 Вт;
- электропитание ~220В;
- ИБП встроен;
- шкаф 19 U.



Переносной автономный усилительный комплекс «ОТЗВУК – ПАУК»

- интерфейс : микрофон, SD-карта;
- номинальная выходная мощность – 210 Вт;
- время работы от батареи – 7 часов (речь);
- разборчивость речи на удалении 1 км;
- зарядка +24, ~220В; - переносной вес – 16 кг;

ПАУК

Переносной Автономный Усилительный Комплекс

Разработан для решения задач по оповещению. Предназначен для передачи речевых сообщений и звуковых сигналов на расстояние до 1000 метров.



ПАУК устанавливается на:

любой технике

позициях подразделений

блокпостах

зданиях (сооружениях)

Применение изделия ПАУК:

➤ Оповещение гражданского населения:

- Об организации гуманитарных коридоров
- Местах выдачи гуманитарной помощи
- Окончании боевых действий
- Выходе из убежищ и т.п.

➤ Доведение звуковых сообщений до противника, как на открытой местности, так и находящихся в укрепленных районах и домах;

➤ Подача установленных (специальных) сигналов управления;

➤ Доведение информации агитационного характера диверсионно-разведывательных групп

➤ Обнаружение мест укрытия снайперов и минометных расчетов;

➤ Озвучивание мероприятий массового характера

ПАУК необходим для:

- 1 передовых подразделений
- 2 специальных подразделений
- 3 личного состава на блокпостах
- 4 военно-гражданских администраций

СЛЫШИМОСТЬ ПОДТВЕРЖДЕНА ИСПЫТАНИЯМИ:

↔ 1000 м

при благоприятных условиях


↔ 500 м

в условиях повышенной шумности

ТТХ ПАУК:

 **2 мин**
время установки на машину

 **210 ватт**
мощность акустических систем

 **12 вольт**
источник питания АКБ
7 часов автономной работы

 **16 кг**
масса комплекта

 **до 1000 м**
слышимость сообщений

НАДЁЖНОСТЬ ИСПОЛНЕНИЯ:

- противоударный корпус
- пылевлагозащищенное исполнение
- отечественные детали
- качественные комплектующие

Комплект поставки:

- усилительный блок с АКБ
- блок акустических систем
- пульт управления
- микрофон
- диктофон
- карта памяти
- соединительные кабели
- комплект креплений



#СвоихНеБросаем



8 (812) 718-19-01



mail@otzvuk.spb.ru

192029, г. Санкт-Петербург,
Большой Смоленский пр., д.
10, литер А, офис 400