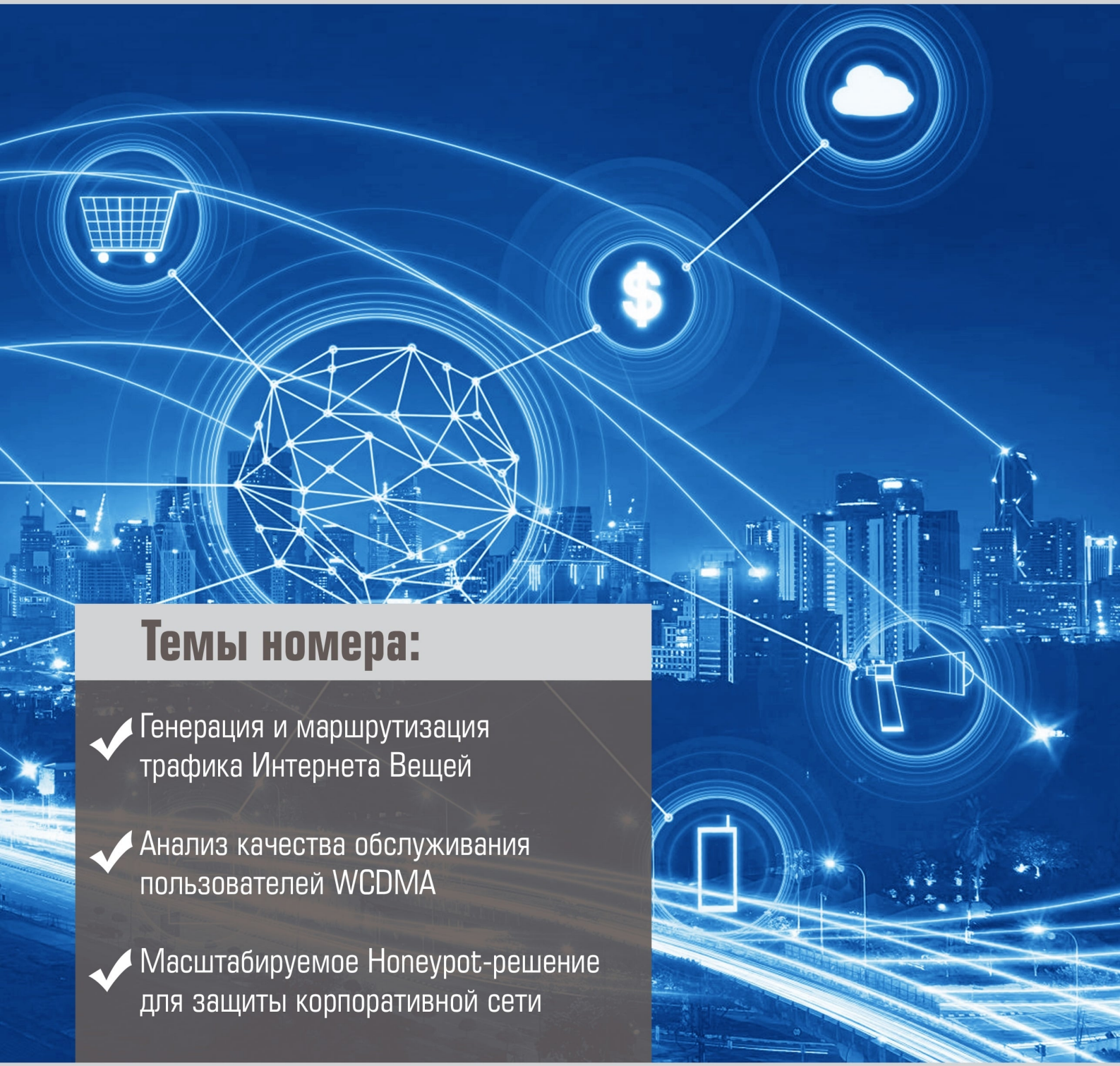
ТУЗС
Том 5. № 3
2019

научный журнал

ТРУДЫ УЧЕБНЫХ ЗАВЕДЕНИЙ СВЯЗИ



Темы номера:

- Генерация и маршрутизация трафика Интернета Вещей
- Анализ качества обслуживания пользователей WCDMA
- Масштабируемое Honeypot-решение для защиты корпоративной сети

Vol. 5. Iss. 3
2019

PROCEEDINGS OF TELECOMMUNICATION UNIVERSITIES

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

Научный журнал

ТРУДЫ
УЧЕБНЫХ ЗАВЕДЕНИЙ СВЯЗИ

Том 5

№ 3

Санкт-Петербург

2019

Труды учебных заведений связи. 2019. Т. 5. № 3. ISSN: 1813-324X

Описание журнала

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

05.11.07 Оптические и оптико-электронные приборы и комплексы
05.11.18 Приборы и методы преобразования изображений и звука
05.12.04 Радиотехника, в том числе системы и устройства телевидения
05.12.07 Антенны, СВЧ-устройства и их технологии
05.12.13 Системы, сети и устройства телекоммуникаций
05.12.14 Радиолокация и радионавигация
05.13.01 Системный анализ, управление и обработка информации
05.13.18 Математическое моделирование, численные методы и комплексы программ
05.13.19 Методы и системы защиты информации, информационная безопасность

Выпускается с 1960 года. Выходит 4 раза в год.

Редакционный совет

Редакционная коллегия

Регистрационная информация

Журнал зарегистрирован Федеральной службой по надзору в сфере связи, информационных технологий и массовых коммуникаций: № 77-17986 от 07.04.2004

Подписной индекс по каталогу «Издания органов НТИ» Агентства «Роспечать»: 59983

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

Контактная информация

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

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

Proceedings of Telecommunication Universities. 2019. Vol. 5. Iss. 3. ISSN: 1813-324X

Description

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

05.11.07 Optical and optoelectronic devices and complexes
05.11.18 Devices and methods of transformation of images and sound
05.12.04 Radio engineering, including television systems and devices
05.12.07 Antennas, microwave devices and its technologies
05.12.13 Systems, networks and devices of telecommunications
05.12.14 Radiolocation and radio navigation
05.13.01 System analysis, management and information processing
05.13.18 Mathematical modelling, numerical methods and complexes of programs
05.13.19 Methods and systems of information security, cybersecurity

Since 1960. Published 4 times per year.

Editorial Council

Editorial Board

Registration Information

Registered by Federal Service for Supervision of Communications, Information Technology and Mass Media on 07.04.2004: № 77-17986

Subscription index for «NTI Editions» Agency «Rospechat» catalog: 59983

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

Contact Information

Publisher: Federal State Budget-Financed Educational Institution of Higher Education «The Bonch-Bruevich Saint-Petersburg State University of Telecommunications» (SPbSUT)

Post address: 193232, Saint-Petersburg, Prospekt Bolshevikov, 22/1
Phone: +7 (812) 326-31-63, local 2022, +79643759970
E-mail: tuzs@spbgut.ru
Web: http://tuzs.sut.ru
ВК: http://vk.com/spbtuzs

СОДЕРЖАНИЕ

CONTENTS

DOI:10.31854/1813-324X-2019-5-3

АНАЛИЗ ПАРАМЕТРОВ ФУНКЦИОНИРОВАНИЯ СЕТИ MPLS ПРИ ИЗМЕНЕНИИ ТОПОЛОГИИ

М.А. Буранова[1*], **Р.Т. Латыпов**[1]

[1]Поволжский государственный университет телекоммуникаций и информатики,
Самара, 443010, Российская Федерация
*Адрес для переписки: buranova-ma@psuti.ru

Информация о статье
УДК 519.872
Статья поступила в редакцию 15.05.2019

Ссылка для цитирования: Буранова М.А., Латыпов Р.Т. Анализ параметров функционирования сети MPLS при изменении топологии // Труды учебных заведений связи. 2019. Т. 5. № 3. С. 6–12. DOI:10.31854/1813-324X-2019-5-3-6-12

Аннотация: *Оценка вероятностно-временных характеристик функционирования инфокоммуникационных сетей – задача, которая является одной из основных при проектировании сетей. Учитывая, что трафик современных сетей обладает свойствами самоподобия, возникают затруднения при использовании традиционного математического аппарата теории массового обслуживания. В работе представлены результаты имитационного моделирования оценки задержки, джиттера и вероятности потерь при обработке трафика в сети MPLS. В качестве исследуемых потоков использовали реальный мультимедийный трафик и поток on-off с распределением Парето периодов on и off. В результате установлено, что при увеличении загрузки сети или при увеличении масштаба сети джиттер, как правило, снижается, а задержка и вероятность потерь увеличиваются.*

Ключевые слова: *параметры качества обслуживания (QoS), MPLS, корреляция, имитационное моделирование.*

Введение

В условиях функционирования современных инфокоммуникационных сетей большое значение имеет обеспечение качества обслуживания – QoS (*от англ.* Quality of Service) – для различных типов приложений. Одним из приоритетных в общем объеме трафика, обрабатываемого в глобальной сети, является мультимедийный поток, особенностью обработки которого является требование соблюдения ограничений по параметрам QoS. При этом основное внимание уделяется, как правило, проблеме удержания задержки на определенном уровне, но для мультимедийных потоков не менее важным параметром является джиттер.

Необходимость оценки джиттера привела к тому, что в последние годы данной проблеме уделяется значительное внимание. Так, в [1] получены некоторые результаты, позволяющие определить джиттер для пуассоновского потока, а также для потоков с экспоненциальным распределением длин пакетов и произвольным распределением интервалов времени между пакетами. В [2–4] представлены результаты анализа джиттера в системе типа G/M/1. Также была проведена оценка джиттера при изменении загрузки сети для трех примеров произвольного распределения интервалов времени между пакетами: экспоненциального, Парето и Вейбулла. Но такие ограничения часто не соответствуют тем характеристикам, которые имеют реальные потоки, которые, как правило, обрабатывается в системе, описываемой математической моделью G/G/1.

Одна из технологий, призванных обеспечить требуемый уровень QoS, это многопротокольная коммутация по меткам – MPLS (*от англ.* Multiprotocol Label Switching). В работах [5, 6] проведен анализ задержки пуассоновского потока в сети MPLS в зависимости от масштаба сети. Но поскольку современный трафик отличается от простейшего потока, то возникает необходимость исследования поведения непуассоновских потоков в зависимости от масштаба и загрузки сети.

В качестве анализируемых параметров рассмотрим задержку, джиттер и вероятность потерь, так как эти параметры наиболее характерны при оценке качества обслуживания сетей. В качестве

обрабатываемых потоков используем мультимедийный трафик, зарегистрированный на реальной сети и on-off процесс с распределением Парето периодов on и off. Поскольку для мультимедийных потоков наиболее критичным является отклонение от задержки в процессе передачи (о чем упоминалось выше), то особое внимание уделим джиттеру – изменению задержки в потоке от некоторого минимального значения [7].

В соответствии с рекомендацией Специальной комиссии по интернет-разработкам – IETF (*от англ.* Internet Engineering Task Force) [8] – под джиттером понимается случайная переменная J_i, определяемая как $J_{i+1} = |T_{i+1} - T_i|$, где $T_i = W_i + Q_i$ – время задержки i-го пакета в узле сети (W_i – время ожидания i-го пакета в очереди, Q_i – время его обслуживания).

Основываясь на [1, 2] и используя предположение Линдли [9], что пакет $(i+1)$ не будет ждать в очереди при выполнении условия $V_{i+1} \geq T_i$, где V_{i+1} – интервал времени между приходом $(i+1)$-го и i-го пакета, получим:

$$W_{i+1} = \begin{cases} 0 & \text{при } V_{i+1} \geq T \\ W_i + Q_i - V_{i+1} & \text{в др. случае} \end{cases},$$

и поэтому

$$J_{i+1} = \begin{cases} |Q_{i+1} - T_i| & \text{при } V_{i+1} \geq T \\ |Q_{i+1} - V_{i+1}| & \text{в др. случае} \end{cases}. \quad (1)$$

Считая случайные величины T_i, Q_i и V_i независимыми и некоррелированными в структуре каждой последовательности, индекс i у соответствующих плотностей вероятностей можно отбросить и ввести обозначения: $f_T(x)$, f_V и $f_Q(z)$.

В соответствии с (1) можно записать:

$$P(J_{i+1} = \omega) = \iiint\limits_{X,Y,Z} P(V_{i+1} = y) \cdot P(Q_{i+1} = z) \cdot P(T_i = x)\, dx\, dz\, d. \quad (2)$$

В (2) учтена независимость случайных величин T_i, Q_{i+1} и V_{i+1}, а области интегрирования X, Y, Z выбираются с учетом возможных значений случайных переменных, которые определяются условием, аналогичным условию (1):

$$\omega = \begin{cases} |z - x| & \text{при } y \geq x \\ |z - y| & \text{в др. случае} \end{cases}.$$

Для плотностей вероятностей из выражения (2) следует [8]:

$$f_{J_{i+1}}(\omega) = \int_0^\infty f_{V_{i+1}}(y) \int_0^\infty f_{Q_{i+1}}(z)[f_T(z-\omega)U(y-x) + + f_T(z-y)U(x-y)]\, dzdy,$$

где $U(x) = \begin{cases} 1 & \text{если } x \geq 0 \\ 0 & \text{в др. случае} \end{cases}$.

Знание плотности $_{J\,i+1}(\omega)$ позволяет найти среднее значение $E\ (J_{\ i+1})$:

$$E(J_{i+1}) = \int_0^\infty \omega f_{J_{i+1}}(\omega) d\omega = \int_0^\infty f_{V_{i+1}}(y) \int_0^\infty f_{Q_{i+1}}(z) \times \int_0^\infty \left[\omega f_{T_i}(z-\omega)U(y-x) + \omega f_{T_i}(z-y)U(x-y)\right] dx. \quad (3)$$

Если учесть, что при $y \geq x$ $\omega = |z - x|$, а при $y < x$ $\omega = |z - y|$, то интеграл по dx в (3) можно переписать, опуская индекс i в виде:

$$\int_0^\infty \left[\omega f_{T_i}(z-\omega)U(y-x) + \omega f_{T_i}(z-y)U(x-y)\right] dx = \int_0^y |z-x| f_T(x) dx + |z-y| \int_y^\infty f_T(x) dx.$$

Теперь для среднего значения джиттера можно окончательно записать:

$$J = E(|T_{i+1} - T_i|) = \int_0^\infty f_V(y) \int_0^\infty f_Q(z) \left[\int_0^y |z-x| f_T(x) dx + |z-y| \int_y^\infty f_T(x) dx \right] \cdot dz \cdot dy. \quad (4)$$

Выражение (4) позволяет рассчитать среднее значение джиттера при известных или приближенных функциях плотности вероятностей случайных интервалов времени между поступлениями пакетов, времени обслуживания и времени ожидания пакета в очереди для системы обслуживания общего вида при обслуживании коррелированного трафика.

Очевидно, что оценка задержки и джиттера в системе $G/G/1$ связана с большими вычислительными сложностями [1–3]. Для анализа параметров QoS в исследуемой сети предпочтительней воспользоваться имитационным моделированием.

Для сравнения исследовались два типа потоков: on-off процесс с распределением Парето периодов on и off (трафик Парето, длина пакетов – 1000 байт) и мультимедийный трафик, зарегистрированный на реальной сети. Для оценивания результатов моделирования с использованием трафика, зарегистрированного на реальной сети, предварительно необходимо проанализировать статистические свойства трафика.

Анализ статистических характеристик трафика

Требуется определить законы распределения интервалов времени между пакетами и длин пакетов рассматриваемого трафика, для чего воспользуемся программой Easyfit Professional, позволяющей произвести статистическую проверку гипотез.

Анализ распределения случайных интервалов времени между пакетами показал, что наиболее точным является распределение Вейбулла с параметрами $\alpha = 0{,}37$ и $\beta = 3{,}5 \cdot 10^{-4}$ (рисунок 1а):

$$f(x) = \frac{\alpha}{\beta}\left(\frac{x}{\beta}\right)^{\alpha-1} \exp\left(-\left(\frac{x}{\beta}\right)^{\alpha}\right),$$

где α – параметр формы; β – масштабный параметр.

Аналогично при анализе распределения случайных длин пакетов получена наиболее точная аппроксимация распределением Коши с параметрами $\sigma = 24$ и $\mu = 1{,}4 \cdot 10^{-3}$ (рисунок 1б):

$$f(x) = \left(\pi\sigma\left(1 + \left(\frac{x-\mu}{\sigma}\right)^2\right)\right)^{-1},$$

где σ – непрерывный масштабный коэффициент; μ – непрерывный параметр формы.

Представленная гистограмма (см. рисунок 1б) имеет три ярко выраженных пика. Основной вклад дают длины пакетов: 475 байт, соответствующие первому пику; 1370 байт, соответствующие второму пику; 1442 байта, соответствующие третьему пику. Очевидно, что в данном случае аппроксимация распределением Коши может быть улучшена использованием аппроксимации суммой трех распределений:

$$f(x) = P_1 \cdot \delta(x - x_0) + P_2 \cdot \delta(x - x_1) + P_3 \cdot \delta(x - x_2),$$

где $\delta(x - x_0)$ – дельта функция в точке x_0, соответствующей первому пику; $\delta(x - x_1)$ – она же в точке x_1, соответствующей второму пику; $\delta(x - x_2)$ – она же в точке x_2, соответствующей третьему пику; $P_1 = 0{,}08$; $P_2 = 0{,}51$; $P_3 = 0{,}41$.

Следовательно:

$$f(x) = 0{,}08 \cdot \delta(x - x_0) + 0{,}51 \cdot \delta(x - x_1) + 0{,}41 \times \\ \times \delta(x - x_2),$$

где $P_1 + P_2 + P_3 = 1$.

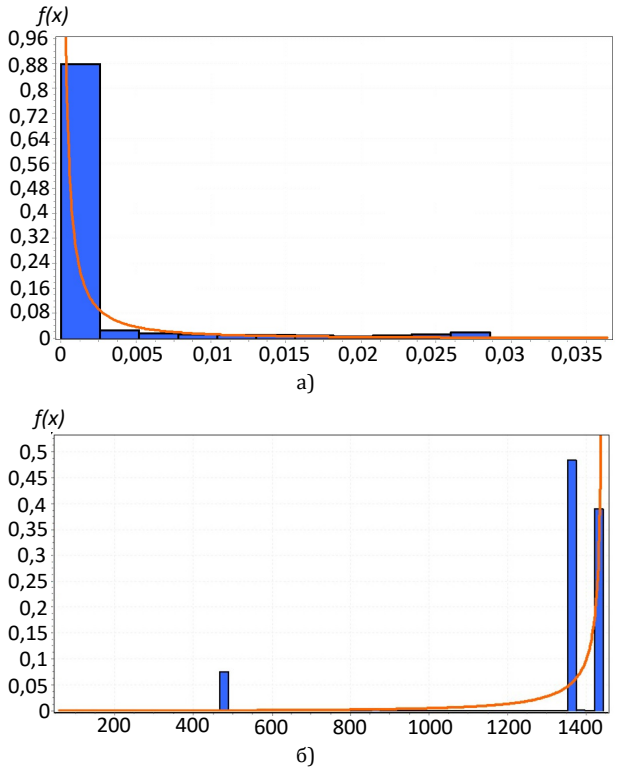


Рис. 1. Гистограмма распределения случайных интервалов времени между пакетами и результат аппроксимации распределением Вейбулла (а) и Коши (б)

Анализ гистограмм и их возможных аппроксимаций на основе критерия Колмогорова – Смирнова, и улучшенных с использованием распределения смеси, показывает, что построение адекватной модели трафика для системы имитационного моделирования с такими параметрами весьма затруднительно.

Для генерируемого программой ns2 потока on-off с распределением Парето периодов on и off анализ гистограмм для интервалов времени между пакетами показал результат аппроксимации, представленный на рисунке 2. Этот анализ, необходимый для более объективной оценки характера и статистической структуры исследуемых потоков, позволил сделать вывод, что наиболее точным является распределение Парето.

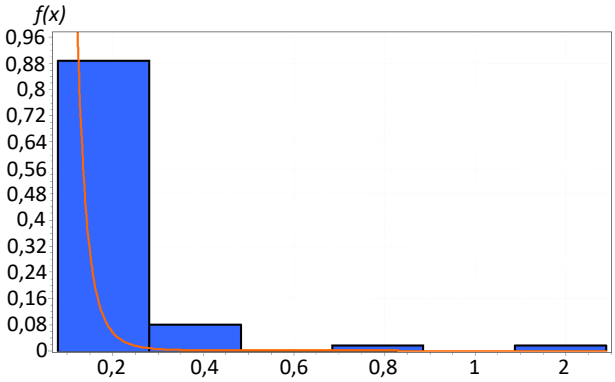


Рис. 2. Гистограмма распределения случайных длин пакетов и результат аппроксимации распределением Pareto

Еще одной важной характеристикой трафика является наличие корреляционных свойств. Для непуассоновских потоков характерна долговременная зависимость между событиями, которая может негативно сказаться на параметрах функционирования систем, обрабатывающих подобный трафик. Случайные процессы могут проявлять свойство долговременной зависимости между событиями через достаточно большие промежутки времени.

Телекоммуникационный трафик, являющийся случайным процессом, обладает долговременной зависимостью, если автокорреляционная функция не суммируема ($\sum_k R(k) = \infty$). Расчет ее выборочной реализации случайного процесса можно провести по формуле [10]:

$$R(k) = \frac{\frac{1}{N-k}\sum_{i=1}^{N-k}(X_i - \bar{X})(X_{i+k} - \bar{X})}{\frac{1}{N}\sum_{i=1}^{N}(X_i - \bar{X})^2},$$

где $\bar{X}$ – среднее значение; N – объем выборки.

График зависимости коэффициентов корреляции $R(k)$ для последовательностей интервалов времени между пакетами и длинами пакетов для реального мультимедийного трафика приведены на рисунках 3а и 3б, из которых видно, что присутствует значительная корреляционная зависимость в последовательностях этих интервалов.

На рисунке 3в приведены коэффициенты корреляции для последовательностей интервалов времени между пакетами потока on-off с распределением Парето периодов on и off, генерируемого программой ns2.

Аналогично реальному мультимедийному трафику в последовательностях интервалов времени между пакетами для генерируемого on-off процесса с распределением Парето присутствует корреляционная зависимость, которая убывает гораздо медленнее по сравнению с мультимедийным трафиком. Длины пакетов данного потока формируются одним размером 1000 байт, следовательно, корреляция будет значительной и стремиться к максимальной.

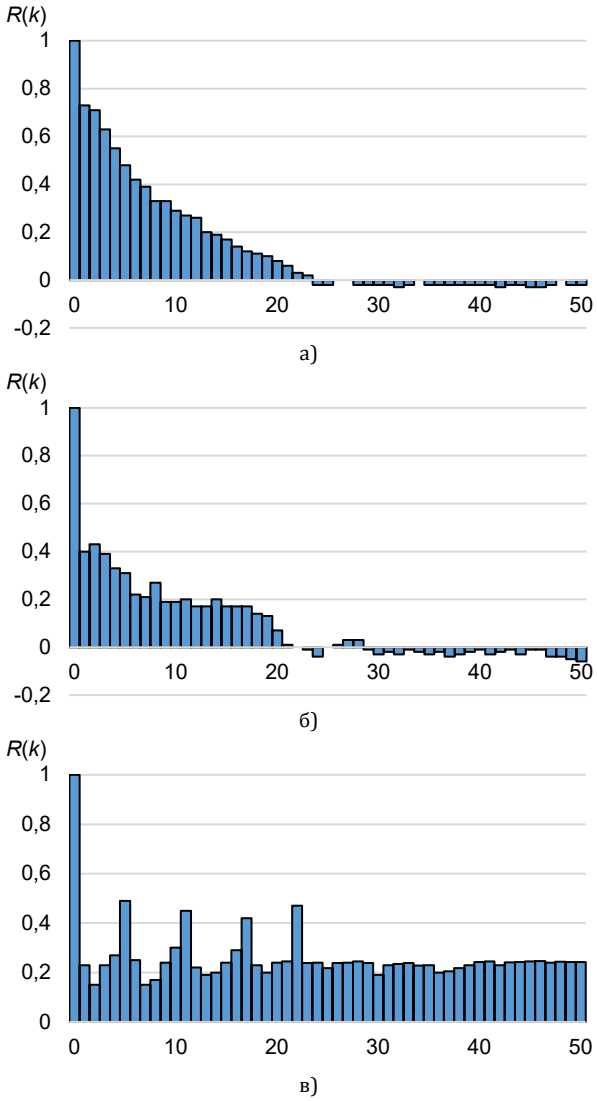


Рис. 3. График зависимости коэффициентов автокорреляции: а) интервалы времени между пакетами; б) размеры пакетов мультимедийного трафика уровня доступа; в) интервалы времени между пакетами трафика по Парето

Анализ статистических характеристик мультимедийного трафика показал, что вероятностный закон распределения случайных интервалов времени между пакетами характеризуется распределением Вейбулла, а длин пакетов – Коши, которое в нашем случае может быть представлено в виде распределения смеси (суммы трех дельта-функций). С учетом установленных корреляционных свойств трафика построение адекватной аналитической модели является затруднительным, что обуславливает разработку имитационной модели с обработкой реального трафика.

Разработка имитационной модели

Имитационная модель, реализованная в программе ns2, позволяет оценить задержку, джиттер задержки пакетов и вероятность их потерь при обработке различных типов трафика, и в схематичном виде представлена на рисунке 4.

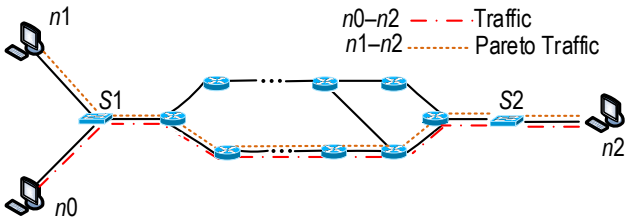


Рис. 4. Схема моделирования в ns2

С использованием разработанной модели было поставлено два эксперимента: 1) исследование зависимости параметров QoS в зависимости от загрузки сети при прохождении трафика через 6 узлов; 2) влияние изменения масштаба сети на параметры QoS (количество узлов варьируется от 5 до 10; коэффициент загрузки ρ = 0,4).

Результаты эксперимента при изменении загрузки сети приведены на рисунках 5а, 5в и 5д. Их анализ показывает, что с увеличением загрузки сети задержка увеличивается.

В тоже время джиттер ведет себя не столь однозначно. При увеличении загрузки джиттер реального трафика снижается до величины загрузки ρ = 0,4, на участке от ρ = 0,4 до ρ = 0,7 появляется явно выраженный локальный максимум; затем при увеличении загрузки джиттер увеличивается. Для on-off процесса с распределением Парето периодов on и off характерно снижение джиттера до ρ = 0,6, затем он увеличивается. Вероятность потерь увеличивается в обоих случаях. Следует заметить, что для реального трафика анализируемые параметры изменяются более резко в сравнении с трафиком Парето. Но рост задержки у трафика Парето начинается при меньшей загрузке (ρ = 0,6). Для сети MPLS такое изменение параметров связано с особенностями реализации технологии и наличием механизмов регуляции перегрузок.

Результаты эксперимента при изменении масштаба сети, а именно при изменении количества узлов в сети показаны на рисунках 5б, 5г и 5е.

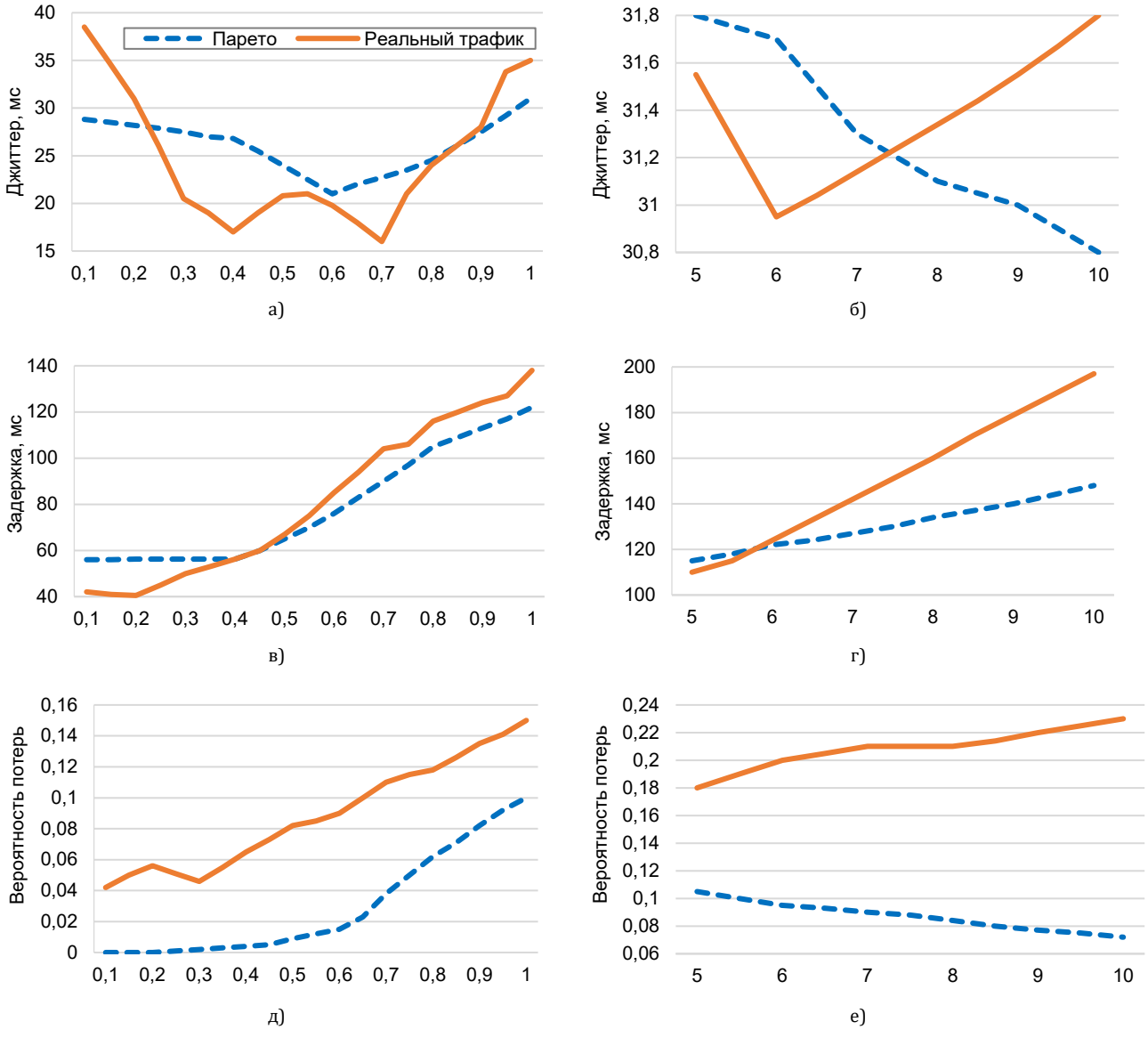


Рис. 5. Изменение джиттера (а, б), задержки (в, г) и вероятности потерь (д, е) в зависимости от загрузки (слева) и количества узлов (справа) в сети MPLS

Анализ результатов второго эксперимента показал, что джиттер пакетов реального трафика, как и при увеличении загрузки сети, снижается до определенного уровня $n = 6$, затем начинает увеличиваться. Для трафика Парето (on-off процесс) джиттер с увеличением количества узлов снижается. Задержка ожидаемо увеличивается, но увеличение незначительно. Изменение вероятности потерь пакетов реального трафика незначительно увеличивается, в тоже время для трафика Парето снижается. При этом эти изменения лежат в пределах 0,05.

Обратим внимание, что оцениваемые параметры QoS ведут себя более предсказуемо, кривые более гладкие для трафика Парето. При этом корреляционные связи для интервалов времени между пакетами и длин пакетов у этого трафика выше, чем рассматриваемого мультимедийного потока. Отсюда следует, что при увеличении коэффициента корреляции для статистик трафика (интервалов времени между пакетами и длин пакетов) параметры QoS улучшаются и становятся более предсказуемыми без локальных максимумов.

Заключение

Определены вероятностные законы распределения случайных моментов поступления пакетов на обслуживание (распределение Вейбулла) и длин пакетов (распределение Коши) для мультимедийного трафика; полученные распределения относятся к классу распределений с «тяжелыми хвостами».

Получены оценки задержки, джиттера и вероятности потерь при изменениях загрузки сети и масштаба сети. В результате серии проведенных экспериментов с имитационной моделью обработки трафика установлены следующие зависимости.

Во-первых, при увеличении уровня загрузки сети MPLS:

– задержка и вероятность потерь также увеличиваются;

– джиттер имеет тенденцию к снижению до $\rho = 0{,}4$, на участке от $\rho = 0{,}4$ до $\rho = 0{,}7$ появляется явно выраженный локальный максимум, затем наблюдается тенденция к росту.

Во-вторых, при увеличении количества узлов сети MPLS:

– задержка увеличивается;

– джиттер имеет тенденцию к снижению до $n = 6$, затем наблюдается тенденция к росту;

– вероятность потерь увеличивается для реального трафика, а для on-off процесса с распределением Парето периодов on и off – снижается.

Предложенная в работе модель может быть использована при оценке параметров функционирования сети MPLS в условиях обработки различных типов трафика, в том числе при обработке реальных потоков. При этом можно определить наиболее эффективные условия обработки потоков различного типа при изменении топологии и характера функционирования сети.

В развитие данной темы предполагается разработка аналитической модели с учетом наличия в трафике самоподобных свойств, в том числе корреляционных зависимостей. Такая модель может быть построена с использованием аппроксимации моделью $H_l/H_k/1$.

Список используемых источников

1. Dahmouni H., Girard A., Sansò B. An analytical model for jitter in IP networks // Annals of telecommunications – annales des telecommunications. 2012. Vol. 67. Iss. 1-2. PP. 81–90. DOI:10.1007/s12243-011-0254-y

2. Dbira H., Girard A., Sansò B. Calculation of packet jitter for non-poisson traffic // Annals of telecommunications. 2016. Vol. 71. Iss. 5-6. PP. 223–237. DOI:10.1007/s12243-016-0492-0

3. Kartashevskiy V., Buranova M. Analysis of Packet Jitter in Multiservice Network // 5th International Scientific-Practical Conference Problems of Infocommunications Science and Technology (PIC S&T, Kharkiv, Ukraine, 9–12 October 2018). Piscataway, NJ: IEEE, 2018. DOI:10.1109/INFOCOMMST.2018.8632085

4. Буранова М.А. Карташевский В.Г., Латыпов Р.Т. Анализ джиттера мультисервисной сети // XX Международная научно-техническая конференция, XVI Международная научно-техническая конференция «Проблемы техники и технологии телекоммуникаций. Оптические технологии в телекоммуникациях» (Уфа, Россия, 20–22 ноября 2018). Уфа: Уфимский государственный авиационный технический университет, 2018. Том 1. С. 117–119.

5. Kartashevskiy V.G., Buranova M.A. Research of tunneling effect in MPLS network // Proceedings of the 4th International Scientific-Practical Conference Problems of Infocommunications Science and Technology (PIC S&T, Kharkiv, Ukraine, 10–13 October 2017). Piscataway, NJ: IEEE, 2017. DOI:10.1109/INFOCOMMST.2017.8246391

6. Гольдштейн А.В. Механизм эффективного туннелирования в сети MPLS // Вестник связи. 2004. № 2. С. 48–54.

7. Rec. ITU-T Y.1540 (07/16). Internet protocol data communication service – IP packet transfer and availability performance parameters.

8. RFC 33934. Demichelis C, Chimento P. IP Packet Delay Variation Metric for IP Performance Metrics (IPPM). 2000. DOI:10.17487/RFC3393

9. Kleinrock L. Queueing Systems. Volume 1: Theory. New York: Wiley-Interscience, 1975. 417 p.

10. Шелухин О.И., Тенякшев А.М., Осин А.В. Фрактальные процессы в телекоммуникациях. М.: Радиотехника, 2003. 480 с.

* * *

MPLS NETWORK PARAMETERS ANALYSIS WHEN CHANGING THE TOPOLOGY

M. Buranova[1], **R. Latypov**[1]

[1]Povolzhskiy State University of Telecommunications and Informatics,
Samara, 443096, Russian Federation

Article info
The article was received 15 May 2019

For citation: Buranova M., Latypov R. MPLS Network Parameters Analysis when Changing the Topology. *Proceedings of Telecommunication Universities*. 2019;5(3):6–12. (in Russ.) Available from: https://doi.org/10.31854/1813-324X-2019-5-3-6-12

Abstract: *One of the main tasks in network design is to evaluate the probability-time characteristics of the functioning of information and communication networks. Considering that the traffic of modern networks possesses the properties of self-similarity, we observe the difficulties while using the traditional mathematical apparatus of public serve theory. This paper presents us the results of jitter simulation estimating the delay, the probability of traffic loss when traffic processing in MPLS network. It was taken the real multimedia traffic and an on-off flow with a distribution of Pareto periods on and off as the researched flows. As the result, we discovered that when the network load increases or network size increases, jitter usually decreases, while the delay and loss probability increase.*

Keywords: *parameters of quality of service (QoS), MPLS, correlation, simulation.*

References

1. Dahmouni H., Girard A., Sansò B. An analytical model for jitter in IP networks. *Annals of telecommunications – annales des telecommunications*. 2012;67(1-2):81–90. Available from: https://doi.org/10.1007/s12243-011-0254-y
2. Dbira H., Girard A., Sansò B. Calculation of packet jitter for non-poisson traffic. *Annals of telecommunications*. 2016;71(5-6): 223–237. Available from: https://doi.org/10.1007/s12243-016-0492-0
3. Kartashevskiy V., Buranova, M. Analysis of Packet Jitter in Multiservice Network. *5th International Scientific-Practical Conference Problems of Infocommunications Science and Technology, PIC S&T, 9–12 October 2018, Kharkiv, Ukraine*. Piscataway, NJ: IEEE; 2018. Available from: https://doi.org/10.1109/INFOCOMMST.2018.8632085
4. Buranova M.A., Kartashevskiy V.G., Latipov R.T. Jitter analysis in multiservice network. *XXth Mezhdunarodnaia nauchno-tekhnicheskaia konferentsiia, XVIth Mezhdunarodnaia nauchno-tekhnicheskaia konferentsiia "Problemy tekhniki i tekhnologii telekommunikatsii. Opticheskie tekhnologii v telekommunikatsiiakh", 20–22 November 2018, Ufa, Russia.* [Proceedings of the XXth International Scientific and Technical Conference, the XVIth International Scientific and Technical Conference "Problems of Engineering and Telecommunications Technology. Optical Technologies in Telecommunications", 20–22 November 2018, Ufa, Russia]. Ufa: Ufa State Aviation Technical University Publ.; 2018. vol.1. p.117–119. (in Russ.)
5. Kartashevskiy V.G., Buranova M.A. Research of tunneling effect in MPLS network. *Proceedings of the 4th International Scientific-Practical Conference Problems of Infocommunications Science and Technology, PIC S&T, 10–13 October 2017, Kharkiv, Ukraine*. Piscataway, NJ: IEEE; 2017. Available from: https://doi.org/10.1109/INFOCOMMST.2017.8246391
6. Goldshtein A.V. Mekhanizm effektivnogo tunnelirovaniia v seti MPLS [Effective Tunneling Mechanism in an MPLS Network]. *Vestnik sviazi*. 2004;2:48–54. (in Russ.)
7. Rec. ITU-T Y.1540. *Internet protocol data communication service – IP packet transfer and availability performance parameters*. Jule 2016.
8. RFC 33934. Demichelis C, Chimento P. *IP Packet Delay Variation Metric for IP Performance Metrics (IPPM)*. 2000. Available from: https://10.17487/RFC3393
9. Kleinrock L. *Queueing Systems. Volume 1: Theory*. New York: Wiley-Interscience; 1975. 417 p.
10. Shelukhin O.I., Teniakshev A.M., Osin A.V. *Fraktalnye protsessy v telekommunikatsiiakh* [Fractal Processes in Telecommunications]. Moscow: Radiotekhnika Publ.; 2003. 480 p. (in Russ.)

РАДИОЛИНИИ МЕТЕОРНОЙ СВЯЗИ В ТЕЛЕКОММУНИКАЦИОННОЙ СЕТИ СЕВЕРНОГО МОРСКОГО ПУТИ

С.В. Воронин[1], **В.И. Дорошенко**[2], **Ю.Г. Ксенофонтов**[2*]

[1]Санкт-Петербургский университет ГПС МЧС России,
Санкт-Петербург, 196105, Российская Федерация
[2]Государственный университет морского и речного флота имени адмирала С.О. Макарова,
Санкт-Петербург, 198035, Российская Федерация
*Адрес для переписки: ksenofontov.ura@mail.ru

Информация о статье
УДК 621.371
Статья поступила в редакцию 09.06.2019

Ссылка для цитирования: Воронин С.В., Дорошенко В.И., Ксенофонтов Ю.Г. Радиолинии метеорной связи в телекоммуникационной сети Северного морского пути // Труды учебных заведений связи. 2019. Т. 5. № 3. С. 13–18. DOI:10.31854/1813-324X-2019-5-3-13–18

Аннотация: *Целью данной статьи является обоснование целесообразности применения метеорной сети связи как телекоммуникационной основы в сети доступа системы управления движением судов к объектам инфраструктуры Арктики России в прибрежной зоне Северного морского пути. В ней с позиций системного анализа представлены основные параметры, характеризующие телекоммуникационные технологии метеорной связи, структурно-функциональная схема, обобщенная математическая модель сети, состоящей из радиопередатчика и приемника, включая антенные системы. Сформулированы предложения по использованию в качестве ультракоротковолновых антенных систем адаптивных антенных решеток.*

Ключевые слова: *радиолиния метеорной связи, структурно-функциональная схема, адаптивные антенные решетки, коэффициент использования радиолинии, многолучевое распространение.*

Метеорная связь на ультракоротких волнах (УКВ) широко используется во всем мире, в том числе и в условиях Крайнего Севера [1], однако проблема передачи данных по радиолиниям метеорной связи (РМС) относится к числу слабо структурируемых задач. Самую большую неопределенность вносит случайный характер моментов появления метеорных следов [2], пригодных для передачи данных, и случайный характер длительностей существования этих следов, которые способны обеспечить энергетический контакт между корреспондентами. Отсутствие таких экономичных телекоммуникационных сетей тормозит развитие судоходства с использованием Северного морского пути. Один из вариантов, который включает в себя три радиосети на базе РМС, позволяющих сформировать статистически устойчивый канал передачи данных между удаленными объектами инфраструктуры Северного морского пути [3], представлен на рисунке 1, где: А, Б, В – ведущие станции соответствующих подсетей; a_i, b_i – ведомые станции каждой подсети; ПРД – УКВ-передатчик; ПРМ – УКВ-приемник.

Рис. 1. Топология варианта телекоммуникационной сети обмена данными на примере морского спасательно-координационного центра (МСКЦ) в городе Диксон

Центром каждой из радиосетей является ведущая станция (ВДС). В свою очередь, все ведущие станции ВДС-1, ВДС-2 и ВДС-3 включены в единую локальную вычислительную сеть (ЛВС), в центре которой расположен главный сервер, например, МСКЦ, регулирующий работу всех радиосетей.

Исходя из того, что технические средства навигационного оборудования (ТС НО) в Арктике функционируют в сложных географических условиях, и расположены в радиусе до 2000 км от ВДС, возникает необходимость поиска наиболее рационального решения дальней связи по критерию «эффективность-стоимость». Тем не менее, несмотря на широкое использование РМС во всем мире, такой вид связи до настоящего времени не применяется в телекоммуникациях Северного морского пути. В то же время для обеспечения его нормального функционирования в условиях Арктики целесообразно в автоматизированной системе управления движением судов (СУДС) в условиях сложной гидрометеорологической обстановки Севера России применить РМС. Сложные технические средства навигационного оборудования СУДС в этих условиях могут выходить из строя, а поэтому необходим централизованный непрерывный автоматический мониторинг эксплуатационного состояния этих ТС НО. Поэтому для каждого ТС НО необходимо предусмотреть автоматический контроль своей работоспособности и по его результатам формировать формализованное сообщение для центра, осуществляющего такого вида мониторинг. Исходя из решения стоящих перед ним задач, с учетом складывающейся обстановки, частоту передачи и объем таких сообщений определяет СУДС. Если сообщения передаются по прерывистому каналу передачи данных РМС, то в течение каждого энергетического контакта могут быть переданы либо все сообщения полностью, либо (если были прерывания в связи) по частям. Для охвата всех ТС НО на большой территории (до 2000 км) формируется сеть РМС. Эта сеть может охватывать до 200 ТС НО. Территория, которую может охватывать одна РМС, зависит от параметров ее технических средств: мощности радиопередающих устройств (РПДУ), чувствительности радиоприемных устройств (РПУ), физических параметров антенн, реализованных методов модуляции-демодуляции сигнала и др. Эти параметры определяют коэффициент использования $К_и$ пропускной способности РМС, а от него зависит предельное количество ТС НО, которые могут быть охвачены одной РМС. Таким образом, задача построения структуры РМС является многокритериальной задачей и для ее оптимизации требуется нахождение компромиссного решения. В данной работе основное внимание уделяется проблеме повышения $К_и$ путем применения адаптивных антенных решеток (ААР) на УКВ.

Принцип реализации предлагаемого решения следующий. Суммарное количество метеоров в атмосфере Земли оценивается миллионами штук в сутки, но при сгорании не все они оставляют следы, которые возможно использовать для передачи данных на УКВ. Некоторые метеоры после сгорания оставляют ионизированные следы длиной порядка 20 км, которые существуют от нескольких секунд до нескольких минут. Эти следы способны отражать сигналы УКВ и их можно использовать для связи между корреспондентами на расстоянии до 2000 км. В условиях Севера на частотах 40–60 МГц средняя длительность контакта от одного метеорного следа составляет от 0,2 до 200 с, которая изменяется в течение времени (на протяжении суток, времени года и др.) [4–8].

Так как данный канал связи является прерывным по своей природе, то для его оценки вводится такой параметр, как коэффициент использования линии для передачи данных:

$$К_и = \frac{\sum_{i=1}^{n} t_{ci}}{t_н}, \quad (1)$$

где t_{ci} – длительность i-го прохождения сигнала, измеренная на уровне порогового напряжения $U_{пор}$; $t_н$ – время наблюдения.

Коэффициент $К_и$ зависит от длины волны, мощности передатчика, коэффициента усиления антенны и направления главного лепестка ее диаграммы направленности (ДН), величины $U_{пор}$, определяемой заданным отношением сигнал/помеха ($U_с/U_п$) на входе РПУ, а также от числа и частоты появления в ионосфере метеорных следов (рисунок 2). Изменения числа и направления движения метеоров в течение суток и времени года приводит к значительным колебаниям величины $К_и$. В большинстве случаев среднюю величину $К_и$ можно считать приближенно равной 0,05–0,1.

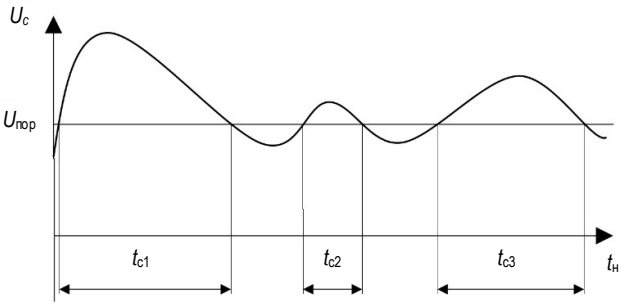


Рис. 2. Временная диаграмма функционирования РМС, характеризующая коэффициент использования пропускной способности $К_и$ (для примера, на рисунке отображены три энергетических контакта между корреспондентами)

Как видно из рисунка 2, система способна функционировать лишь при относительно сильном сигнале, где отношение $U_с/U_п$ превышает пороговое значение.

В РМС в дежурном режиме (режим поиска контакта для связи) используются немодулированные

гармонические колебания. Для увеличения пропускной способности канала передачи данных рекомендуется применить такие методы многопозиционной модуляции, как BPSK, QPSK или QAM, позволяющие увеличить количество кодируемых в единицу времени бит, при этом существенно повысить помехоустойчивость их передачи по каналу РМС [10]. Минимальная мощность принимаемого сигнала на входе РПУ равна [9]:

$$P_{\text{РПУmin}} = AP_{\text{РПДУ}}G^2\lambda^2N_0^2, \qquad (2)$$

где A – коэффициент пропорциональности; $P_{\text{РПДУ}}$ – мощность радиопередающего устройства; λ – длина волны; N_0 – электронная плотность метеорного следа, позволяющая получить уровень сигнала, превышающий пороговый.

Из (2) видно, что при повышении N_0 имеет место регистрация отражений от более плотных (насыщенных) следов, при этом радиолиния использует относительно сильные сигналы.

При постоянном пороговом уровне приема $U_{\text{пор}}$ с возрастанием коэффициента усиления антенны G аппаратура регистрирует сигналы, отраженные также и от менее плотных метеорных следов, что, в свою очередь, непременно повышает чувствительность приемной аппаратуры. Исходя из этого, предлагается один из способов повышения эффективности РМС – выбор направления ориентации ДН и корректировка коэффициента усиления приемной ААР, когда используются наиболее насыщенные метеорные следы, вследствие чего увеличиваются амплитуды сигналов U_{ci} и, соответственно, интервалы t_{ci} (см. рисунок 2), что непременно обеспечивает повышение значения коэффициента $K_{\text{и}}$ (1).

Большой научный интерес представляет вопрос, в какую точку небесного пространства должны быть направлены передающая и приемная антенны. Теоретический анализ показывает, что наилучшие результаты достигаются при некотором отклонении ДН обеих антенн в сторону от направления основной трассы. При этом оптимальный угол ориентации антенн зависит как от времени суток, так и от географического положения линии. Эти отклонения достигают 30°; отсюда ширина диаграммы направленности должна быть порядка 50–60°. Возможна также работа с узконаправленными антеннами. В последнем случае направление главного лепестка должно изменяться в течение суток в соответствии со смещением области с наибольшим числом полезных отражений. Для этой цели предлагается применить особый класс антенн – ААР [11], которые позволяют автоматически подстраивать ширину и направление главного лепестка ДН в соответствии с заданным алгоритмом синхронизации антенн. На линиях метеорной связи наблюдается многолучевое распространение радиоволн, обусловленное существованием нескольких следов, разрывом следа на части и его сильным искривлением под действием сильных атмосферных потоков, а также отражением от регулярных слоев ионосферы. Полоса пропускания метеорного канала может достигать 5…6 МГц, однако на практике из-за многолучевости полоса пропускания радиотракта ограничивается, и, как правило, не превышает 300 кГц. К тому же, увеличение полосы пропускания метеорного тракта требует значительного увеличения мощности передатчика.

В целом, при мощности передатчика 5 кВт и усилении антенн 10 дБ можно получить статистически устойчивую связь на расстоянии до 2000 км.

Идея адаптации ДН ААР состоит в том, что поиск контакта с корреспондентом осуществляется на широкой ДН (порядка 50–60°), а после вхождения в связь осуществляется автоматическое ее сужение с целью снижения возможного уровня посторонних помех на приеме. Это позволит адаптивно повышать как достоверность приема дискретных сигналов, так и скорость передачи данных в течение времени короткого контакта с корреспондентом. Таким образом, не затрагивая другие элементы РМС (РПДУ, РПУ и др.), предлагается повышать коэффициент использования энергетического ресурса РМС за счет более полного использования потенциальных возможностей физической среды, в которой функционирует РМС.

По определению ААР – многоэлементная антенна, в которой амплитуды и фазы передаваемых (принимаемых) сигналов автоматически регулируются и устанавливаются по требуемому закону. В них используется система из N линейно-разнесенных антенных элементов-излучателей (рисунок 3), а также процессор цифровой обработки сигналов, работающий в режиме реального времени. Данный процессор управляет формированием пространственных характеристик антенной системы.

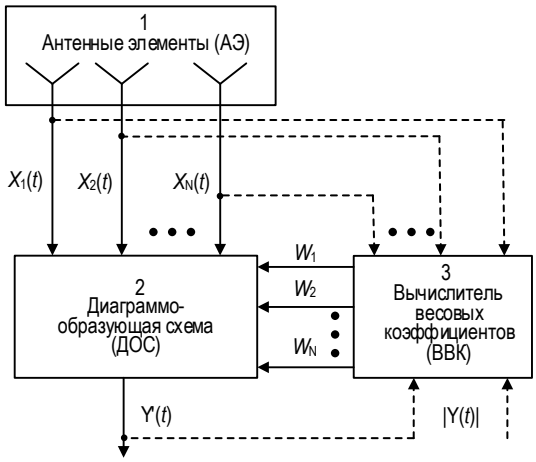


Рис. 3. Структурная схема ААР

В приемной части указанной выше антенной системы сигналы, поступающие от каждого i-го элементов решетки, подвергаются демодуляции и вы-

делению синфазных и квадратурных составляющих. Полученные сигналы перемножаются на весовые коэффициенты (ВК), а затем суммируются, формируя выходной сигнал. Выбор соответствующего набора ВК позволяет сформировать пространственную характеристику ААР так, чтобы максимизировать мощность принимаемого сигнала от передающей станции.

Процесс адаптации зависит от многих факторов: принципа построения адаптивной антенны, типа антенных элементов, типа процессора, используемых алгоритмов адаптации и т. д.

ААР в составе РМС выполняет следующие функции:

– переключается на луч w_k с наилучшим соотношением $U_с/U_п$;

– обнаруживает луч с сигналом, уровень которого значительно ниже уровня шумов;

– определяет направление на источник сигнала с наилучшим соотношением $U_с/U_п$;

– создает узкую ДН в направлении источника сигнала с наилучшим соотношением $U_с/U_п$;

– выполняет корректировку уровня боковых лепестков.

В свою очередь, она обладает двумя основными свойствами: во-первых, способностью формировать многолучевой ДН, что дает возможность обеспечить пространственный обзор, а во-вторых, – способностью функционировать в адаптивном режиме, при котором ААР адаптируется к изменению соотношения $U_с/U_п$.

В многолучевых ААР (рисунок 4) каждому сигналу, соответствующему отдельному лучу ДН, присваивается вес [11]. При этом амплитудная ДН многолучевой ААР определяется следующим выражением:

$$sF(u) = \sum_{k=1}^{K} w_k F_k, \qquad (3)$$

где w_k – весовой коэффициент в канале адаптации k-го луча; $F_k(u)$ – ДН, соответствующая k-му лучу.

В целом ААР в составе РМС решает следующие задачи:

– определяет направления поступления сигналов от каждого k-го источника и их количество K;

– идентифицирует полезные сигналы и помехи;

– формирует узкие ДН в направлении полезных источников и минимальные уровни боковых лепестков в направлении источников помех;

– производит формирование пространственно-временной области.

В качестве обобщенной математической модели рассмотрим общий случай функционирования РМС, в которой одновременно присутствуют отражения от нескольких следов метеоров разной плотности, и, соответственно, образуются несколько трасс $r_j\left(j = \overline{1,k}\right)$.

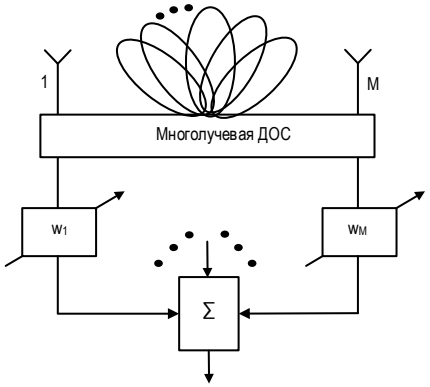


Рис. 4. Структурная схема многолучевой ААР

Процесс передачи сообщений в такой системе описывается системой операторных уравнений (помехи в канале в данном случае не учитываются):

$$s(\lambda, t) = A[\lambda, s(t)], \qquad (4)$$

$$s(\lambda, r, t) = Bs(\lambda, t), \qquad (5)$$

$$e_j\left(\lambda, r_j, t\right) = C_j s(\lambda, r, t), \left(j = \overline{1,k}\right), \qquad (6)$$

$$e_\Sigma(\lambda, t) = \sum_{j=1}^{k} D_j e_j\left(\lambda, r_j, t\right), \left(j = \overline{1,k}\right), \qquad (7)$$

$$\lambda = E e_\Sigma(\lambda, t). \qquad (8)$$

Структурно-функциональная схема тракта, реализующая систему (4–8), представлена на рисунке 5, где: $A, A_i\left(i = \overline{1,N}\right)$ – устройства преобразования сообщений в каналах, несущих полезную информацию; B – ДН передающей антенны; $C_j\left(j = \overline{1,k}\right)$ – физическая среда (метеорный след, обеспечивающий отражение сигналов на УКВ); $D_j\left(j = \overline{1,k}\right)$ – j-ая ДН многолучевой приемной ААР УКВ-диапазона; E – входное устройство приемника, содержащее узкополосную фильтрующую цепь, демодулятор и низкочастотное фильтрующее звено; λ – передаваемое сообщение в основном канале; $s(t)$ – переносчик информации.

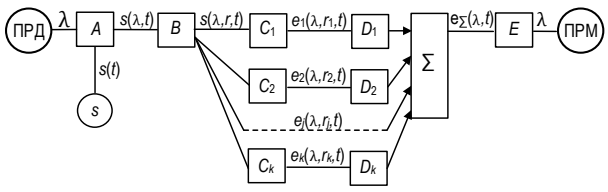


Рис. 5. Структурно-функциональная схема канала РМС с использованием приемной многолучевой ААР УКВ-диапазона

Так как в (7) учитывается лишь свойство направленности приемной антенной системы, то комплексную ДН можно описать выражением:

$$D\left(r_j\right) = kD(\alpha_{п1}, \alpha_{п2}) e^{i\psi_D(\alpha_{п1}, \alpha_{п2})}, \qquad (9)$$

где $D(\alpha_{п1}, \alpha_{п2})$ – амплитудная ДН; $\psi_D(\alpha_{п1}, \alpha_{п2})$ – фазовая ДН; $(\alpha_{п1}, \alpha_{п2})$ – угловые координаты полезного отраженного сигнала, несущего сообщение λ в

вертикальной и горизонтальной плоскостях соответственно, наблюдаемого по j-му каналу в трехмерной системе пространственной системе (x, y, z); k – нормирующий коэффициент.

В соответствии с операторным уравнением (7) и соотношением (9) на выходе антенной системы получим:

$$e_{\Sigma}(\lambda, t) = Re\left\{\sum_{j=1}^{K} A_j(\lambda, r_j, t) D_j(\alpha_{п1}, \alpha_{п2}) e^{i\omega_c t}\right\}, \quad (10)$$

где A_j – комплексная огибающая электрической составляющей поля в раскрыве антенной системы.

С выхода антенной системы сигнал преобразуется оператором E, и в итоге получаем решение (оценку) $\tilde{\lambda}$, воспроизводящее переданное сообщение с определенной достоверностью. В общем случае эта оценка определяется следующим операторным уравнением, полученным из системы (4–8):

$$\tilde{\lambda} = E\left\{\sum_{j=1}^{K} D_j C_j B A[\lambda, s(t)]\right\}. \quad (11)$$

Большая часть энергии, излучаемой передающей антенной, расходуется в пространстве крайне нерационально, поскольку в данный момент приемная антенна ориентирована строго в определенном направлении. Имея предположение, что сигнал посылался бы только в направлении наилучшего его отражения, то это позволило бы значительно повысить эффективность связи в энергетическом плане. Это может быть отмечено возрастанием соотношения сигнал/помеха при передаче данных между корреспондентами, и, соответственно, способствует увеличению $K_и$.

Вывод

Проведенные исследования показали, что повышение коэффициента использования линии $K_и$ с целью увеличения пропускной способности РМС может быть достигнуто путем использования на приемной стороне ААР УКВ-диапазона.

Дальнейшие исследования необходимо проводить в направлении совершенствования технических характеристик ААР, учитывая возможности их применения в арктическом регионе РФ с учетом специфики распространения УКВ-сигнала, отраженного от метеорных следов.

Список используемых источников

1. Дорошенко В.И., Стратонова О.Н., Пивоварова А.К. Метеорная связь в районах Крайнего Севера России // Материалы IV Межвузовской научно-практической конференции аспирантов, студентов и курсантов «Современные тенденции и перспективы развития водного транспорта России» (Санкт-Петербург, Россия, 14 мая 2015 года). СПб.: ГУМРФ, 2015. С. 31–33.

2. Капралов Д.Д., Кирик Д.И. Стохастическая модель метеорного радиоканала // Труды учебных заведений связи. 2018. Т. 4. № 3. С. 54–64. DOI:10.31854/1813-324X-2018-4-3-54-64

3. Дорошенко В.И., Ксенофонтов Ю.Г. Применение метеорной связи в системах обеспечения безопасности объектов инфраструктуры Северного морского пути // Вопросы оборонной техники. Серия 16: Технические средства противодействия терроризму. Серия 16. 2019. № 1-2(127-128). С. 3–11.

4. Титков С.Б. Технические предложения по использованию метеорной связи // Защита информации. Инсайд. 2006. № 3(9). С. 74–80.

5. Рябов И.В., Толмачев С.В., Лебедева А.А. Принципы программно-определяемых радиосистем и их применение в рамках задачи исследования метеорной радиосвязи // Современные наукоемкие технологии. 2016. № 7-1. С. 59–66.

6. Стругов Ю.Ф., Семенов А.М., Добровольский С.М., Батырев И.А. Стохастическое моделирование каналов с аддитивными и мультипликативными помехами. Схема реализации // Математические структуры и моделирование. 2015. № 2(34). С. 48–63.

7. Качнов А.И., Пенкин А.А., Рыбаков А.В. Разработка мобильной системы информационного обеспечения с использованием каналов метеорной связи // V Международная научно-техническая и научно-методическая конференция «Актуальные проблемы инфотелекоммуникаций в науке и образовании» (Санкт-Петербург, Россия, 10–11 марта 2016). Сборник научных статей. СПб.: СПбГУТ, 2016. С. 177–181.

8. Благов Д.С., Волвенко С.В. Повышение скорости передачи информации в метеорных системах связи путем использования сигналов переменной длительности // Научно-технические ведомости Санкт-Петербургского государственного политехнического университета. Информатика. Телекоммуникации. Управление. 2010. № 5(108). С. 7–13.

9. Белокопытов А.Е. Выбор эффективного вида цифровой модуляции в системах радиосвязи по критериям эффективности // Научный альманах. 2015. № 11-3(13). С. 35–38. DOI:10.17117/na.2015.11.03.035

10. Рябов И.В., Толмачев С.В., Лебедева А.А. Аппаратно-программный комплекс для обнаружения метеорных следов с изменяемой полосой пропускания // Радиотехнические и телекоммуникационные системы. 2016. № 4(24). С. 66–75.

11. Петров В.П. Алгоритмы оценки пространственного спектра в адаптивных цифровых антенных решетках // Вестник СибГУТИ. 2014. № 4. С. 60–70.

* * *

RADIOCHANNELS OF METEOR-BURST COMMUNICATION NETWORK OF THE NORTHERN SEA ROUTE

S. Voronin[1], **V. Doroshenko**[2], **Y. Ksenofontov**[2]

[1]Saint-Petersburg University of State Fire Service of Emercom of Russia,
St. Petersburg, 196105, Russian Federation
[2]State University of Maritime and Inland Shipping,
St. Petersburg, 198035, Russian Federation

Article info
The article was received 09 June 2019

For citation: Voronin S., Doroshenko V., Ksenofontov Y. Radiochannels of Meteor-Burst Communication Network of the Northern Sea Route. *Proceedings of Telecommunication Universities*. 2019;5(3):13–18. (in Russ.) Available from: https://doi.org/10.31854/1813-324X-2019-5-3-13-18

Abstract: *The aim of this article is to justify the usefulness of meteor communication network usage as a telecommunication basis on the access connectivity network for Vessel traffic management on their way to the Arctic Russian infrastructure in the coastal zone of the northern sea route. It represent us the main options, from the point of view of system analysis, which characterise the telecommunication technologies of meteor connection, structural-functional scheme, generalized mathematical model of the network consisting of the radiotransmitter and receiver including antenna systems. It is represented the usage of adaptive antenna grids as UHF antenna systems.*

Keywords: *radioline meteor communication, structural and functional scheme, adaptive antenna grids, coefficient of using radio channel transmitting capability, multi ray distribution.*

References

1. Doroshenko V.I., Stratonova O.N., Pivovarova A.K. Meteornaia sviaz v raionakh Krainego Severa Rossii [Meteor Communication in the Far North of Russia]. *Materialy IV Mezhvuzovskoi nauchno-prakticheskoi konferentsii aspirantov studentov i kursantov "Sovremennye tendentsii i perspektivy razvitiia vodnogo transporta Rossii", 14 May 2015, St. Peterburg, Rossia* [Proceedings of the IV Interuniversity Scientific-Practical Conference of Graduate Students, Students and Cadets "Current Trends and Prospects for the Development of Water Transport in Russia",14 May 2015, St. Petersburg, Russia]. St. Petersburg: Admiral Makarov State University of Maritime and Inland Shipping Publ.; 2015. p.31–33. (in Russ.)

2. Kapralov D., Kirik D. Stochastic Model of Meteor-Burst Radio Channel. *Proceedings of Telecommunication Universities*. 2018;4(3):54–64. (in Russ.) Available from: https://doi.org/10.31854/1813-324X-2018-4-3-54-64

3. Doroshenko V.I., Ksenofontov Y.G. Application of Meteor Communication in the Security Systems of the Northern Sea Route Infrastructure Objects. *Military Enginery. Scientific and Technical Journal. Counter-terrorism technical devices. Issue 16.* 2019;1-2(127-128):3–11. (in Russ.)

4. Titkov S.B. Tekhnicheskie predlozheniia po ispolzovaniiu meteornoi sviazi [Technical Proposals for the Use of Meteor Communication]. *Zašita informacii. Inside*. 2006;3(9):74–80. (in Russ.)

5. Ryabov I.V., Tolmachev S.V., Lebedeva A.A. Principles of Software-Based Radiosystems and its Application within the Framework of Meteor-Burst Communication Investigation. *Sovremennye naukoemkie tekhnologii*. 2016;7-1:59–66. (in Russ.)

6. Strugov I.F., Semenov A.M., Dobrovolskii S.M., Batyrev I.A. Stokhasticheskoe modelirovanie kanalov s additivnymi i multiplikativnymi pomekhami. Skhema realizatsii [Stochastic modeling of channels with additive and multiplicative noise. Implementation scheme]. *Mathematical Structures and Modeling*. 2015;2(34):48–63. (in Russ.)

7. Kachnov A., Penkin A.A., Rybakov A. The Development of Mobile Information Provision Systems Using Meteor Communication Channels. *Proceedings of the* Vth *International Conference on Infotelecommunications in Science and Education, 1–11 March 2016, St. Petersburg, Russia*. St. Petersburg: The Bonch-Bruevich Saint-Petersburg State University of Telecommunications Publ.; 2016. p.177–181. (in Russ.)

8. Blagov D.S., Volvenko S.V. Increase of speed of information transfer in meteor-burst communication systems by use of signals of variable duration. *St. Petersburg State Polytechnical University Journal. Computer Science. Telecommunication and Control Systems*. 2010;5(108):7–13. (in Russ.)

9. Belokopytov A.E. The choice of an effective form of digital modulation in the radio communication systems according to the criteria of efficiency. *Science Almanac*. 2015;11-3(13):35–38. (in Russ.) Available from: https://doi.org/10.17117/na.2015.11.03.035

10. Ryabov I.V., Tolmachev S.V., Lebedeva A.A. Hardware and software package for meteor trails detection having variable bandwidth. *RTS Journal*. 2016;4(24):66–75. (in Russ.)

11. Petrov V.P. Spatial spectrum analysis algorithms in adaptive digital arrays. *Vestnik SibGUTI.* 2014;4:60–70. (in Russ.)

МАТЕМАТИЧЕСКИЕ МОДЕЛИ ОЦЕНКИ СКРЫТНОСТИ СПУТНИКОВЫХ КАНАЛОВ РАДИОСВЯЗИ С БЕСПИЛОТНЫМИ ЛЕТАТЕЛЬНЫМИ АППАРАТАМИ. ЧАСТЬ 1

А.Т. Егоров[1], **А.А. Ломакин**[1], **Д.Г. Пантенков**[1*]

[1]АО «Кронштадт»,
Москва, 115432, Российская Федерация
*Адрес для переписки: pantenkov88@mail.ru

Информация о статье
УДК 621.399
Статья поступила в редакцию 18.04.2019

Ссылка для цитирования: Егоров А.Т., Ломакин А.А., Пантенков Д.Г. Математические модели оценки скрытности спутниковых каналов радиосвязи с беспилотными летательными аппаратами. Часть 1 // Труды учебных заведений связи. 2019. Т. 5. № 3. С. 19–26. DOI:10.31854/1813-324X-2019-5-3-19-26

Аннотация: *В настоящее время спутниковая радиосвязь является основным видом радиосвязи применительно к большинству подвижных объектов специального назначения, в том числе к беспилотным летательным аппаратам (БЛА) тяжелого и сверхтяжелого классов большой продолжительности полета, которые при выполнении поставленных целевых задач вынуждены перемещаться относительно места взлета (аэродрома) на значительные расстояния (до нескольких тысяч километров). При этом актуальным становится вопрос качества канала спутниковой линии радиосвязи на всем ее участке между передающим и приемным устройствами, в том числе обеспечения помехозащищенности и скрытности передачи командно-телеметрической и целевой информации. Одновременно необходимо учесть возможность использования средств радиомониторинга спутникового канала радиосвязи, что может привести к перехвату канала управления или доступу к целевой информации от полезных нагрузок БЛА. В данной статье, состоящей из двух частей, рассмотрены способы повышения эффективности передаваемой информации по спутниковым каналам радиосвязи между БЛА и наземным пунктом управления и обработки информации, а также противодействия средствам радиомониторинга, сформулированы предложения и рекомендации по повышению скрытности спутниковых каналов передачи данных.*

Ключевые слова: *комплексы с беспилотными летательными аппаратами, система спутниковой радиосвязи, космический аппарат, повышение эффективности функционирования, средства радиомониторинга, математическое моделирование, помехозащищенность, скрытность спутниковой радиолинии, сигнально-энергетические параметры.*

Введение

В настоящее время в РФ активно развивается беспилотная авиация в интересах различных Заказчиков: по состоянию на 2019 год отечественной промышленностью разработан типоряд комплексов с беспилотными летательными аппаратами (БЛА) различного класса и целевого назначения – легкие («Типчак», «Zala 421-04М», «Элерон-3»), средние («Элерон-10», «Форпост», «Корсар»), тяжелые («Орион»), сверхтяжелые («Альтаир», «Охотник»), которые решают как задачи повышения обороноспособности и безопасности РФ, так и отвечают интересам гражданских потребителей. Одним из ключевых элементов комплексов с БЛА является радиолиния с использованием космических аппаратов (КА) на различных орбитах (загоризонтная радиосвязь), что позволяет существенно повысить эффективность применения комплексов с БЛА при решении поставленных целевых задач за счет увеличения радиуса его действия [1–16].

В данной статье представлены методы пространственной избирательности и сигнальной обработки при передаче полезной (целевой) информации между БЛА и земными станциями спутниковой связи (ЗС СпС) из состава наземного пункта управления и обработки информации, проведена оценка влияния этих методов обеспечения скрытности на эффективность функционирования системы СпС и

средств радиомониторинга (РМ). Следует отметить, что в целях упрощения (но без ущерба для понимания) в статье сделано допущение, что скрытность несимметричного дуплексного канала спутниковой радиосвязи БЛА учитывает только сигнально-энергетические параметры сигнально-кодовых конструкций, без учета типа и параметров кодирования.

Известен ряд работ по данной или смежной тематикам [17–19], в которых рассматриваются вопросы помехозащищенности спутниковых систем связи и навигации, приведены оценки влияния широкополосных заградительных, узкополосных и сосредоточенных по спектру помех на эти системы, уделено значительное внимание вопросам помехоустойчивого кодирования. При этом не в полной мере рассматриваются вопросы оптимальной обработки сигналов – согласованной фильтрации и корреляционной обработки, что гипотетически позволяет существенным образом повысить отношение сигнал/шум на входе приемника, а также не учитывается возможность постановки помех по боковому и заднему лепестку диаграммы направленности полезного сигнала.

1. Общая постановка задачи разработки модели системы спутниковой связи, обеспечивающая ее скрытное функционирование от средств радиомониторинга

С математической точки зрения функционирование такой системы можно рассматривать как взаимодействие двух антагонистических систем. Целью непосредственно самой системы СпС является обеспечение заданного качества передаваемой информации от БЛА/земной станции на КА-ретранслятор и от КА-ретранслятора на земную станцию/БЛА при условии скрытности ее передачи от средств РМ. В свою очередь, целью системы РМ является обнаружение сигналов спутниковой связи [7–8]. В самом общем виде функционирование системы СпС, скрытой от системы РМ [1–6], представлено на рисунке 1.

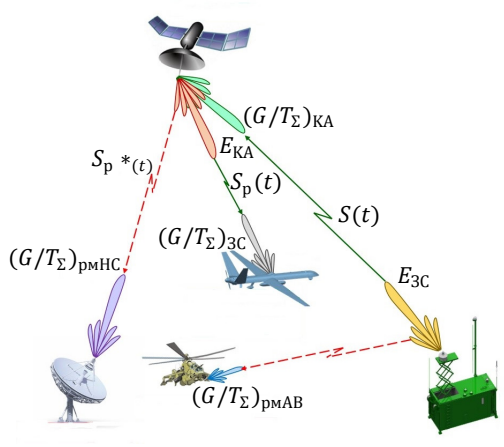


Рис. 1. Функционирование системы СпС, обеспечивающей скрытую передачу сигналов от системы радиомониторинга

На практике качество передачи информации в системах радиосвязи оценивается вероятностью ошибочного приема элементарной посылки (или кодовой комбинации) [5]:

$$P_{ош} = f\left(q_{вх\,сс}, \vec{W}\right), \quad (1)$$

где $q_{вх\,сс}$ – отношение мощности принимаемого сигнала к мощности шумов на входе приемной системы (далее по тексту – $q_{вх}$) ЗС; $\vec{W}$ – вектор параметров принимаемого сигнала СпС, включая параметры модуляции (демодуляции) и кодирования (декодирования).

Для системы РМ одной из основных задач является обнаружение сигналов от объектов мониторинга. При этом эффективность ее решения определяется вероятностью обнаружения сигнала [3, 5]:

$$P_{обн} = f(P_{лт}, q_{вх\,РМ}, M_s), \quad (2)$$

где $P_{лт}$ – вероятность ложной тревоги, которая при решении задачи энергетического обнаружения сигнала определяет порог обнаружения; M_s – параметр, определяющий модель обнаруживаемого сигнала на входе обнаружителя (сигнал со случайной начальной фазой или сигнал со случайной амплитудой и начальной фазой); $q_{вх\,РМ}$ – $q_{вх}$ для РМ:

$$q_{вх\,РМ} = \frac{P_{с\ вх\ РМ}}{P_{ш\ РМ}}.$$

Одним из параметров, определяющих эффективность задач как приема связного сигнала, так и РМ, является вышеобозначенное $q_{вх}$ [7–10]:

$$q_{вх\,СС} = \frac{P_{с\ вх\ ЗС}}{P_{ш\ пр}}, \quad (3)$$

где $P_{с\ вх\ ЗС}$ – мощность принимаемого сигнала на входе приемной системы; $P_{ш\ пр}$ – мощность шумов приемной системы.

При этом в общем случае мощность сигнала на входе приемной системы $P_{с\ вх\ ЗС(КА)}$ ЗС или КА, наземной или авиационной станции РМ, является функцией от целого ряда факторов:

$$P_{с\ вх\ ЗС} = f\left(E(\alpha,\beta), G_{пр}, L_\Sigma\right) \quad (4)$$

где $E(\alpha,\beta)$ – эквивалентная изотропная мощность, излучаемая источником связного сигнала ЗС или КА-ретранслятором в направлении (α,β) на ЗС или на КА, на наземную или авиационную станции РМ; $G_{пр}$ – коэффициент усиления приемной антенны ЗС или КА, авиационной или наземной станции РМ); L_Σ – суммарные потери сигнала на трассе распространения «ЗС-КА» или «КА-ЗС», «ЗС-АВ РМ» (авиационная станция радиомониторинга) или «КА-НС РМ» (наземная станция радиомониторинга).

Мощность шумов на входе приемной системы в общем случае определяется по формуле [7–10]:

$$P_{ш\ пр} = k_Б \cdot T_{\Sigma\,Ш} \cdot \Delta F_{пр}, \quad (5)$$

где $k_Б$ – постоянная Больцмана, равная $1{,}38 \cdot 10^{-23}$ (Дж/К); $T_{\Sigma Ш}$ – суммарная шумовая температура приемной системы ЗС или КА, наземной или авиационной станции РМ, включая шумы антенны и входного приемного тракта (К); $\Delta F_{пр}$ – полоса пропускания приемного тракта (Гц).

Известно, что основная задача при проектировании любой системы связи заключается в синтезе (обосновании и выборе) параметров связного сигнала, методов его обработки, определении параметров приемного и передающего трактов, при которых обеспечивается качество передачи информации не хуже заданного $(P_{ош} \le P_{ош\ тр})$. Очевидно, что для выполнения этого условия мощность связного сигнала на входе приемной системы должна быть максимально большой.

С другой стороны, в условиях ведения РМ за средствами СпС необходимо обеспечить вероятность обнаружения сигнала станцией РМ не больше заданной величины $(P_{обн} \le P_{обн\ зад})$. При этом, мощность связного сигнала на входе приемной системы наземной станции РМ должна быть минимальной [7–10].

В данной ситуации при одном источнике излучения связного сигнала наблюдается противоречие в требованиях к мощности связного сигнала, которая для обеспечения качественной связи должна быть максимально большой на входе ЗС СпС, а в интересах обеспечения скрытности от средств мониторинга – минимальной на входе наземной станции РМ.

Анализ известных методов разрешения такого рода противоречий показывает, что решение задачи синтеза применительно к рассматриваемой ситуации возможно за счет применения метода пространственной избирательности и метода сигнальной обработки [4–11]. Далее проведем оценку влияния этих методов обеспечения скрытности на эффективность функционирования системы СпС и средств РМ.

2. Оценка эффективности мер обеспечения пространственной избирательности при организации линий спутниковой связи на скрытность их функционирования от средств радиомониторинга

Косвенными показателями эффективности функционирования системы СпС и средств РМ является отношение мощностей связного сигнала и шумов на входе приемных систем станций СпС и средств РМ соответственно [9–14], которые определяются на основе энергетических расчетов линий:

– при обеспечении связи на направлениях «КА-ЗС» и «ЗС-КА»;

– при ведении РМ на направлениях «КА-СРМ» (средство радиомониторинга) и «ЗС-СРМ».

Проведение энергетических расчетов этих линий основано на применении уравнения радиосвязи.

Отношение мощности связного сигнала к мощности шумов на входе приемной системы ЗС или КА определяется по формуле [5,6]:

$$\left(\frac{P_С}{P_Ш}\right) = \frac{P_{пер\ КА(ЗС)} \cdot G_{пер\ КА(ЗС)} \cdot \eta_{пер\ КА(ЗС)}}{L_{\Sigma\ ЗС-КА} \cdot k_Б} \times \times \frac{G_{пр\ ЗС(КА)} \cdot \eta_{пр\ ЗС(КА)}}{T_{\Sigma\ Ш\ ЗС(КА)} \cdot \Delta F_{пр\ ЗС(КА)}}, \quad (6)$$

где $P_{пер\ КА(ЗС)}$ – выходная мощность передатчика КА или ЗС соответственно (Вт); $G_{пер\ КА(ЗС)}$ – коэффициент усиления передающей антенны (раз); $\eta_{пер\ КА(ЗС)}$ – коэффициент передачи по мощности волноводного (фидерного) тракта передающей системы (раз); $G_{пр\ ЗС(КА)}$ – коэффициент усиления приемной антенны (раз); $\eta_{пр\ ЗС(КА)}$ – коэффициент приема по мощности волноводного (фидерного) тракта приемной системы (раз); $L_{\Sigma\ ЗС-КА}$ – суммарные потери на трассе распространения «ЗС-КА» (раз); $T_{\Sigma\ Ш\ ЗС(КА)}$ – суммарная шумовая температура приемной системы (К°); $\Delta F_{пр\ ЗС(КА)}$ – полоса пропускания приемной системы (Гц).

Выражение (6) получено для линии СпС при выполнении следующих условий:

– приемная и передающая антенные системы наведены друг на друга по максимуму принимаемого сигнала;

– поляризация приемной и передающей антенн совпадают;

– полоса пропускания приемной системы согласована со спектром принимаемого сигнала.

В большинстве случаев средства РМ располагаются вне зоны освещенности главного лепестка передающей антенны наблюдаемого средства связи. В этом случае прием связного сигнала средствами РМ возможен по боковым лепесткам диаграммы направленности передающей антенны источника сигнала, что приводит к его ослаблению относительно усиления в главном лепестке.

Отношение мощности связного сигнала к мощности шумов на входе приемной системы средства РМ наземного или воздушного базирования определяется по формуле:

$$\left(\frac{P_С}{P_Ш}\right)_{вх\ НСрм(АСрм)} = \frac{P_{пер\ КА(ЗС)} \cdot G_{КА-ЗС} \cdot \eta_{пер\ КА(ЗС)}}{L_{\Sigma\ КА-НСрм(ЗС-АСрм)} \cdot k_Б} \times \times \frac{G_{пр\ НСрм(АСрм)} \cdot \eta_{пр\ НСрм(АСрм)} \cdot k_{пол}}{T_{\Sigma\ Ш\ НСрм(АСрм)} \cdot \Delta F_{пр\ НСрм(АСрм)}}, \quad (7)$$

где $G_{КА-ЗС}$ – коэффициент усиления по боковым и задним лепесткам диаграммы направленности передающей антенны КА или ЗС соответственно в направлении средства РМ (раз); $G_{пр\ НСрм(АСрм)}$ – коэффициент усиления приемной антенны наземной станции (НСрм) или авиационного средства РМ

(АСрм) соответственно (раз); $\eta_{\text{пр НСрм(АСрм)}}$ – коэффициент передачи по мощности волноводного (фидерного) тракта приемной системы (раз); $k_{\text{пол}}$ – коэффициент, учитывающий различие поляризаций передающей и приемной антенн (раз); $L_{\Sigma\ \text{КА–НСрм(ЗС–АСрм)}}$ – суммарные потери на трассе распространения «КА-НСрм» или «ЗС-АСрм» (раз); $T_{\Sigma\ \text{Ш НСрм(АСрм)}}$ – суммарная шумовая температура приемной системы (К°); $\Delta F_{\text{пр НСрм(АСрм)}}$ – полоса пропускания приемной системы (Гц).

Анализ выражений (1–7) показывает, что повышение скрытности линий СпС, при условии обеспечения требуемого уровня эффективности функционирования системы связи, возможно за счет увеличения:

– коэффициента усиления передающей антенны при одновременном уменьшении уровня ее излучений по боковым и задним лепесткам;

– коэффициента усиления приемной антенны;

– ширины спектра связного сигнала (полосы пропускания приемной системы).

Для реализации мер пространственной селекции на практике, как на приемной, так и на передающей стороне, применяются антенные системы с узкой диаграммой направленности (ДН), которые имеют большой коэффициент усиления и низкий уровень излучения в направлении боковых и задних лепестков.

Выигрыш в скрытности линии СпС от принятия в этих системах узконаправленных антенн можно оценить с помощью энергетического показателя $h_{\text{пи}} = \frac{P_{\text{с мпи}}}{P_{\text{с ompи}}}$ при выполнении следующих условий: $\left(\frac{P_\text{с}}{P_\text{ш}}\right)_{\text{вх зс(КА)}} \geq \left(\frac{P_\text{с}}{P_\text{ш}}\right)_{\text{вх зс(КА) тр}}, \left(\frac{P_\text{с}}{P_\text{ш}}\right)_{\text{вх СРМ}} \leq \left(\frac{P_\text{с}}{P_\text{ш}}\right)_{\text{вх СРМ тр}}$.

Параметром, определяющим уровень боковых и задних лепестков ДН антенной системы, является направление (угол) прихода (излучения) сигнала (Θ). Зависимость нормированной ДН антенной системы от угла относительно направления максимума для фиксированных значений частоты (f = 36,75 ГГц) и диаметра антенны ($D_\text{А}$ = 0,435 м), соответствующих коэффициенту усиления антенны равному 42,27 дБ, приведены на рисунке 2.

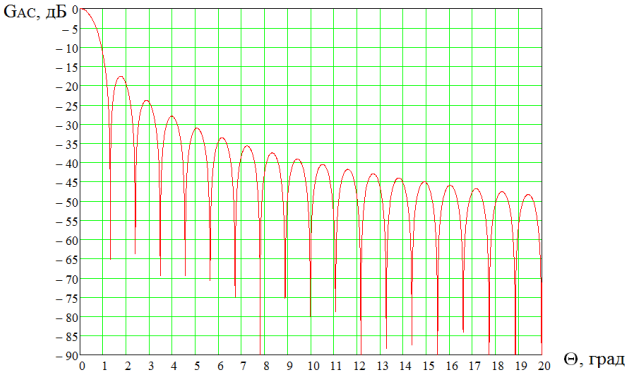


Рис. 2. Зависимость нормированной ДН антенной системы от угла относительно направления максимума

Кроме того, на практике, до начала ведения мониторинга точное местоположение источника связного сигнала для средств, осуществляющих РМ, неизвестно. Для устранения этой неопределенности в средствах РМ либо применяются антенные системы с относительно широкой ДН, либо применяются узконаправленные антенные системы, но дополнительно осуществляется поиск сигналов по пространству. В первом случае снижается мощность сигнала РМ, а во втором – увеличивается время ведения РМ за счет поиска сигналов по пространству. В результате в обоих случаях снижается эффективность решения задачи РМ, что в конечном итоге также позволяет разрешить имеющееся противоречие.

3. Модель функционирования системы спутниковой связи с применением методов сигнальной обработки для обеспечения скрытности ее функционирования от средств радиомониторинга

В большинстве практических случаев, если к системе СпС не предъявляются особые требования, то для организации связи в основном применяются простые сигналы, у которых база равна единице. Среди всего множества простых сигналов в системах СпС наиболее широко применяются сигналы с двукратной фазовой манипуляцией (BPSK, *от англ.* Binary Phase-Shift Keying) и с четырехкратной фазовой манипуляцией (QPSK, *от англ.* Quadrature Phase-Shift Keying), которые обладают хорошей помехоустойчивостью (эффективностью, оцениваемой вероятностью ошибочного приема на бит информации). На рисунке 3 представлены зависимости вероятности ошибочного приема от отношения мощности сигнала к мощности шумов на входе демодуляторов сигналов BPSK и QPSK, а также требуемое для большинства систем связи значение вероятности ошибки при передаче данных [10, 11, 14].

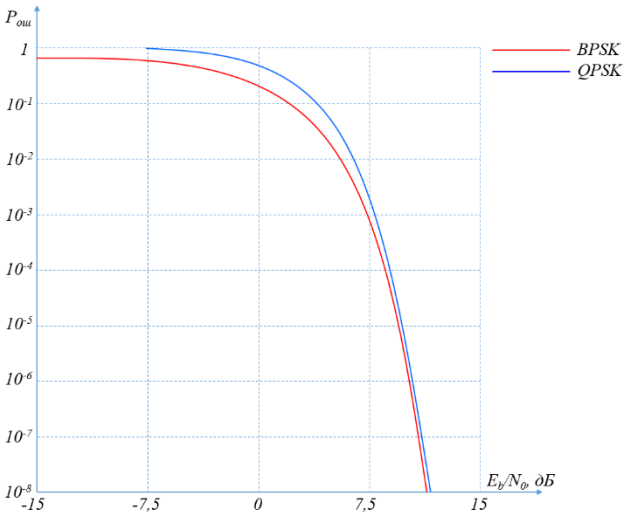


Рис. 3. Зависимости вероятности ошибочного приема от отношения мощности сигнала к мощности шумов на входе демодуляторов сигналов BPSK и QPSK

Анализ представленных зависимостей (см. рисунок 3) показывает, что для обеспечения требуемой вероятности ошибочного приема 10^{-6} пороговое отношение мощности сигнала к мощности шумов на входе демодуляторов сигналов BPSK и QPSK должно составлять порядка 11 дБ. Для обеспечения такого отношения необходимо иметь большую мощность излучения связного сигнала, что ведет к снижению скрытности радиосвязи.

Применение только мер пространственной избирательности для обеспечения скрытности функционирования системы СпС от средств РМ обычно недостаточно, поэтому на практике дополнительно применяются методы помехоустойчивого кодирования и последующего декодирования связных сигналов. Однако эти методы имеют ряд ограничений и обеспечивают незначительное снижение порогового отношения мощности сигнала к мощности шумов на входе демодуляторов (до 5–7 дБ).

Другим способом повышения эффективности обеспечения скрытности является применение методов сигнальной обработки. Эти методы основаны на применении в системах связи сложных сигналов в сочетании с их оптимальной обработкой при приеме, что позволяет увеличить отношение мощности сигнала к мощности шумов на входе демодулятора сигналов приемного тракта ЗС или КА-ретранслятора. В результате этого расширяется спектр излучаемого связного сигнала и одновременно появляется возможность снижения уровня излучаемой мощности связного сигнала без ухудшения качества принимаемого сигнала в соответствующей линии радиосвязи, но при этом уменьшается отношение сигнал/шум в приемной системе средства РМ.

С другой стороны, в средствах РМ для увеличения отношения мощности сигнала к мощности шумов на входе обнаружителя также могут применяться квазиоптимальные методы предварительной обработки сигналов (некогерентное накопление сигналов или авто-/взаимокорреляционная обработка сигналов). Применение методов оптимальной обработки сигналов по сравнению с квазиоптимальными при ограниченной длительности излучения сигнала источником позволяет получить значительно больший выигрыш в отношении мощности сигнала к мощности шумов. В средствах РМ применение методов оптимальной обработки сигналов ограничено отсутствием информации о несущей частоте, параметрах и структуре принимаемых сигналов, в то время как средства связи располагают такой информацией и имеется возможность синхронизации сигналов на передающем и приемном концах линии радиосвязи. Тем самым, обеспечивается скрытность функционирования системы СпС от средств РМ.

На практике для реализации в полной мере требований по скрытности функционирования системы СпС, как правило, необходимо одновременно применять как меры пространственной избирательности, так и методы оптимальной обработки сигналов.

Для повышения скрытности передачи информации в радиолиниях в качестве мер сигнальной обработки применяются сложные широкополосные сигналы (ШПС), расширяющие спектр информационного сигнала. В качестве ШПС, обеспечивающих скрытность передачи информации, могут применяться следующие их типы:

– фазоманипулированные (ФМн) сигналы, предварительно модулированных расширяющей спектр кодовой последовательностью (ФМн-ШПС);

– сигналы с программной перестройкой рабочей частоты (ППРЧ);

– комбинированные сигналы ФМн-ШПС с ППРЧ.

С позиции обеспечения скрытности передачи информации, наиболее предпочтительным является применение сигналов типа ФМн-ШПС.

Шумоподобными сигналами называются такие сигналы, у которых база сигналов (B) много больше единицы. База сигнала характеризует расширение спектра ШПС относительно спектра информационного сигнала (сообщения) и равна:

$$B = \Delta F_c \cdot T_{\text{ип}} = \frac{\Delta F_c}{V_{\text{и}}} = \frac{T_{\text{ип}}}{\tau_{\text{э}}} \gg 1, \qquad (9)$$

где ΔF_c – ширина спектра ШПС; $\tau_{\text{э}}$ – длительность элементарной посылки ШПС; $T_{\text{пи}}$ – длительность посылки информационного сигнала; $V_{\text{и}}$ – скорость передачи информации.

При приеме ФМн-ШПС наибольший выигрыш в отношении сигнал/шум на выходе ($q_{\text{вых}}$) по отношению ко входу ($\rho_{\text{вх}}$) обеспечивают устройства, реализующие методы оптимального приема (оптимальные приемники сигналов) [3, 4]. В качестве оптимальных приемников применяются метод согласованной фильтрации и метод оптимального корреляционного приема. Структуры устройств, реализующих методы оптимального приема ФМн-ШПС [2], представлены на рисунке 4.

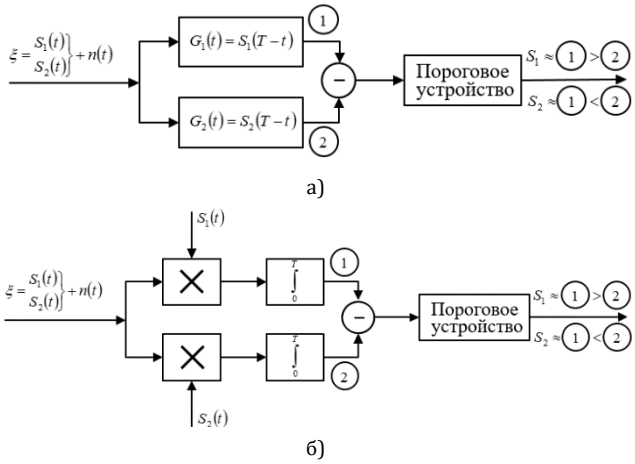


Рис. 4. Структуры устройств, реализующих оптимальные методы согласованной фильтрации (а) и оптимального корреляционного приема сигналов (б)

Указанные методы оптимального приема различаются технической реализацией и обеспечивают одинаковый выигрыш в отношении мощности сигнал/шум на выходе ($q_{вых}$) по отношению к мощности сигнал/шум на входе ($\rho_{вх}$), который равен базе ШПС:

$$B = \frac{\rho_{вх}}{q_{вых}}. \quad (10)$$

Одним из основных показателей эффективности приема информации при передаче дискретных сигналов является вероятность ошибочного приема на бит передаваемой информации ($P_{ош}$), которая при оптимальном приеме ФМн-ШПС определяется соотношением [3, 6]:

$$P_{ош} = 1 - \Phi\left(\sqrt{2 \cdot \rho \cdot \frac{T_{ип}}{\tau_э}}\right), \quad (11)$$

где $\Phi(x)$ – интеграл вероятности, который рассчитывается по выражению:

$$\Phi(x) = \frac{1}{\sqrt{2 \cdot \pi}} \times \int_{-\infty}^{x} exp\left(\frac{-z^2}{2}\right) dz\,.$$

На основе данного соотношения получены зависимости вероятности ошибочного приема ФМн-ШПС от отношения мощности сигнала к мощности шума на входе приемной системы для фиксированных значений базы сигнала, которые приведены на рисунке 5.

На рисунке 5 представлены указанные зависимости для значений базы сигнала B, равной 20, 30 и 40 дБ.

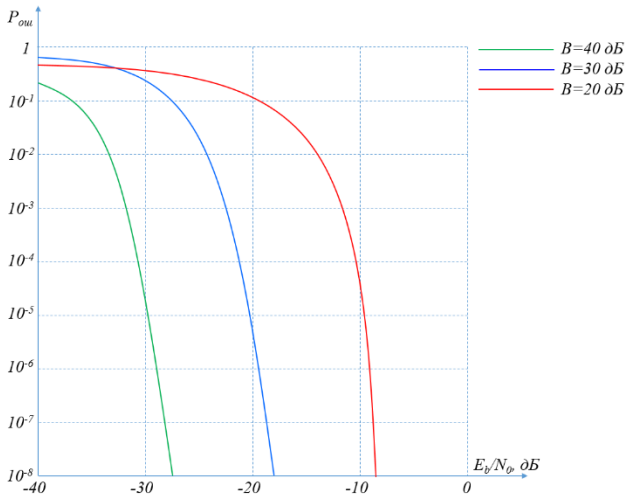


Рис. 5. Зависимости вероятности ошибочного приема от отношения мощности сигнал/шум на входе приемной системы

Анализ приведенных зависимостей (см. рисунок 5) показывает, что даже при отрицательных отношениях мощности сигнала к мощности шума на входе приемной системы (менее единицы) можно обеспечить эффективный прием связного сигнала, так как это отношение линейным образом зависит от мощности связного сигнала, излучаемой источником (КА или ЗС). Тогда, увеличив базу связного сигнала, можно обеспечить его эффективный прием при пониженной мощности излучения, но при этом уменьшится отношение мощности сигнала к мощности шума на входе приемной системы средств РМ и его эффективное обнаружение становится невозможным.

В качестве другого типа сложных сигналов для организации связи применяются сигналы с ППРЧ. При этом скрытность связи достигается за счет того, что сигнал на одной частотной позиции излучается ограниченной длительности, а смена частотных позиций происходит по псевдослучайному закону, который известен на передающем и приемном концах линии связи, но неизвестен средствам РМ. При наличии ограничений на длительность излучения сигнала осуществление его РМ становится невозможным.

Заключение

На основе проведенного анализа функционирования системы СпС в условиях противодействия средствам РМ можно сформировать следующие предложения и рекомендации по обеспечению скрытности спутникового канала радиосвязи с БЛА.

Во-первых, максимально использовать пространственную скрытность КА.

Во-вторых, минимизировать ширину ДН и мощность излучения связного сигнала за счет увеличения добротности приемного тракта средства ЗС СпС. Кроме того, в процессе функционирования системы необходимо адаптивно изменять мощность излучения сигнала в зависимости от складывающейся радиоэлектронной обстановки (потерь в атмосфере, скорости передачи информации, мест дислокации средств РМ и другой информации о средствах РМ).

И в-третьих, использовать в средствах спутниковой радиосвязи сигнально-кодовые конструкции с минимальными пороговыми значениями отношения энергии бита к спектральной плотности мощности шума в сочетании с методами оптимальной обработки сигналов (корреляционная обработка и согласованная фильтрация).

Список используемых источников

1. Тюлин А.Е., Бетанов В.В., Ларин В.К. Информационное обеспечение управления космическими аппаратами. Системный подход к решению задач. М.: Радиотехника, 2019. 272 с. DOI:10.18127/B9785931081854

2. Тестоедов Н.А., Косенко В.Е., Выгонский Ю.Г., Кузовников А.В., Мухин В.А., Чеботарев В.Е. и др. Космические системы ретрансляции. М.: Радиотехника, 2017. 448 с.

3. Бузов А.Л., Букашкин С.А. Специальная радиосвязь. Развитие и модернизация оборудования и объектов. М.: Радиотехника, 2017. 448 с.
4. Кузовников А.В. и др. Современные технологии радиомониторинга в спутниковых системах связи и ретрансляции. М.: Радиотехника, 2015. 214 с.
5. Журавлев В.И., Руднев А.Н. Цифровая фазовая модуляция. М.: Радиотехника, 2012. 208 с.
6. Немировский М.С., Локшин Б.А., Аронов Д.А. Основы построения систем спутниковой связи. М.: Горячая линия – Телеком, 2017. 432 с.
7. Пантенков Д.Г., Литвиненко В.П. Компьютерное моделирование передачи полезной информации в спутниковых радиолиниях при многолучевой связи // Вестник Воронежского государственного технического университета. 2013. Т. 9. № 3-1. С. 127–131.
8. Великоиваненко В.И., Гусаков Н.В., Донченко П.В., Ломакин А.А., Пантенков Д.Г., Соколов В.М. Система спутниковой связи с последовательным зональным обслуживанием // Космонавтика и ракетостроение. 2014. № 2(75). С. 48–56.
9. Литвиненко В.П., Глушков А.Н., Пантенков Д.Г. Некогерентный цифровой демодулятор «в целом» кодированных сигналов с фазовой манипуляцией. Патент на изобретение RUS 2556429 от 14.07.2014. Опубл. 10.07.2015. Бюл. № 19.
10. Вейко А.В., Великоиваненко В.И., Ломакин А.А. и др. Методический подход оценки компенсации доплеровского смещения частоты в спутниковых линиях информационного обмена при эксплуатации космических систем связи // Проблемные вопросы развития наземных комплексов, стартового оборудования и эксплуатации летательных аппаратов. 2018. № 13. С. 289–297.
11. Иванкин Е.Ф. Информационные системы с апостериорной обработкой результатов наблюдений. М.: Горячая линия – Телеком, 2008. 168 с.
12. Лепин В.Н. Помехозащита радиоэлектронных систем управления летательными аппаратами и оружием. М.: Радиотехника, 2017. 416 с.
13. Рудой В.М. Системы передачи информации: учебное пособие. М.: Радиотехника, 2007. 280 с.
14. Ярлыкова М.С. Марковская теория оценивания в радиотехнике. М.: Радиотехника, 2004. 505 с.
15. Шелухин О.И., Тенякшев А.М., Осин А.В. Моделирование информационных систем. М.: Радиотехника, 2005. 368 с.
16. Верба В.С., Татарский Б.Г. Комплексы с беспилотными летательными аппаратами. В 2-х книгах. М.: Радиотехника, 2016. 1352 с.
17. Дворников С.В., Духовницкий О.Г. Оценка помехозащищенности профессионального радионавигационного оборудования системы Глонасс // Информация и космос. 2015. № 4. С. 73–77.
18. Агиевич С.Н., Луценко С.А. Оценка помехоустойчивости спутниковых систем радиосвязи с фазоманипулированными широкополосными сигналами // Вопросы оборонной техники. Серия 16: Технические вопросы противодействия терроризму. 2018. № 123-124. С. 132–137.
19. Чипига А.Ф., Пашинцев В.П. Повышение энергетической скрытности систем спутниковой связи при близком размещении приемника радиоперехвата // Нелинейный мир. 2013. Т. 11. № 9. С. 659–671.

* * *

MATHEMATICAL MODEL OF SATELLITE COMMUNICATION SYSTEMS WITH UNMANNED AERIAL VEHICLES AND COUNTER-MEANS OF RADIO CONTROL. PART 1

A. Egorov[1], A. Lomakin[1], D. Pantenkov[1]

[1]JSC Kronstadt,
Moscow, 115432, Russian Federation

Article info
The article was received 18 April 2019

For citation: Egorov A., Lomakin A., Pantenkov D. Mathematical Models of Satellite Communication Systems with Unmanned Aerial Vehicles and Counter-Means of Radio Control. Part 1. *Proceedings of Telecommunication Universi-ties*. 2019;5(3):19–26. (in Russ.) Available from: https://doi.org/10.31854/1813-324X-2019-5-3-19-26

Abstract: *Currently, satellite radio communication is the main type of radio communication related to the majority of special purpose mobile objects, including unmanned aerial vehicles (UAV) of heavy and super heavy classes of long flight duration, which are forced to move over long distances up to several thousand kilometers from the take of place (airport). In this point we face the problem of quality of the channel of the satellite radio communication line on its*

entire way between the transmitting and receiving devices, including providing the interference protection, stealth and secrecy of transmission of command telemetry and target information. At the same time, it is necessary to take into account the possibility of using the means of radio control of a satellite radio channel from an eventual enemy, which can lead to the interception of the control channel or access to target information from the payloads of UAV. In this scientific and technical article, which consists of two parts, considered the issues of improving the efficiency of transmitted information via satellite communication channels between the UAV and the ground control and information processing point, and the issue of countering the means of radio control of the eventual enemy, formulated proposals and recommendations.

Keywords: *complexes with unmanned aerial vehicles, satellite radio communication system, spacecraft, improving the efficiency of the unmanned aerial vehicle, radio monitoring tools, mathematical modeling, noise immunity, stealth satellite radio line, signal and energy parameters.*

References

1. Tiulin A.E., Betanov V.V., Larin V.K. *Informatsionnoe obespechenie upravleniia kosmicheskimi apparatami. Sistemnyi podkhod k resheniiu zadach* [Information Support for Spacecraft Control. A Systematic Approach to Solving Problems]. Moscow: Radiotekhnika Publ.; 2019. 272 p. (in Russ.) Available from: https://doi.org/10.18127/B9785931081854
2. Testoedov N.A., Kosenko V.E., Vygonskii Iu.G., Kuzovnikov A.V., Mukhin V.A., Chebotarev V.E., et al. *Kosmicheskie sistemy retransliatsii* [Space Relay Systems]. Moscow: Radiotekhnika Publ.; 2017. 448 p. (in Russ.)
3. Buzov A.L., Bukashkin S.A. *Spetsialnaia radiosviaz. Razvitie i modernizatsiia oborudovaniia i obieektov* [Special Radio Communication. Development and Modernization of Equipment and Facilities]. Moscow: Radiotekhnika Publ.; 2017. 448 p. (in Russ.)
4. Kuzovnikov A.V., et al. *Sovremennye tekhnologii radiomonitoringa v sputnikovykh sistemakh sviazi i retransliatsii* [Modern Technologies of Radio Monitoring in satellite Communication Systems and Relaying]. Moscow: Radiotekhnika Publ.; 2015. 214 p. (in Russ.)
5. Zhuravlev V.I., Rudnev A.N. *Tsifrovaia fazovaia moduliatsiia* [Digital Phase Modulation]. Moscow: Radiotekhnika Publ.; 2012. 208 p. (in Russ.)
6. Nemirovskii M.S., Lokshin B.A., Aronov D.A. *Osnovy postroeniia sistem sputnikovoi sviazi* [Basics of Building Satellite Communications Systems]. Moscow: Goriachaia Liniia – Telekom; 2017. 432 p. (in Russ.)
7. Pantenkov D.G., Litvinenko V.P. Computer modeling of the transmission of useful information in the satellite radio links with multipath communication. *Bulletin of Voronezh State Technical University*. 2013;9(63–1):127–131. (in Russ.)
8. Velikoivanenko V.I., Gusakov N.V., Donchenko P.V., Lomakin A.A., Pantenkov D.G., Sokolov V.M. Satellite Communication System with Consistent Zone Service. *Cosmonautics and Rocket Engineering*. 2014;2(75):48–56. (in Russ.)
9. Litvinenko V.P., Glushkov A.N., Pantenkov D.G. *Non-Coherent Digital Demodulator of "Integrally" Coded Phase-Shift Keyed Signals*. Patent RF, no. 2556429, 14.07.2014 (in Russ.)
10. Veiko V.A., Velikoivanenko V.I., Lomakin A.A., et al. Methodical approach of estimation of compensation of Doppler frequency offset in the satellite lines of information exchange in the operation of space communication systems. *Problems of development of ground complexes, starting equipment and operation of aircraft*. 2018;13:289–297. (in Russ.)
11. Ivankin E.F. *Informatsionnye sistemy s aposteriornoi obrabotkoi rezultatov nabliudenii* [Information Systems with a Posteriori Processing of Observation Results]. Moscow: Goriachaia Liniia – Telekom; 2008. 168 p. (in Russ.)
12. Lepin V.N. *Pomekhozashchita radioelektronnykh sistem upravleniia letatelnymi apparatami i oruzhiem* [Noise Protection of Radio Electronic Control Systems of Aircraft and Weapons]. Moscow: Radiotekhnika Publ.; 2017. 416 p. (in Russ.)
13. Rudoy V.M. *Sistemy peredachi informatsii uchebnoe posobie* [Information Transmission Systems: Textbook]. Moscow: Radiotekhnika Publ.; 2007. 280 p. (in Russ.)
14. Yarlukov M.S. *Markovskaia teoriia otsenivaniia v radiotekhnike* [Markov's Theory of Estimation in Radio Engineering]. Moscow: Radiotekhnika Publ.; 2004. 505 p. (in Russ.)
15. Shelukhin O.I., Teniakchev A.M., Osin A.V. *Modelirovanie informatsionnykh system* [Modeling of Information Systems]. Moscow: Radiotekhnika Publ.; 2005. 368 p. (in Russ.)
16. Verba V.S., Tatarsky B.G. *Kompleksy s bespilotnymi letatelnymi apparatami* [Complexes with Unmanned Aerial Vehicles in 2 Books]. Moscow: Radiotekhnika Publ.; 2016. 1352 p. (in Russ.)
17. Dvornikov S.V., Dukhovnitsky O.G. Otsenka pomekhozashchishchennosti professionalnogo radionavigatsionnogo oborudovaniia sistemy Glonass [The Estimation of Noise Immunity of Professional Navigation Equipment GLONASS]. Informatsiia i kosmos. 2015;4:73–77. (in Russ.)
18. Agievich S.N., Lutsenko S.A. Estimation of noise immunity of satellite radio communication systems with Phase-Manipulated Broadband Signals. *Military Enginery. Issue 16. Counter-terrorism technical devices*. 2018;123–124:132–137. (in Russ.)
19. Chipiga A.F., Pashintsev V.P. Increase of power reserve systems of satellite communication at close placement of the receiver of radio interception. *Nonlinear World*. 2013;11(9):659–671. (in Russ.)

ИССЛЕДОВАНИЕ И ГЕНЕРАЦИЯ ТРАФИКА ПРОМЫШЛЕННОГО ИНТЕРНЕТА ВЕЩЕЙ

Р.В. Киричек[1], **В.А. Кулик**[1*]

[1]Санкт-Петербургский государственный университет телекоммуникаций им. проф. М.А. Бонч-Бруевича, Санкт-Петербург, 193232, Российская Федерация
*Адрес для переписки: vslav.kulik@gmail.com

Информация о статье
УДК 654.027
Статья поступила в редакцию 10.07.2019

Ссылка для цитирования: Киричек Р.В., Кулик В.А. Исследование и генерация трафика промышленного Интернета Вещей // Труды учебных заведений связи. 2019. Т. 5. № 3. С. 27–36. DOI:10.31854/1813-324X-2019-5-3-27-36

Аннотация: *Данная работа посвящена исследованию трафика промышленного Интернета Вещей и разработке алгоритма для его генерации. На основе проведенного анализа предметной области был построен ряд его классификаций, с помощью которых были выбраны различные типовые приложения, устройства и системы, и на их основе разработана модельная сеть, имитирующая работу сетевой инфраструктуры промышленного предприятия в интересах проведения экспериментальных исследований трафика промышленного Интернета Вещей. Аналитические модели, полученные в ходе исследования, использовались для разработки алгоритма его генерации, результаты работы которого были сопоставлены с исходными аналитическими моделями.*

Ключевые слова: *промышленный Интернет Вещей, классификация, модельная сеть, исследование трафика, генерация трафика.*

Введение

Концепция Интернета Вещей, активно развивающаяся в последнее время, с каждым днем охватывает все большее число областей человеческой жизнедеятельности, таких как беспилотное управление транспортом [1–3], управление городской инфраструктурой [1, 4], контроль проведения медицинских операций [1, 5–6], автоматизация жилых помещений, офисов и др. С недавнего времени в рамках концепции Интернета Вещей развивается новое направление – промышленный Интернет Вещей (ПИВ) [7] – которое затрагивает вопросы создания гетерогенной интеллектуальной системы автоматизации работы промышленных предприятий.

В рамках ПИВ планируется провести автоматизацию работы промышленного оборудования, расчетов экономических показателей, обеспечения безопасности работников и пр. Основным отличием систем данного типа является их тесное взаимодействие с облачными и граничными технологиями и использование высокопроизводительных самообучающихся систем как для текущей оценки работы предприятия, так и для планирования его развития [8].

На основе вышесказанного, одной из актуальных проблем является интеграция решений ПИВ (далее по тексту – ПИВ-решения) в сетевую инфраструктуру промышленных предприятий [9] – для этого потребуется провести ее предварительное исследование на устойчивость к трафику ПИВ (далее по тексту – ПИВ-трафик). Такое исследование можно провести с помощью систем нагрузочного тестирования, однако для ее реализации потребуется разработать алгоритм генерации ПИВ-трафика, который будет использоваться для имитации исходящего потока сетевых пакетов от различных устройств, систем и приложений.

Реализовать подобный алгоритм представляется возможным на основе аналитических моделей, полученных при предварительном исследовании свойств ПИВ-трафика на основе анализа перехваченного трафика от систем промышленной автоматизации. В связи с тем, что в настоящее время комплексные системы ПИВ (далее по тексту – ПИВ-системы), затрагивающие большинство сфер автоматизации промышленных предприятий, не получили широкого распространения, перехват и анализ трафика предлагается провести на базе модельной сети, включающей в свой состав различные виды ПИВ-решений. Эти решения можно подобрать на основе существующей нормативно-правовой базы, например, на основе международных и отраслевых рекомендаций.

Сегодня не существует каких-либо рекомендаций, описывающих различные типы ПИВ-решений и их свойства, но, тем не менее, можно воспользоваться рекомендациями по типовой архитектуре и технологиям ПИВ-систем [10–11]. На основе этих документов предлагается разработать классификации источников трафика, сценариев работы и типов обслуживания.

Классификация источников ПИВ-трафика

Для разработки модельной сети, которую предлагается использовать для исследования свойств ПИВ-трафика, необходимо определить возможные типы источников трафика. В качестве основных для ПИВ-решений можно выделить следующие:

– датчики и актуаторы – используются для автоматизации работы промышленного оборудования; могут подключаться как напрямую к промышленному оборудованию и управляться через специальные приложения (например, с помощью ЧПУ), так и через специальные системы контроля и управления работы промышленного оборудования (например, SCADA, SAP Hana, OPC UA и др.) [8, 10, 12–13];

– бизнес-приложения (CRM, ERM и др.) – одним из наиболее важных аспектом работы предприятия является автоматизация работы бизнес-процессов предприятия [10, 14–15];

– открытые веб-данные – информация из открытых источников или веб-страниц в сети может использоваться как для обеспечения функционирования различных бизнес-процессов, так и для целей оптимизации работы предприятия с помощью различных аналитических алгоритмов [16];

– мультимедийные системы – в качестве источников могут выступать видеокамеры и микрофоны, которые используются для систем обеспечения безопасности предприятия [10, 17–18];

– системы позиционирования – данные системы могут использоваться для позиционирования промышленного оборудования, людей и транспорта, как в рамках предприятия, так и глобально, в масштабах региона или даже планеты [10, 19].

Естественно предположить, что каждый из вышеперечисленных видов трафика будет иметь уникальные сетевые параметры, такие как характер поступления и размер сетевых пакетов, коэффициент самоподобия, тип протоколов сетевого, транспортного и прикладного уровней, наличие (отсутствие) криптографических протоколов для обеспечения безопасности при передаче данных и др.

Каждый из источников трафика может работать по собственному уникальному сценарию сетевого взаимодействия, поэтому в рамках данного исследования можно выделить следующие сценарии работы различных типов устройств ПИВ (далее по тексту – ПИВ-устройств) [20]:

– регулярный – оконечное ПИВ-устройство отправляет пакеты данных на удаленное устройство хранения данных предприятия (например, сервер систем управления базами данных, системы промышленного управления и контроля работы предприятия и др.) с заранее заданной периодичностью;

– событийно-ориентированный – то же, по наступлению какого-либо события (запрос данных пользователем или другим устройством, отправка информации об изменении состояния и др.);

– по расписанию – следует из названия.

Также приложения и услуги ПИВ имеют собственные требования ко времени обслуживания. В частности, имеет смысл выделить следующие типы обслуживания:

– реального времени (приложения и услуги имеют жесткие ограничения по времени доставки сообщений, и поэтому данный тип сообщений доставляется за минимальное возможное время);

– толерантные к задержкам (жесткие ограничения по времени доставки отсутствуют, допустимы задержки).

Вышеприведенные классификации трафика были разработаны с учетом ряда требований к ПИВ-системам, определенных в международных отраслевых стандартах и рекомендациях [10–11].

Для разработки модельной сети на основе предложенной классификации предлагается рассмотреть существующие приложения, устройства и системы, которые можно отнести к одному из исследуемых источников ПИВ-трафика.

Модельная сеть для исследования свойств ПИВ-трафика

На соответствие предложенной классификации источников ПИВ-трафика был исследован ряд систем, применяемых в решениях промышленной автоматизации.

1) Системы, состоящие из промышленных устройств для аддитивного производства (см. тип «Датчики и актуаторы»):

– Trumpf TruPrint 1000 – промышленная система (ПС) аддитивной печати металлических изделий;

– 3D Systems ProJet 4500 – ПС аддитивной печати пластиковых изделий.

2) Система контроля ресурсов предприятия (СКРП) на основе системы 1С Битрикс (см. тип «Бизнес-приложения»).

3) Системы передачи информации для решения задач видеонаблюдения (см. тип «Мультимедийные системы»):

– система для организации видеомониторинга в режиме реального времени на основе программного обеспечения с открытым исходным кодом Open Broadcast Server (OBS);

– система видеомониторинга для хранения и предоставления видеоданных по запросу, основанная на облачном решении Ivideon, поставляемом вместе с IP-камерой OCo OP-2220F-MSD.

4) Открытые веб-приложения (см. тип «Открытые веб-данные»):

– Open Weather Maps (OWM) – используемое для определения текущего состояния окружающей среды (температура, атмосферное давление, уровень влажности и т. д.) на заданной территории;

– Open Street Maps (OSM) – используемое для определения местоположения различных объектов (техника, сотрудники, животные и т. д.) в глобальной системе координат.

5) Система локального позиционирования (СП) объектов на производстве Nanotron NanoPAN 5375 (см. тип «Системы позиционирования»).

В рамках проведенного авторами исследования, на базе лаборатории Интернета Вещей СПбГУТ была разработана модельная сеть [21], структура которой представлена на рисунке 1, где подключение к сети связи общего пользования необходимо для проведения исследования систем, соответствующих источнику трафика типа «Открытые веб-данные», а тестируемая сеть представляет собой ЛВС, имитирующую архитектуру локальной сети промышленного предприятия. На базе разработанной модельной сети стало возможным провести исследование свойств трафика от приложений, устройств и систем, применяемых в рамках ПИВ.

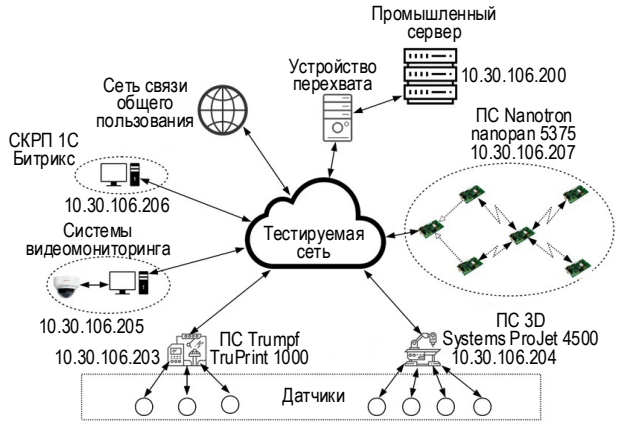


Рис. 1. Структура модельной сети для тестирования ПИВ-систем

Анализ ПИВ-трафика

В качестве основных свойств трафика, полученного от каждого из источников ПИВ-систем, имитируемых разработанной модельной сетью, были выбраны распределение интенсивности поступления и средний размер пакета, а также коэффициент Хёрста (самоподобия) для трафика. Для каждой из систем был произведен перехват трафика в количестве не менее 2000 пакетов.

Для анализа интенсивности поступления пакетов от источника использовались временные значения, представляющие собой интервалы времени между их поступлениями на сетевой интерфейс. Получившаяся выборка была разбита на 100 равноразмерных временных отрезков (между максимальным и минимальным значением) и с их помощью была построена вероятностно-временная характеристика для исследуемого трафика. Для каждого из полученных распределений с помощью критерия согласия Колмогорова – Смирнова подбиралось наиболее подходящее вероятностное распределение. Затем с помощью метода наименьших квадратов и алгоритма обобщенного приведенного градиента была проведена аппроксимация исходных данных. В таблице 1 приведены выбранные вероятностные распределения и их коэффициенты для каждого из исследуемых типов трафика. Подобная процедура была проведена для анализа распределения размеров перехваченных сетевых пакетов. В таблице 2 приведены выбранные вероятностные распределения и их коэффициенты для каждого из исследуемых типов трафика, а также средние значения размера сетевых пакетов при доверительной вероятности 95 % [22].

Также на основе метода нормированного размаха (RS-анализа) был рассчитан коэффициент Хёрста для выборок [14, 20], ранее полученных и исследованных при анализе интенсивности поступления пакетов.

Ниже приведены полученные значения для каждого из исследуемых источников трафика: Trumpf TruPrint 1000 – 0,83; 3D Systems ProJet 4500 – 0,96; Система OBS – 0,62; Система Ivideon – 0,56; 1С Битрикс – 0,41; Веб-приложение OWM – 0,57; Веб-приложение OSM – 0,51; Nanotron NanoPAN 5375 – 0,54.

На основе результатов анализа трафика от систем, применяемых в ПИВ, могут быть сделаны следующие выводы:

1) трафик для систем Trumpf TruPrint 1000, 3D Systems ProJet 4500 и OBS, согласно полученному значению коэффициента Хёрста (см. таблицу 3), является самоподобным;

2) трафик для систем Ivideon, веб-приложение OWM, веб-приложение OSM и Nanotron NanoPAN 5375 является самоподобным, близким к абсолютно случайному потоку;

3) трафик для системы 1С Битрикс является антиперсистентным, близким к абсолютно случайному потоку;

4) полученные вероятностные распределения интервалов времени между поступлениями сетевых пакетов и их размера для каждого из источников трафика могут быть использованы для моделирования идентичного сетевого потока при тестировании сетевой инфраструктуры предприятий перед внедрением исследуемых решений, а также других подобных им систем;

5) для получения более точных данных о ВВХ работы ПИВ-систем необходимо составить классификацию конкретных сценариев работы систем для каждого из исследуемых типов.

ТАБЛИЦА 1. Вероятностные распределения, описывающие интенсивность поступления сетевых пакетов

Источник трафика	Исследуемые интервалы, мкс	Вероятность попадания в интервал, %	Выбранное вероятностное распределение	Коэффициенты распределения
Trumpf TruPrint 1000	295000–339000	87,18	Бета первого рода	u = 64,53; v = 3089,15
	4213000–4213442	2,92	Бета первого рода	u = 6,56; v = 446,59
	5218000–5218442	9,71	Бета первого рода	u = 6,66; v = 422,41
3D Systems ProJet 4500	50000–56300	49,62	Гамма	α = 92,86; λ = 50000
	235000–288000	49,86	Гамма	α = 165,99; λ = 5882
Система OBS	0–516158	99,93	Экспоненциальное	λ = 169,50
Система Ivideon	0–1926	66,46	Гамма	α = 8,99; λ = 11111
	1926–16000	33,50	Эрланга	m = 2; λ = 1886,79
1С Битрикс	0–279	59,71	Вейбулла – Гнеденко	α = 36,85; c = 0,00019
	279–500000	37,85	Экспоненциальное	λ = 122,80
Веб-приложение OWM	0–50408	96,61	Экспоненциальное	λ = 1112,82
Веб-приложение OSM	0–10806	98,75	Экспоненциальное	λ = 5738,94
Nanotron NanoPAN 5375	0–238057	99,30	Эрланга	m = 3; λ = 40,00

ТАБЛИЦА 2. Вероятностные распределения, описывающие характер распределения размера сетевых пакетов

Источник трафика	Среднее значение размера пакета, байт	Исследуемые интервалы, байт	Вероятность попадания в интервал, %	Выбранное вероятностное распределение	Коэффициенты распределения
Trumpf TruPrint 1000	966±10	184	12,73	Эмпирическое дискретное	–
		1080	87,27		
3D Systems ProJet 4500	573±7	67	49,99	Равномерное дискретное	–
		1080	49,90		
Система OBS	1285±4	74–437	3,17	Равномерное непрерывное	–
		437–703	10,05	Гамма	α = 5,80; λ = 17
		703–1433	5,86	Равномерное непрерывное	–
		1434	80,92	Детерминированное	–
Система Ivideon	1451±2	1458	78,99	Эмпирическое дискретное	–
		1514	19,51		
1С Битрикс	1019±26	66	15,65	Эмпирическое дискретное	–
		74	5,19		
		203	3,45		
		276	3,54		
		574	4,22		
		1079	2,70		
		1466	61,80		
Веб-приложение OWM	945±22	66	20,98	Детерминированное	–
		67–302	8,32	Экспоненциальное	λ = 0,015
		302–990	8,11	Равномерное непрерывное	–
		990–1420	14,61	Вейбулла – Гнеденко	α = 10,58; c = 276,27
		1434	47,78	Детерминированное	–
Веб-приложение OSM	1326±6	66–1433	11,35	Равномерное непрерывное	–
		1434	88,65	Детерминированное	–
Nanotron NanoPAN 5375	366±3	74	11,87	Детерминированное	–
		75–437	19,55	Гамма	α = 18,86; λ = 11
		438	68,53	Детерминированное	–

На основе полученных аналитических моделей, представляющих собой аппроксимированные вероятностные распределения интервалов времени между поступлениями сетевых пакетов (см. таблицу 1) и их размера (см. таблицу 2) предлагается разработать алгоритм генерации ПИВ-трафика и сопоставить результаты его работы с вышеопределенными (исходными) распределениями.

Алгоритм генерации ПИВ-трафика

Для разработки алгоритма генерации ПИВ-трафика были выбраны следующие распределения случайных чисел:

– непрерывное равномерное (для генерации применяется алгоритм, описанный в [22, с. 211]);

– двухпараметрическое гамма (для случаев, когда параметр масштаба $\alpha < 1$ для генерации применяется алгоритм 1 описанный в [22, с. 140], для случаев, когда $\alpha > 1$ – описанный в [23, с. 112]);

– двухпараметрическое бета первого рода (для случаев, когда параметры формы $u > 1$ и $v > 1$ для генерации применяется алгоритм 2, в остальных случаях применяется алгоритм Йонка, описанные в [22, с. 216]);

– двухпараметрическое Вейбулла – Гнеденко (для генерации применяется алгоритм, описанный в [22, с. 158]);

– экспоненциальное (для генерации применяется алгоритм, описанный в [22, с. 136]);

– Эрланга m-го порядка (для генерации применяется алгоритм, описанный в [22, с. 147]).

Для генерации исходных псевдослучайных числовых значений согласно выбранным методам был использован метод генерации псевдослучайных чисел Фибоначчи с запаздыванием [24] с параметрами $\alpha = 55$ и $\beta = 24$. На основе выбранных алгоритмов был разработан общий алгоритм генерации псевдослучайных последовательностей согласно требуемому закону распределения. Блок-схемы, описывающие алгоритм работы генератора ПИВ-трафика, изображены на рисунках 2 и 3, где используемые переменные обозначают: C – количество источников трафика; N – количество сетевых пакетов, отправляемых каждым из источников; D (Dt, Dm) – параметры вероятностных распределений для интервалов времени между отправкой сетевых пакетов (Dt) и их размером (Dm). В D входят следующие параметры: $DTarr$ – последовательность, содержащая типы вероятностных распределений, применяемых для генерации трафика; DN – количество типов вероятностных распределений; $Karr$ – последовательность коэффициентов для используемых типов вероятностных распределений; $Parr$ – вероятность попадания псевдослучайного значения в тот или иной тип вероятностного распределения; V_{min}, V_{max} – минимальное и максимальное значение для псевдослучайного числа.

Разработанное специальное программное обеспечение (СПО), реализующее алгоритм на языках программирования C и C++ [25], было включено в ранее разработанную модельную сеть в качестве источника трафика; затем было проведено тестирование модельной сети с его применением. Данное СПО генерирует поток сетевых пакетов, имитируя работу одного или более ранее исследованных источников ПИВ-трафика. В качестве исходных моделей для имитации трафика были выбраны аналитические модели интенсивности поступления трафика на сетевой интерфейс, определенные ранее (см. таблицу 1, «выбранное вероятностное распределение» и «коэффициенты распределения»).

В ходе тестирования был произведен перехват сетевых пакетов, генерируемых СПО, и проведено сравнение исходного вероятностного распределения с экспериментальным, полученным в ходе аппроксимации данных по интенсивности поступления сетевых пакетов перехваченного трафика. Экспериментальные данные по интенсивности поступления сетевых пакетов были аппроксимированы с помощью метода наименьших квадратов и оптимизационного алгоритма обобщенного приведенного градиента.

Полученная функция была сопоставлена с исходным вероятностным распределением, с помощью критерия согласия Колмогорова – Смирнова. Также в ходе исследования интервалов времени между поступлением сетевых пакетов было получено их среднее значение для экспериментальных данных (сокращенно – Эксп.), данных, полученных в результате аппроксимации (сокращенно – Аппр.), а также данных, полученных на основе аналитической модели (сокращенно – Мат.). Результаты сравнения при выбранном уровне доверительной вероятности 95 % приведены в таблице 3.

На рисунке 3 представлены результаты сравнения исходных и аппроксимированных экспериментальных распределений интервалов поступления сообщений (в милисекундах), выбранных для описания характера трафика различных ПИВ-систем.

На основании графического анализа результатов тестирования разработанного алгоритма можно сделать вывод, что интервалы времени между поступлением пакетов для генерируемого трафика имеют высокую степень приближения к интервалам времени, соответствующих исходным аналитическим моделям. Тем не менее, при значениях интервалов менее 1 мс возникают проблемы, связанные с программными задержками отправки сетевых пакетов. Данная проблема связана с особенностями разработанного СПО и может быть решена путем оптимизации работы модуля программы, отвечающего за отправку пакетов.

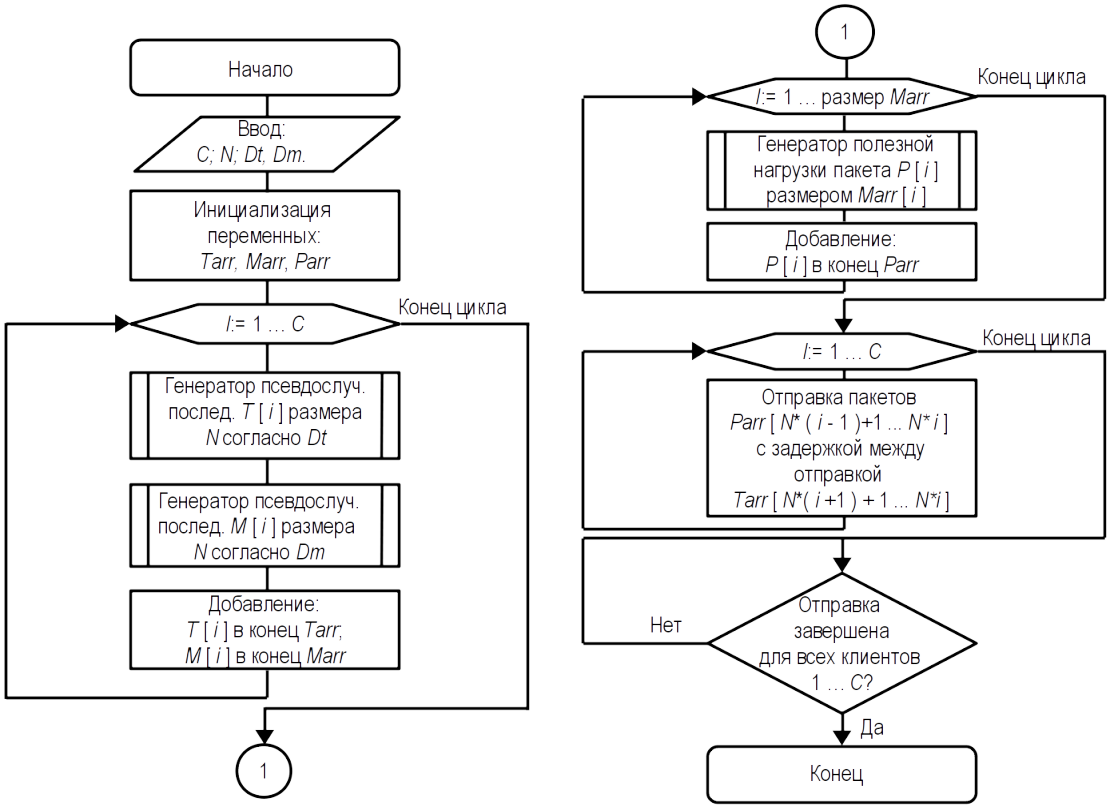


Рис. 2. Блок-схема алгоритма работы генератора ПИВ-трафика

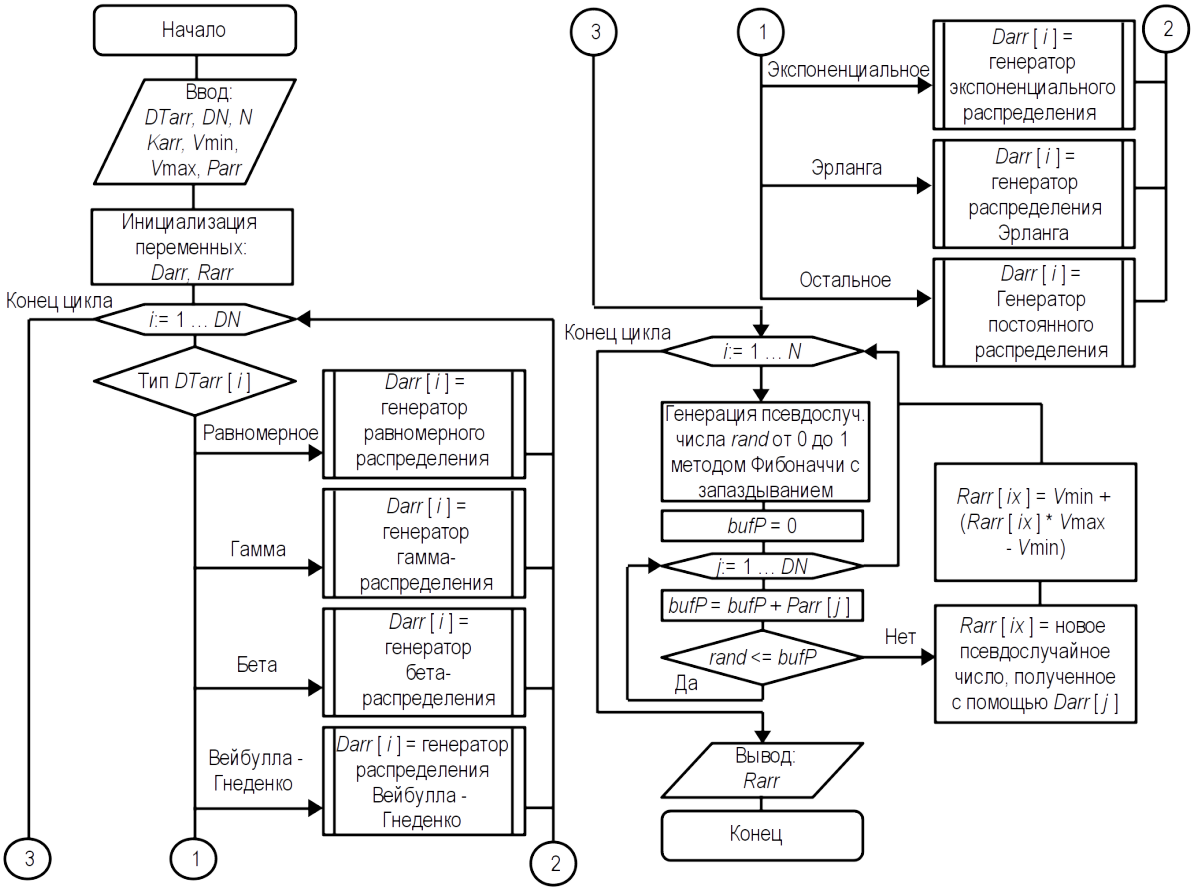


Рис. 3. Блок-схема алгоритм работы метода генерации псевдослучайных чисел по заданным распределениям

ТАБЛИЦА 3. Результаты сравнения исходной и экспериментальной интенсивности поступления сетевых пакетов

Промышленная система	Исходное распределение	Среднее значение интервалов времени между поступлениями пакетов, Эксп./Аппр./Мат. (мс)	Аппроксимация экспериментального распределения	Критерий согласия Колмогорова
Trumpf TruPrint 4500	Бета первого рода (u = 64,53; v = 3089,15)	18,01±0,943/18,09±0,521/17,81±0,516	u = 68,64; v = 3286,33	0,048 < 1,36
3D Systems ProJet	Гамма (α = 92,86; λ = 50000)	2,06±0,014/1,36±0,032/1,33±0,026	α = 87,41; λ = 50000	0,061 < 1,36
Система OBS	Экспоненциальное (λ = 169,50)	6,22±0,122/7,27±0,143/6,13±0,117	λ = 140,73	0,086 < 1,36
Система Ivideon	Гамма (α = 8,99; λ = 50000)	1,05±0,003/0,66±0,009/0,63±0,011	α = 8,37; λ = 11111	0,038 < 1,36
1С Битрикс	Вейбулла – Гнеденко (α = 36,85; c = 0,00019)	0,36±0,006/0,17±0,003/0,17±0,003	α = 12,42; c = 0,00019	0,83 < 1,36
Веб-приложение OWM	Экспоненциальное (λ = 1112,82)	1,06±0,019/1,12±0,022/1,03±0,020	λ = 1021,97	0,068 < 1,36
Веб-приложение OSM	Экспоненциальное (λ = 5738,94)	0,31±0,006/0,31±0,006/0,28±0,005	λ = 4922,05	0,34 < 1,36
Nanotron NanoPAN 5375	Эрланга (m = 3; λ = 40)	75,04±0,839/75,29±1,458/74,91±1,452	m = 3; λ = 39,80	0,002 < 1,36

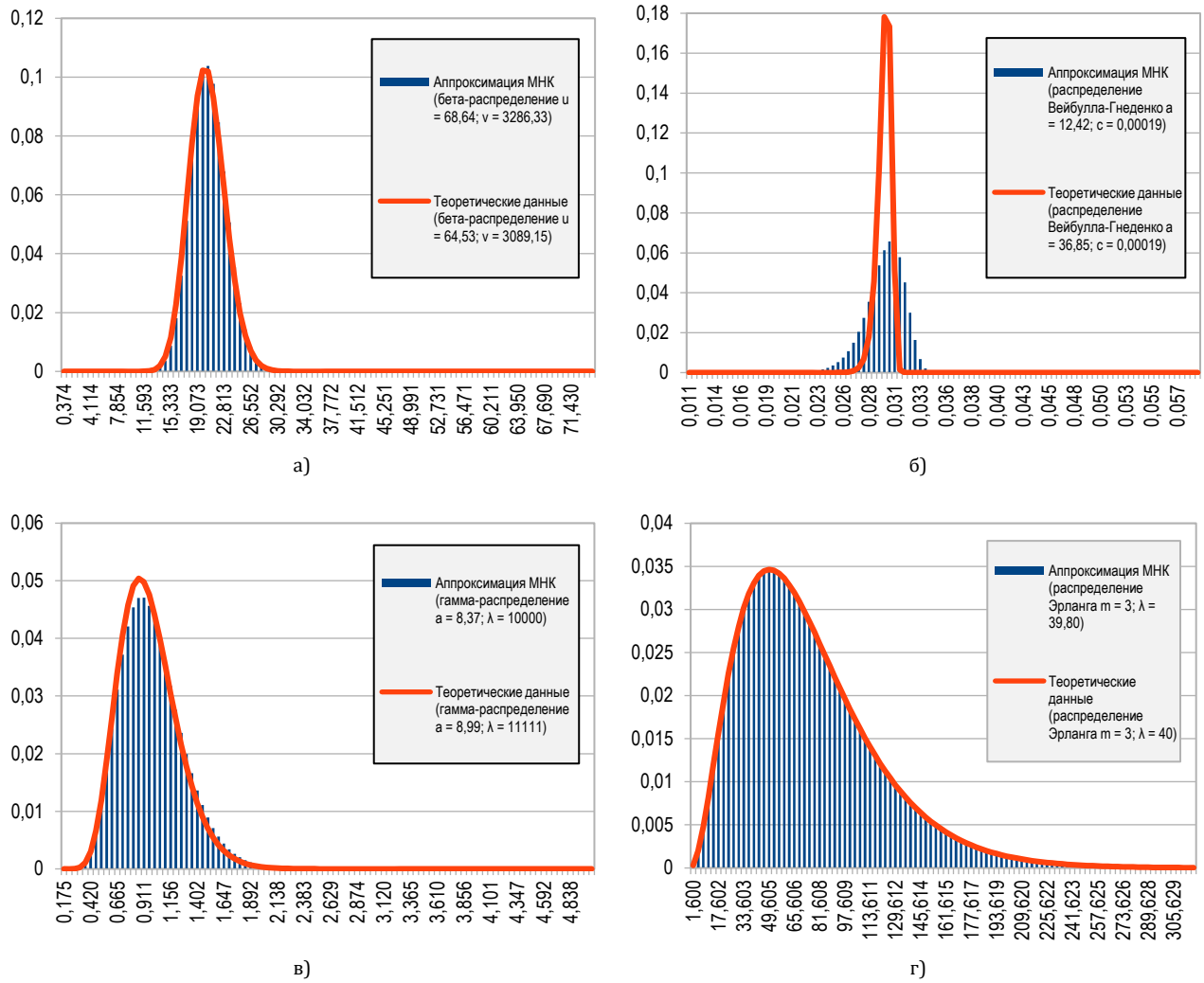


Рис. 4. Результаты сравнения вероятностных распределений трафика ПИВ-систем: а) Trumpf TruPrint 4500; б) 1С Битрикс; в) Ivideon; г) Nanotron NanoPAN 5375

Заключение

С помощью разработанной авторами классификации источников трафика промышленного Интернета Вещей и исследованных на базе модельной сети его типовых решений были получены аналитические модели, описывающие интенсивность поступления и распределения размера сетевых пакетов от каждого из исследованных источников трафика и позволяющие проводить моделирование потока сообщений от ПИВ-систем. Модельная сеть, созданная для исследования трафика типовых ПИВ-решений, также позволяет проводить натурные эксперименты по изучению влияния трафика на тестируемую сеть.

Практическая и научная значимость разработанного авторами алгоритма генерации ПИВ-трафика заключается в возможности исследования его свойств и влияния на сетевую инфраструктуру промышленных предприятий средствами имитационного и математического моделирования.

В дальнейшем, согласно полученным в данной статье аналитическим моделям, предполагается разработать имитационную модель для изучения работы высоконагруженных ПИВ-систем. Также на их основе предлагается разработать программно-аппаратный комплекс для проведения нагрузочного тестирования промышленных сетей.

Список используемых источников

1. Кучерявый А.Е., Владыко А.Г., Киричек Р.В., Маколкина М.А., Парамонов А.И., Выборнова А.И. и др. Перспективы научных исследований в области сетей связи на 2017–2020 годы // Информационные технологии и телекоммуникации. 2016. Т. 4. № 3. С. 1–14. URL: https://www.sut.ru/doci/nauka/review/20163/1-14.pdf (дата обращения 04.09.2019)

2. Makolkina M., Paramonov A., Vladyko A., Dunaytsev R., Kirichek R., Koucheryavy A. The Use of UAVs, SDN, and Augmented Reality for VANET Applications // Proceedings of the 3d International Conference on Artificial Intelligence and Industrial Engineering (AIIE, Shanghai, China, 26–27 November 2017). Lancaster: DEStech Publ., 2017. PP. 364–368. DOI:10.12783/dtcse/aiie2017/18244

3. Giyenko A., Cho Y.I. Intelligent UAV in smart cities using IoT // Proceedings of the 16th International Conference on Control, Automation and Systems (ICCAS, Gyeongju, South Korea, 16–19 October 2016). Piscataway, NJ: IEEE, 2016. PP. 207–210. DOI:10.1109/ICCAS.2016.7832322

4. Rhee S. Catalyzing the Internet of Things and smart cities: Global City Teams Challenge // Proceedings of the 1st International Workshop on Science of Smart City Operations and Platforms Engineering in partnership with Global City Teams Challenge (SCOPE – GCTC, Vienna, Austria, 11 April 2016). Piscataway, NJ: IEEE, 2016. DOI:10.1109/SCOPE.2016.7515058

5. Volkov A., Muthanna A., Pirmagomedov R., Kirichek R. SDN Approach to Control Internet of Thing Medical Applications Traffic // Proceedings of the 20th International Conference on Distributed Computer and Communication Networks (DCCN, Moscow, Russia, 25–29 September 2017). Communications in Computer and Information Science. Cham: Springer, 2017. Vol. 700. PP. 467–476. DOI:10.1007/978-3-319-66836-9_39

6. Pirmagomedov R., Blinnikov M., Glushakov R, Muthanna A., Kirichek R., Koucheryavy A. Dynamic Data Packaging Protocol for Real-Time Medical Applications of Nanonetworks // Proceedings of the 17th International Conference on Next Generation Wired/Wireless Networking (NEW2AN), 10th Conference on Internet of Things and Smart Spaces (ruSMART), 3d International Workshop on Nano-scale Computing and Communications (NsCC), St. Petersburg, Russia, 28–30 August 2017. Lecture Notes in Computer Science. Cham: Springer, 2017. Vol. 10531. PP. 196–205. DOI:10.1007/978-3-319-67380-6_18

7. Geng H. Internet of Things and Data Analytics Handbook. New York: John Wiley, 2017.

8. Tom R.J., Sankaranarayanan S. IoT based SCADA integrated with Fog for power distribution automation // Proceedings of the 12th Iberian Conference on Information Systems and Technologies (CISTI, Lisbon, Portugal, 21–24 June 2017). Piscataway, NJ: IEEE, 2017. DOI:10.23919/CISTI.2017.7975732

9. Kulik V., Kirichek R. The Heterogeneous Gateways in the Industrial Internet of Things // Proceedings of the 10th International Congress on Ultra Modern Telecommunications and Control Systems and Workshops (ICUMT, Moscow, Russia, 5–9 November 2018). Piscataway, NJ: IEEE, 2018. PP. 210–215. DOI:10.1109/ICUMT.2018.8631232

10. Rec. ITU-T Y.4003 (06/2018) Overview of smart manufacturing in the context of the industrial Internet of things. URL: https://www.itu.int/rec/T-REC-Y.4003-201806-I/en (дата обращения 09.09.2019)

11. Lin S.-W., Miller B., Durand J., Bleakley G., Chigani A., Martin R., et al. Industrial Internet of Things. Volume G1: Reference Architecture. Industrial Internet Consortium. 2017. URL: https://iiconsortium.org/IIC_PUB_G1_V1.80_2017-01-31.pdf (дата обращения 09.09.2019)

12. Shahzad A., Kim Y.G., Elgamoudi A. Secure IoT Platform for Industrial Control Systems // Proceedings of the International Conference on Platform Technology and Service (PlatCon, Busan, South Korea, 13–15 February 2017). Piscataway, NJ: IEEE, 2017. DOI:10.1109/PlatCon.2017.7883726

13. Cho H., Jeong J. Implementation and Performance Analysis of Power and Cost-Reduced OPC UA Gateway for Industrial IoT Platforms // Proceedings of the 28th International Telecommunication Networks and Applications Conference (ITNAC, Sydney, Australia, 21–23 November 2018). Piscataway, NJ: IEEE, 2018. DOI:10.1109/ATNAC.2018.8615377

14. Маколкина М.А., Окунева Д.В., Кулик В.А., Тельтевская В.А., Щербак А.С., Киричек Р.В. Исследование взаимодействия приложений дополненной реальности с облачными сервисами 1С // Электросвязь. 2017. № 12. С. 49–53.

15. Chamekh M., Hamdi M., Asmi S.E., Kim T.H. Secured Distributed IoT Based Supply Chain Architecture // Proceedings of the 27th International Conference on Enabling Technologies: Infrastructure for Collaborative Enterprises (WETICE, Paris, France, 27–29 June 2018). Piscataway, NJ: IEEE, 2018. PP. 199–202. DOI:10.1109/WETICE.2018.00045

16. Smit H., Delamer I.M. Service-oriented Architectures in Industrial Automation // Proceedings of the 4th IEEE International Conference on Industrial Informatics (INDIN, Singapore, Singapore, 16–18 August 2006). Piscataway, NJ: IEEE, 2006.

DOI:10.1109/INDIN.2006.275707
17. Kirichek R., Golubeva M., Kulik V., Koucheryavy A. The home network traffic models investigation // Proceedings of the 18th International Conference on Advanced Communication Technology (ICACT, Pyeongchang, South Korea, 31 January – 3 February 2016). Piscataway, NJ: IEEE, 2016. PP. 97–100. DOI:10.1109/ICACT.2016.7423288
18. Escudero J.I., Gonzalo F., Mejias M., Parada M., Luque J. Multimedia in the operation of large industrial networks // Proceeding of the IEEE International Symposium on Industrial Electronics (ISIE, Guimaraes, Portugal, 7–11 July 1997). Piscataway, NJ: IEEE, 1997. Vol. 3. PP. 1281–1285. DOI:10.1109/ISIE.1997.648929
19. Macagnano D., Destino G., Abreu G. Indoor positioning: A key enabling technology for IoT applications // Proceeding of the IEEE World Forum on Internet of Things (WF-IoT, Seoul, South Korea, 6–8 March 2014). Piscataway, NJ: IEEE, 2014. DOI:10.1109/WF-IoT.2014.6803131
20. Парамонов А.И. Разработка и исследование комплекса моделей трафика для сетей связи общего пользования. Автореферат дис. … докт. техн. наук. СПб.: СПбГУТ, 2014.
21. Рекомендация МСЭ-Т Q.3900 (09/2006). Методы тестирования и архитектура модельных сетей для тестирования технических средств СПП, используемых в сетях электросвязи общего пользования. URL: https://www.itu.int/ rec/ T-REC-Q.3900-200609-I/en (дата обращения 09.09.2019)
22. Вадзинский Р.Н. Справочник по вероятностным распределениям. СПб.: Наука, 2001. 295 с.
23. Емельянов А.А. Лаг-генераторы для моделирования рисковых ситуаций в системе Actor Pilgrim // Прикладная информатика. 2011. № 5(35). С. 98–117.
24. Bruce S. Applied Cryptography: Protocols, Algorithms, and Source Code in C. New York: John Wiley & Sons, Inc., 1996.
25. Кулик В. Генератор трафика Промышленного Интернета Вещей // Cloud Version Control System Bitbucket. URL: https://bitbucket.org/vslavk/generate_iiot_traffic/src/master (дата обращения 20.07.2019)

* * *

INDUSTRIAL INTERNET OF THINGS TRAFFIC RESEARCH AND GENERATION

R. Kirichek[1], V. Kulik[1]

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

Article info
The article was received 10 July 2019

For citation: Kirichek R., Kulik V. Industrial Internet of Things Traffic Research and Generation. *Proceedings of Telecommunication Universities*. 2019;5(3):27–36. (in Russ.) Available from: https://doi.org/10.31854/1813-324X-2019-5-3-27-36

Abstract: *In this research paper we can see the analysis of the application types, devices, and systems which are used to find the solutions in the industrial Internet of Things. On the basis of a research in a scientific field, we got the developed classification for problem solving in the industrial Internet of Things, including traffic from industrial equipment, traffic of business applications, traffic from open web sources, various types of multimedia traffic and traffic generated by positioning systems. Based on the developed classification, various typical applications, devices, and systems were selected and there was developed the Model network for their traffic analysis. With the help of the developed model network there was traffic analysis research of the industrial Internet of Things. Based on the obtained traffic properties, the algorithm of the traffic generator was described. The results of the traffic generator were compared with the initial probability distributions obtained at the traffic analysis from the different types of traffic sources.*

Keywords: *Internet of Things, industrial Internet of Things, traffic analysis, traffic generation.*

References

1. Koucheryavy A., Vladyko A., Kirichek R., Makolkina M., Paramonov A., Vybornova A., et al. The prospects for research in the field of communications networks on the 2017–2020 years. *Telecom IT*. 2016;4(3):1–14. (in Russ.) Available from: https://www.sut.ru/doci/nauka/review/20163/1-14.pdf [Accessed 4th September 2019]
2. Makolkina M., Paramonov A., Vladyko A., Dunaytsev R., Kirichek R., Koucheryavy A. The Use of UAVs, SDN, and Augmented Reality for VANET Applications. *Proceedings of the 3d International Conference on Artificial Intelligence and Industrial Engineering, AIIE, 26–27 November 2017, Shanghai, China.* Lancaster: DEStech Publ.; 2017. p.364–368. Available from: https://doi.org/10.12783/dtcse/aiie2017/18244

3. Giyenko A., Cho Y.I. Intelligent UAV in smart cities using IoT. *Proceedings of the 16th International Conference on Control, Automation and Systems, ICCAS, 16–19 October 2016, Gyeongju, South Korea*. Piscataway, NJ: IEEE; 2016. p.207–210. Available from: https://doi.org/10.1109/ICCAS.2016.7832322

4. Rhee S. Catalyzing the Internet of Things and smart cities: Global City Teams Challenge. *Proceedings of the 1st International Workshop on Science of Smart City Operations and Platforms Engineering in partnership with Global City Teams Challenge, SCOPE – GCTC, 11 April 2016, Vienna, Austria*. Piscataway, NJ: IEEE; 2016. Available from: https://doi.org/10.1109/SCOPE.2016.7515058

5. Volkov A., Muthanna A., Pirmagomedov R., Kirichek R. SDN Approach to Control Internet of Thing Medical Applications Traffic. *Proceedings of the 20th International Conference on Distributed Computer and Communication Networks, DCCN, 25–29 September 2017, Moscow, Russia. Communications in Computer and Information Science*. Cham: Springer; 2017. vol.700. p.467–476. Available from: https://doi.org/10.1007/978-3-319-66836-9_39

6. Pirmagomedov R., Blinnikov M., Glushakov R, Muthanna A., Kirichek R., Koucheryavy A. Dynamic Data Packaging Protocol for Real-Time Medical Applications of Nanonetworks. *Proceedings of the 17th International Conference on Next Generation Wired/Wireless Networking, NEW2AN, 10th Conference on Internet of Things and Smart Spaces, ruSMART, 3d International Workshop on Nano-scale Computing and Communications, NsCC, 28–30 August 2017, St. Petersburg, Russia. Lecture Notes in Computer Science.* Cham: Springer; 2017. vol.10531. p.196–205. Available from: https://doi.org/10.1007/978-3-319-67380-6_18

7. Geng H. *Internet of Things and Data Analytics Handbook*. New York: John Wiley; 2017

8. Tom R.J., Sankaranarayanan S. IoT based SCADA integrated with Fog for power distribution automation. *Proceedings of the 12th Iberian Conference on Information Systems and Technologies, CISTI, 21–24 June 2017, Lisbon, Portugal*. Piscataway, NJ: IEEE; 2017. Available from: https://doi.org/10.23919/CISTI.2017.7975732

9. Kulik V., Kirichek R. The Heterogeneous Gateways in the Industrial Internet of Things. *Proceedings of the 10th International Congress on Ultra Modern Telecommunications and Control Systems and Workshops, ICUMT, 5–9 November 2018, Moscow, Russia*. Piscataway, NJ: IEEE; 2018. p.210–215. Available from: https://doi.org/10.1109/ICUMT.2018.8631232

10. Rec. ITU-T Y.4003 *Overview of smart manufacturing in the context of the industrial Internet of things*. June 2018. Available from: https://www.itu.int/rec/T-REC-Y.4003-201806-I/en [Accessed 09 September 2019]

11. Lin S.-W., Miller B., Durand J., Bleakley G., Chigani A., Martin R., et al. *Industrial Internet of Things. Volume G1: Reference Architecture*. Industrial Internet Consortium. 2017. Available from: https://iiconsortium.org/IIC_PUB_G1_V1.80_2017-01-31.pdf [Accessed 09 September 2019]

12. Shahzad A., Kim Y.G., Elgamoudi A. Secure IoT Platform for Industrial Control Systems. *Proceedings of the International Conference on Platform Technology and Service, PlatCon, 13–15 February 2017, Busan, South Korea*. Piscataway, NJ: IEEE; 2017. Available from: https://doi.org/10.1109/PlatCon.2017.7883726

13. Cho H., Jeong J. Implementation and Performance Analysis of Power and Cost-Reduced OPC UA Gateway for Industrial IoT Platforms. *Proceedings of the 28th International Telecommunication Networks and Applications Conference, ITNAC, 21–23 November 2018, Sydney, Australia*. Piscataway, NJ: IEEE; 2018. Available from: https://doi.org/10.1109/ATNAC.2018.8615377

14. Makolkina M.A., Okuneva D.V., Kulik V.A., Teltevskaya V.A., Shcherbak A.S., Kirichek R.V. Research of interaction between augmented reality applications and 1C cloud services. *Elektrosvyaz*. 2017;12:31–35. (in Russ.)

15. Chamekh M., Hamdi M., Asmi S.E., Kim T.H. Secured Distributed IoT Based Supply Chain Architecture. *Proceedings of the 27th International Conference on Enabling Technologies: Infrastructure for Collaborative Enterprises, WETICE, 27–29 June 2018, Paris, France*. Piscataway, NJ: IEEE; 2018. p.199–202. Available from: https://doi.org/10.1109/WETICE.2018.00045

16. Smit H., Delamer I.M. Service-oriented Architectures in Industrial Automation. *Proceedings of the 4th IEEE International Conference on Industrial Informatics, INDIN, 16–18 August 2006, Singapore, Singapore*. Piscataway, NJ: IEEE; 2006. Available from: https://doi.org/10.1109/INDIN.2006.275707

17. Kirichek R., Golubeva M., Kulik V., Koucheryavy A. The home network traffic models investigation. *Proceedings of the 18th International Conference on Advanced Communication Technology, ICACT, 31 January – 3 February 2016, Pyeongchang, South Korea*. Piscataway, NJ: IEEE; 2016. p.97–100. Available from: https://doi.org/10.1109/ICACT.2016.7423288

18. Escudero J.I., Gonzalo F., Mejias M., Parada M., Luque J. Multimedia in the operation of large industrial networks. *Proceeding of the IEEE International Symposium on Industrial Electronics, ISIE, 7–11 July 1997, Guimaraes, Portugal*. Piscataway, NJ: IEEE; 1997. vol.3. p.1281–1285. Available from: https://doi.org/10.1109/ISIE.1997.648929

19. Macagnano D., Destino G., Abreu G. Indoor positioning: A key enabling technology for IoT applications. *Proceeding of the IEEE World Forum on Internet of Things, WF-IoT, 6–8 March 2014, Seoul, South Korea*. Piscataway, NJ: IEEE; 2014. Available from: https://doi.org/10.1109/WF-IoT.2014.6803131

20. Paramonov A.I. *Razrabotka i issledovanie kompleksa modeley trafika dlya setey svyazi obshchego pol'zovaniya* [Development and Research of Complex Traffic Models for Public Communication Networks]. DSc Thesis. St. Petersburg: The Bonch-Bruevich Saint-Petersburg State University of Telecommunications Publ.; 2014. (in Russ.)

21. Rec. ITU-T Q.3900. *Methods of testing and model network architecture for NGN technical means testing as applied to public telecommunication networks*. September 2006. Available from: https://www.itu.int/rec/T-REC-Q.3900-200609-I/en [Accessed 09 September 2019]

22. Vadzinskiy R.N. *Spravochnik po veroyatnostnym raspredeleniyam* [Probability Distribution Handbook]. St. Petersburg: Nauka Publ.; 2001. 295 p. (in Russ.)

23. Emelyanov A. Software lag-generators for simulation of risk situations in Actor Pilgrim Simulation System. *Applied informatics*. 2011;5(35):98–17. (in Russ.)

24. Bruce S. *Applied Cryptography: Protocols, Algorithms, and Source Code in C*. New York: John Wiley & Sons, Inc.; 1996.

25. Kulik V. *Generate IIOT Traffic*. Cloud Version Control System Bitbucket. Available from: https://bitbucket.org/vslavk/generate_iiot_traffic/src/master [Accessed 20 July 2019]

МЕТОД МАРШРУТИЗАЦИИ ТРАФИКА В СЕТИ ИНТЕРНЕТА ВЕЩЕЙ НА ОСНОВЕ МИНИМУМА ВЕРОЯТНОСТИ КОЛЛИЗИЙ

А.Е. Кучерявый[1], **О.А. Махмуд**[1], **А.И. Парамонов**[1*]

[1]Санкт-Петербургский государственный университет телекоммуникаций им. проф. М.А. Бонч-Бруевича, Санкт-Петербург, 193232, Российская Федерация
*Адрес для переписки: alex-in-spb@yandex.ru

Информация о статье
УДК 004.7
Статья поступила в редакцию 31.05.2019

Ссылка для цитирования: Кучерявый А.Е., Махмуд О.А., Парамонов А.И. Метод маршрутизации трафика в сети Интернета Вещей на основе минимума вероятности коллизий // Труды учебных заведений связи. 2019. Т. 5. № 3. С. 37–44. DOI:10.31854/1813-324X-2019-5-3-37-44

Аннотация: *В статье рассматривается анализ основных подходов к выбору маршрутов в сетях Интернета Вещей и предлагается метод выбора маршрутов с учетом вероятности коллизий, что позволяет сформировать логическую структуру сети. Предлагаемый метод использует оценки вероятности коллизий для различных участков и реализуют выбор маршрута как задачу минимизации этой вероятности на всем множестве доступных маршрутов. Метод основан на использовании алгоритма поиска кратчайших путей в графе. Предлагаемый метод был реализован средствами имитационного моделирования, с помощью которых была получена оценка его эффективности, для сетей с высокой плотностью узлов по отношению к методам, основанным на оценке длины маршрута.*

Ключевые слова: *Интернет Вещей, коллизия, маршрут, самоподобный трафик, простейший поток, имитационное моделирование.*

Введение

Развитие концепции Интернета Вещей приводит к интенсивному росту количества различных устройств, подключенных к сетям связи [1, 2]. Она направлена на дальнейшее развитие инфокоммуникационной системы в части охвата тех сфер деятельности человека, которые еще не были вовлечены в процесс информационного обмена, т. е. перейти на уровень «умных» вещей, «умных» домов и в целом интеллектуального мира [1–5]. При этом технологии доступа к сети могут быть самыми различными. Это могут быть как устройства, поддерживающие стандарты сетей сотовой связи и беспроводного широкополосного доступа, так и специализированные стандарты, ориентированные на построение беспроводных сенсорных сетей (БСС) [3, 4]. Плотность таких устройств может быть очень высока. Согласно прогнозу (исходя из данных на 2020 г.), количество устройств Интернета Вещей может возрасти к 2022 г. до 32 миллиардов. Потенциально такие устройства смогут находиться как в зоне обслуживания сетей подвижной связи, так и вне их. Задача их функционирования состоит в доставке данных к средствам обработки или команд управления в обратном направлении. В связи с широким разнообразием целевых назначений и технологий структуры построения сетей могут быть различны.

В частности, для организации сетей могут использоваться различные технологии самоорганизации, позволяющие строить mesh и ad hoc сети. Использование этих технологий позволяет существенно расширить возможности сетей в части расширения зоны обслуживания, легкости развертывания, обеспечения надежности и живучести. Задача самоорганизации включает в себя подзадачу выбора маршрутов для пропуска трафика между узлами сети [5]. От способа ее реализации существенно зависят характеристики сети (пропускная способность, задержка доставки данных, потери пакетов и др.). Работа по выбору маршрута связана с передачей дополнительного трафика в сети связи, а также к потерям времени доступности узлов сети [6, 7]. Это снижает качество ее параметров функционирования. Поэтому целесообразно эту работу сводить к минимуму. В частности, этому может способствовать качество получаемых в результате маршрутов.

Выбор структуры сети и путей пропуска трафика является одной из основных проблем перспектив-

ных сетей связи, в задачи которых входит и обслуживание трафика Интернета Вещей. Известно множество работ, посвященных вопросам выбора структуры и маршрутизации трафика.

Так, в работе [8] предложен метод оценки связности БСС. В [9] были получены результаты сравнения протоколов маршрутизации для БСС и выбора конкретного протокола для построения сенсорной сети в зависимости от плотности узлов. В [10] представлен анализ протокола RPL с точки зрения IoT с учетом следующих эталонных показателей: надежность, мобильность, неоднородность ресурсов и масштабируемость. В работе [11] приведены результаты исследований в области оптимизации маршрутов в сетях Интернета Вещей. В [12–14] были рассмотрены способы выбора маршрута по критерию минимальной длины, а в данной работе предлагается выбрать – по критерию минимальной вероятности коллизий. Также в ряде работ рассматривались методы обеспечения связности для D2D-коммуникаций (*от англ. Device to Device* – устройство-устройство), которые обеспечивают выбор по минимальному затуханию или максимальному отношению сигнал/шум).

В данной работе предлагается метод выбора маршрута в сети по его показателю качества, за который принимаем минимум коллизий (вероятность коллизий). Этот показатель для БСС позволяет также косвенно учесть вероятность потерь кадров и полосу пропускания.

1. Постановка задачи

Задача выбора маршрута является одной из задач построения некой оптимальной логической структуры сети. Будем полагать, что имеется n узлов (источников трафика Интернета Вещей), которые распределены некоторым образом в зоне обслуживания и образуют гомогенную структуру, характеристики которой неизменны для любого фрагмента зоны обслуживания. При этом связь источника с получателем трафика может быть организована как напрямую, так и через транзитные узлы, в качестве которых могут выступать любые узлы-источники трафика. В зависимости от технологии реализации канала трафик соседних (смежных) узлов может приводить к задержкам, потерям кадров и снижению полосы пропускания. Рост задержки, потерь и снижение полосы пропускания являются следствием занятости канала (среды распространения, участка радиочастотного спектра) передаваемыми сигналами. Если применяемый стандарт не реализует механизмов предотвращения конфликтов, то занятость канала приводит к коллизии.

Как правило, под коллизией понимают ситуацию, при которой на вход приемника одновременно поступают два или более сигналов от различных передатчиков; в результате наложения сигналов ни одно из принимаемых сообщений не оказывается успешно принятым и все передаваемые на этом интервале элементы данных (кадры) оказываются потерянными. Теоретически возможно, что некоторые данные могут быть приняты, однако вероятность этого крайне мала, и далее этот случай не рассматривается. Многие современные стандарты беспроводной связи реализуют механизмы предотвращения коллизий, которые обеспечивают снижение их вероятности путем анализа состояния среды передачи и определенного алгоритма выделения времени на передачу, но естественным образом приводит к задержкам передачи, т. е. использованию ресурса времени. Таким образом, вероятность коллизии, даже при использовании механизма их предотвращения, характеризует использование (занятость) среды передачи.

Вероятность коллизий прямо или косвенно отражает качество канала связи или всего маршрута. Показатели полосы пропускания, потерь пакетов и задержки непосредственно связаны с этой вероятностью. Поэтому далее будем использовать ее как метрику для выбора маршрута в сети связи.

2. Модель узла сети и метод выбора маршрута

Будем считать, что узел может быть оснащен антенным, радиопередающим и/или радиоприемным устройствами. Все узлы, возможно кроме шлюзовых, имеют типовое оснащение. Зона связи узла представляет собой круг радиуса r с центром в точке его размещения. Для большинства стандартов, применяемых для организации сетей Интернета Вещей, скорость передачи данных зависит от условий приема сигнала, однако, для упрощения задачи будем полагать, что скорость передачи данных в пределах зоны связи неизменна (не зависит от расстояния до узла). Такой подход часто оправдан, т. к. при проектировании сети стараются максимально повысить ее пропускную способность и расположения узлов выбирают таким образом, чтобы условия связи обеспечивали максимально достижимую скорость. Каждый из узлов во время передачи данных занимает среду передачи, размеры которой ограничены зоной интерференции, и в данной модели также представляет собой круг радиуса R. Обычно $R \geq r$. Одновременная передача данных двумя и более узлами приводит к потере данных (коллизии), в том числе, когда приемный узел находится в зоне интерференции хотя бы одного из конфликтующих узлов.

Пусть среднее время передачи кадра равно τ, а интенсивность передачи кадров λ. При оценке вероятности коллизии будем рассуждать следующим образом. Коллизия происходит тогда, когда за время передачи кадра будет начата или закончена еще хотя бы одна передача. Иными словами, когда интервал передачи кадра пересечется еще с одним или более интервалами передачи (рисунок 1). Данная модель аналогична модели ALOHA, описанной, например, в работах [15–17].

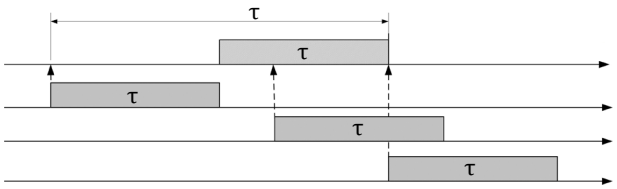


Рис. 1. Пример события коллизии

Из рисунка видно, что для того, чтобы произошло наложение на рассматриваемый кадр одной и более передач, достаточно, чтобы эти передачи были начаты за интервал времени, равный 2τ, т. е. во время передачи рассматриваемого кадра или не позднее, чем за время τ до начала рассматриваемого кадра. Таким образом, вероятность коллизии равна вероятности начала одной или более передач кадров за интервал времени 2τ:

$$p_c = p_{\geq 1}(2\tau) = 1 - p_0(2\tau). \qquad (1)$$

Если трафик можно описать моделью простейшего потока, то вероятность коллизии можно вычислить, подставив в (1) формулу для вероятности распределения Пуассона $p_k(x) = \frac{(\lambda x)^k}{k!} e^{-\lambda x}$. Тогда вероятность коллизий узла для 2D-модели, при допущении, что зона связи узла представляет собой круг радиуса R, можно определить как:

$$p_c = 1 - e^{-\lambda 2\tau}. \qquad (2)$$

Аналогичный результат можно было получить, рассматривая функцию распределения интервалов времени между моментами начала передачи кадров в простейшем потоке. Все кадры, передача которых была начата на интервале 2τ, будут повреждены. Среднее количество поврежденных в результате коллизии кадров будет равно $m = 2\lambda\tau p_c$. Интенсивность коллизий может быть определена как $\eta = \lambda p_c$, где $\lambda = \sum_{i=1}^{k} \lambda_i$ – интенсивность передачи (кадров) i-ым узлом в зоне связи (кадров/с); k – количество узлов в зоне связи.

Использование модели простейшего потока весьма удобно, но не всегда оправдано, так как в большинстве случаев потоки трафика в современных сетях существенно отличаются от простейшего. Как показывают результаты исследований, чаще всего трафик в БСС обладает свойствами самоподобного процесса [18]. Поэтому при описании таких процессов используют распределение Парето для моделирования интервалов времени между моментами поступления кадров (пакетов):

$$F(t) = P(X < x) = 1 - \left(\frac{t_m}{t}\right)^k, \quad x_m > 0, \qquad k > 0$$

$$M(x) = \frac{k t_m}{k-1}, \quad k > 1.$$

Тогда вероятность того, что интервал времени будет менее 2τ, равна:

$$p_c = p(X < 2\tau) = 1 - \left(\frac{t_m}{2\tau}\right)^k. \qquad (3)$$

Отличие свойств трафика от свойств простейшего потока естественным образом отражается на функционировании рассматриваемой модели, поскольку вероятность коллизий будет определяться уже не распределением Пуассона. Модель с распределением Парето позволяет оценить степень влияния этого отличия на вероятность коллизий.

Вероятность коллизии характеризует канал связи между узлами сети: чем она меньше, тем доступен больший ресурс канала, следовательно, вероятна большая пропускная способность канала. На рисунке 2 приведены зависимости вероятности коллизии от использования канала для двух моделей потоков: простейшего и потока, интервалы времени между заявками в котором подчинены распределению Парето.

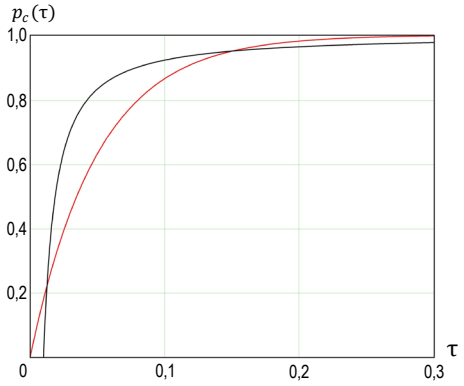


Рис. 2. Зависимость вероятности коллизий от использования канала

Как видно из графиков, в области средних нагрузок вероятность коллизии выше для потока второго типа. В области малых и больших значений нагрузки вероятность коллизии выше для модели простейшего потока. Если трафик проходит через маршрут из n независимых участков, то вероятность потери данных (кадра) из-за коллизий для всего маршрута будет равна:

$$p_c = 1 - \prod_{i=1}^{m} \left(1 - p_{ci}\right). \qquad (4)$$

где p_{ci} – вероятность коллизии на i-ом участке маршрута, определяемая как было показано выше.

Задачу поиска маршрута с минимальной вероятностью коллизий можно сформулировать как:

$$P = \underset{r \in \Omega}{\operatorname{argmin}}(p_c), \qquad (5)$$

где Ω – все множество возможных маршрутов.

Как видно из (2–3), вероятность коллизии тем больше, чем больше интенсивность трафика (использование канала). Таким образом, при выборе маршрута можно руководствоваться как величиной вероятности коллизии (потери кадра из-за коллизии), так и величиной интенсивности трафика в зоне связи. Для поиска маршрута, согласно

критерию (5), может быть использован любой алгоритм поиска кратчайшего пути во взвешенном графе. Для этого сеть должна быть описана графом $G(V,E)$ с множеством вершин $V = \{v_{ij}\}$, $i,j = 1 \dots n$, которые соответствуют узлам сети и множеством ребер (дуг) E, релевантным потенциально возможным связям (каналам) между узлами сети. Узлы характеризуются зоной связи (в данном случае, радиусом R), в центре которого находится данный узел. Узлы сети описываются их координатами (x_i, y_i) и расстояниями между ними:

$$D = \{d_{ij}\}, i,j = 1 \dots n, \quad d_{ij} = \sqrt{(x_i - x_j)^2 + (y_i - y_j)^2}.$$

Ребра между узлами существуют, если расстояние между узлами меньше R, иначе можно записать: $E = \{e_{ij}\}$, $i,j = 1 \dots n$; $v_j \in R_i \Rightarrow \exists e_{ij}$.

Каждому из ребер графа приписан весовой коэффициент $C = \{c_{ij}\}$, $i,j = 1 \dots n$, определяющий метрику, по которой производится выбор маршрута. В данном случае в качестве весов ребер (или дуг) должны быть выбраны логарифмы вероятности коллизий, оценка которой может быть получена согласно (2) или (3) в зависимости от рассматриваемой модели потока:

$$c_{ij} = -\log\left(1 - p_{ij}\right), \quad i,j = 1 \dots n, \qquad (6)$$

где p_{ij} – вероятность коллизий в маршруте между узлами i и j.

3. Анализ результатов моделирования

На рисунке 3 приведены результаты имитационного моделирования. Параметры модели: область обслуживания – квадрат со стороной 200 м; узлы размещены случайным образом (координаты x и y – случайные числа, подчиненные равномерному закону распределения); количество узлов – 200; радиус связи узла равен радиусу интерференции и составляет 60 м. Результат выбора «кратчайшего» пути (пути наименьших коллизий) с использованием критерия (5) представлен на рисунке 3б. На рисунке 3а для сравнения приведен результат выбора пути по критерию наименьшей длины.

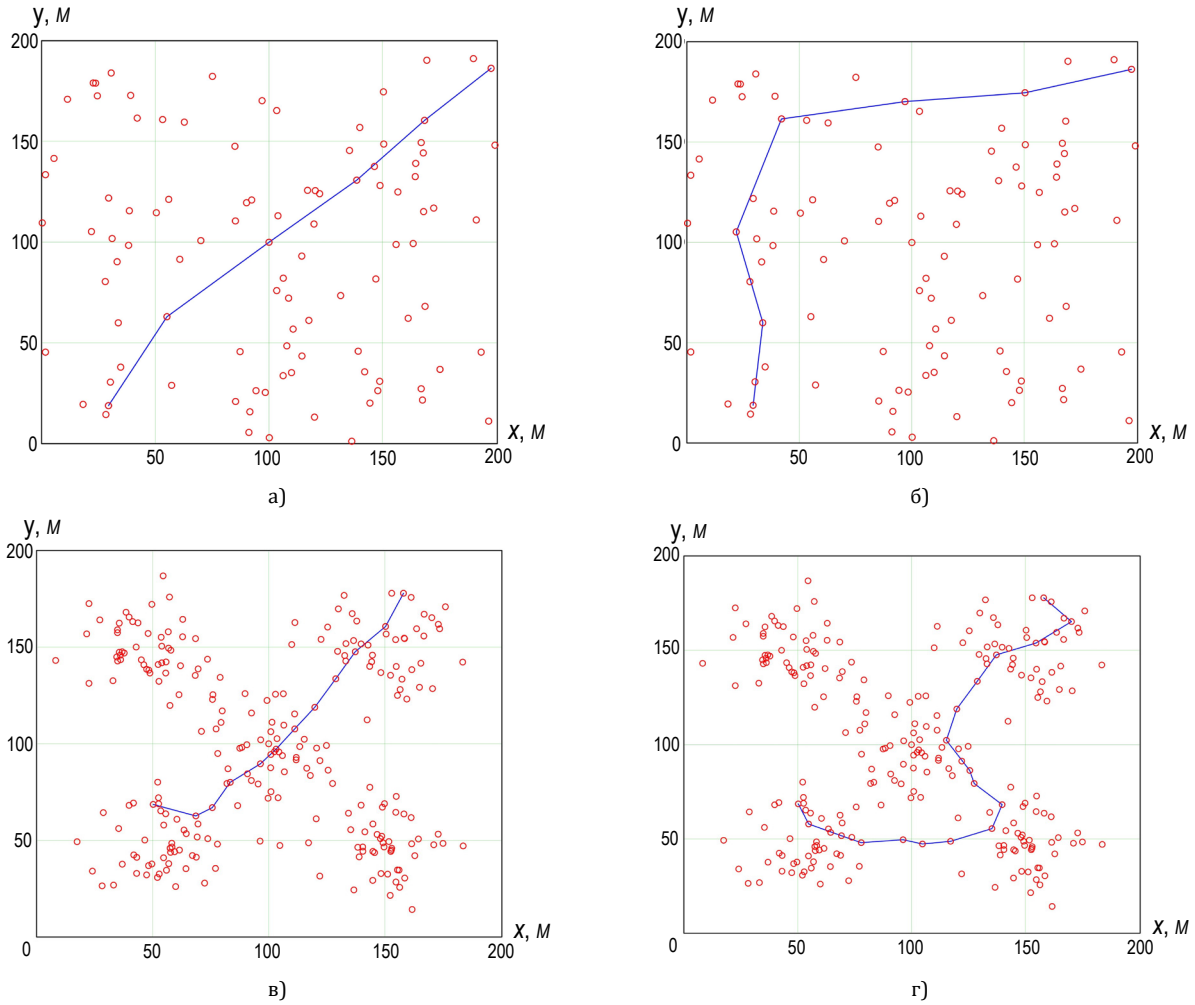


Рис. 3. Результат выбора «кратчайшего» пути при равномерном (а, б) и мультимодальном (в, г) распределении узлов сети по критериям наименьшей длины (слева) и минимальной вероятности коллизий (справа)

При моделировании были сделаны следующие допущения. Производимый в узле трафик равновероятно распределялся между всеми узлами сети (от каждого узла к каждому). В качестве модели генерируемого узлами трафика использовалось распределение Парето (3), а все потоки рассматривались как стационарные. Вероятность коллизий оценивалась согласно моделям (3–4) на основе данных о трафике.

Из приведенного рисунка видно, что маршрут, построенный на основе критерия минимума вероятности коллизий, существенно отличается от маршрута, построенного на основе критерия минимума длины. На рисунках 3в и 3г приведен аналогичный пример для мультимодального распределения узлов в зоне обслуживания (распределение имеет пять центров рассеяния). Можно заметить, что маршрут, выбираемый по минимуму коллизий, стремится «обходить» области с высокой плотностью узлов. Это ожидаемый результат, т. к. в области с высокой плотностью узлов в зону интерференции попадает большее их количество, следовательно, согласно (2) или (3) имеет место большая вероятность коллизий.

Стоит отметить, что полученные результаты согласуются с опубликованными в [19] для сети, построенной с использованием D2D-коммуникаций, где взаимное влияние узлов сети проявляется через снижение отношения сигнал/шум. В среднем, результат поиска дает маршрут с вероятностью коллизий на 20 % меньшей, чем маршрут, найденный по критерию минимальной длины. Эффективность алгоритма зависит от способа размещения узлов сети – приведенные результаты моделирования соответствуют равномерному случайному и мультимодальному распределению узлов сети на территории обслуживания.

Для проверки полученных результатов была разработана имитационная модель БСС стандарта IEEE 802.15.4 (рисунок 4) в системе имитационного моделирования Contiki Cooja [20]. Для сравнительного анализа был выбран протокол маршрутизации RPL в стандартном режиме, т. е. при выборе маршрута по метрике расстояния и в модифицированном режиме по метрике (3). Сеть состояла из 25 узлов. Результаты имитационного моделирования показали, что задержка доставки пакета зависит от использования канала, причем при выборе маршрута по предложенной метрике задержка меньше, чем в случае выбора по расстоянию.

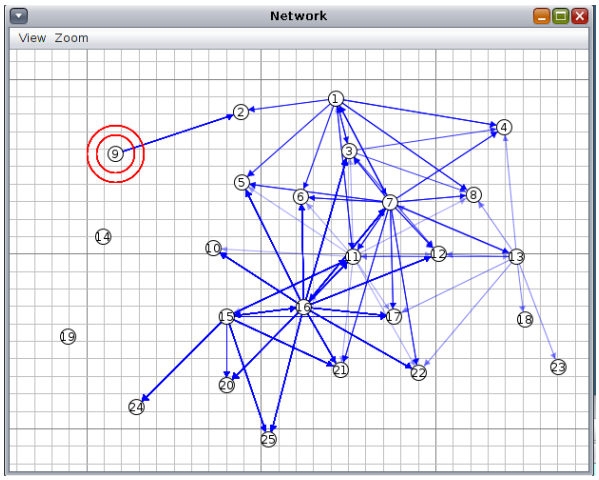
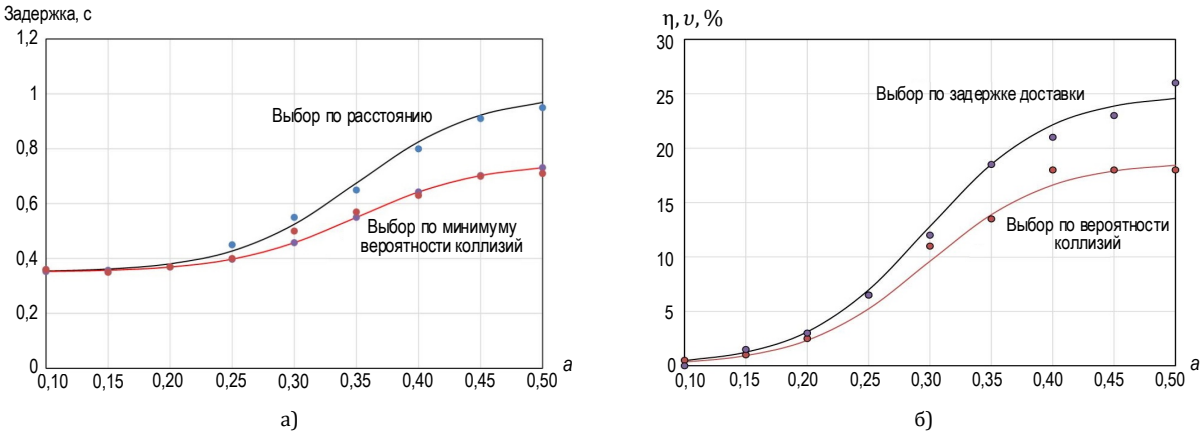


Рис. 4. Имитационная модель в Contiki Cooja

Эффективность метода возрастает с ростом интенсивности трафика, производимого узлами сети. Например, при использовании канала на 0,5 задержка для предлагаемого метода меньше на величину около 25 %, что подтверждает сделанные предположения. Выбранная технология использует механизм предотвращений коллизий. Однако, расчетная оценка согласно модели (3) в данном случае, также была близка к указанному выше значению и при использовании канала 0,5 составила 18 %.

На рисунке 5 приведены зависимости эффективности предложенного метода от интенсивности трафика по отношению к методу, использующему критерий минимального расстояния.



а) б)

Рис. 5. Зависимость эффективности от нагрузки по задержке (а) и относительная эффективность по задержке и вероятности коллизий (б)

Приведенные на правом графике значения η (черная линия) и ν (красная линия) отражают относительное изменение средней величины задержки и вероятности коллизий, соответственно, при использовании предложенного метода, в зависимости от интенсивности трафика для протокола RPL. Данные зависимости показывают, что эффективность метода возрастает с ростом интенсивности трафика, что является ожидаемым результатом. При увеличении интенсивности близкой к 0,5 рост эффективности замедляется.

Заключение

Построение сетей Интернета Вещей предполагает применение различных технологий и структур, многие из которых требуют решения задачи выбора маршрута пропуска трафика (передачи сообщения). Выбор маршрута в сети может производиться на основе различных критериев и в общем случае является задачей оптимизации, а ее решение позволяет найти маршрут, удовлетворяющий некоторому критерию качества. Таким критерием может быть один или несколько параметров, применяемых для описания качества канала передачи данных.

Анализ основных показателей качества беспроводного канала связи показал, что большинство из них прямо или косвенно связаны с таким показателем как вероятность коллизий. Несмотря на то, что многие применяемые протоколы используют технологии предотвращения коллизий, вероятность коллизии косвенно характеризует использование канала, задержку и его полосу пропускания (пропускную способность).

Предложенная в работе модель характеризует качество канала на основе вероятности коллизий и может быть использована как для модели простейшего потока, так и для модели самоподобного потока трафика. При наличии данных о свойствах трафика конкретных приложений модель достаточно просто может быть модифицирована заменой выражения (3) на функцию распределения для соответствующего потока.

На основе предложенной модели разработан метод поиска маршрута с минимальной вероятностью коллизий. Для реализации метода может быть использован любой алгоритм поиска кратчайшего пути в графе.

Результаты по отношению к протоколу RPL были проверены в системе имитационного моделирования Contiki Cooja и показали эффективность предлагаемого метода (в части выбора маршрута с лучшими параметрами качества обслуживания трафика) на уровне 25 % по величине задержки доставки и 18 % по вероятности коллизий. Полученные зависимости показали, что его эффективность возрастает при увеличении интенсивности трафика, поэтому данный метод может найти применение при построении сетей Интернета Вещей при соответствующих значениях трафика.

Предлагаемый метод является одним из возможных методов решения задачи маршрутизации. Его эффективность показана как меньшая вероятность коллизий, а также как меньшая величина задержки доставки данных по отношению к методам, основанным на критерии длины маршрута, что подтверждает возможность его применения как альтернативного метода выбора маршрутов.

Список используемых источников

1. Кучерявый А.Е., Парамонов А.И., Кучерявый Е.А. Сети связи общего пользования. Тенденции развития и методы расчета. М.: ФГУП ЦНИИС, 2008. 290 с.

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

3. Кучерявый А.Е., Прокопьев А.В., Кучерявый Е.А. Самоорганизующиеся сети. СПб: Типография «Любавич», 2011. 312 с.

4. Muthanna A., Prokopiev A., Koucheryavy A. The mixed telemetry/image USN in the overload conditions // Proceedings of the 16th International Conference on Advanced Communication Technology (ICACT, Pyeongchang, South Korea, 16–19 February 2014). Piscataway, NJ: IEEE, 2014. DOI:10.1109/ICACT.2014.6779006

5. Мутханна А.С., Прокопьев А.В., Кучерявый А.Е. Сравнительный анализ протоколов маршрутизации RPL и AODV // II Международная научно-техническая и научно-методическая конференция «Актуальные проблемы инфотелекоммуникаций в науке и образовании» (Санкт-Петербург, Россия, 27–28 февраля 2013). Сборник научных статей. СПб.: СПбГУТ, 2013. С. 167–171.

6. Hoang T., Kirichek R., Paramonov A., Houndonougbo F., Koucheryavy A. Adaptive routing in wireless sensor networks under electromagnetic interference // Proceedings of the 31st International Conference on Information Networking (ICOIN, Da Nang, Vietnam, 11–13 January 2017). Piscataway, NJ: IEEE, 2017. PP. 76–79. DOI:10.1109/ICOIN.2017.7899479

7. Hoang L.T., Kirichek R.V., Paramonov A.I., Koucheryavy A.E. Development of Methods to Maintain the Functionality of Wireless Sensor Networks Under Intentional Electromagnetic Interference Conditions // Electrosvyaz. 2017. № 3. С. 32–38.

8. Paramonov A., Nurilloev I., Koucheryavy A. Provision of Connectivity for (Heterogeneous) Self-organizing Network Using UAVs // Proceedings of the 17th International Conference on Next Generation Wired/Wireless Networking (NEW2AN), 10th Conference on Internet of Things and Smart Spaces (ruSMART), IIId Workshop on Nano-scale Computing and Communications (NsCC), St. Petersburg, Russia, 28–30 August 2017. Lecture Notes in Computer Science. Cham: Springer, 2017. Vol. 10531. PP. 569–576. DOI:10.1007/978-3-319-67380-6_53

9. Paramonov A., Hussain O., Samouylov K., Koucheryavy A., Kirichek R., Koucheryavy Y. Clustering Optimization for Out-of-Band D2D communications // Wireless Communications and Mobile Computing. 2017. Vol. 2017. DOI:10.1155/2017/6747052

10. Makolkina M., Vikulov A., Paramonov A. The Augmented Reality Service Provision in D2D Network // Proceedings of the 20th International Conference on Distributed Computer and Communication Networks (DCCN, Moscow, Russia, 25–29

September 2017). Communications in Computer and Information Science. Cham: Springer, 2017. Vol. 700. PP. 281–290. DOI:10.1007/978-3-319-66836-9_24

11. Nurilloev I., Paramonov A., Koucheryavy A. Connectivity Estimation in Wireless Sensor Networks // Proceedings of the 16th International Conference on Next Generation Wired/Wireless Networking (NEW2AN) and 9th Conference on Internet of Things and Smart Spaces (ruSMART), St. Petersburg, Russia, 26–28 September 2016. Lecture Notes in Computer Science. Cham: Springer, 2016. Vol. 9870. PP. 269–277. DOI:10.1007/978-3-319-46301-8_22

12. Muthanna A., Masek P., Hosek J., Fujdiak R., Hussein O., Paramonov A., Koucheryavy A. Analytical Evaluation of D2D Connectivity Potential in 5G WIRELESS Systems // Proceedings of the 16th International Conference on Next Generation Wired/Wireless Networking (NEW2AN) and 9th Conference on Internet of Things and Smart Spaces (ruSMART), St. Petersburg, Russia, 26–28 September 2016. Lecture Notes in Computer Science. Cham: Springer, 2016. Vol. 9870. PP. 395–403. DOI:10.1007/978-3-319-46301-8_33

13. Dao N., Koucheryavy A., Paramonov A. Analysis of Routes in the Network Based on a Swarm of UAVs // Kim K. J., Joukov N. (eds.) Information Science and Applications (ICISA). Lecture Notes in Electrical Engineering. Singapore: Springer, 2016. Vol. 376. PP. 1261–1271. DOI:10.1007/978-981-10-0557-2_119

14. Kirichek R., Paramonov A., Vladyko A., Borisov E. Implementation of the Communication Network for the Multi-Agent Robotic Systems // International Journal of Embedded and Real-Time Communication Systems. 2016. Vol. 7. Iss. 1. PP. 48–63. DOI:10.4018/IJERTCS.2016010103.

15. Abramson N. THE ALOHA SYSTEM: Another Alternative for Computer Communications // Proceedings of the American Federation of Information Processing Societies (AFIPS) Fall Joint Computer Conference (Houston, USA, 17–19 November 1970). New York: ACM, 1970. PP. 281–285. DOI:10.1145/1478462.1478502

16. Abramson N. The Throughput of Packet Broadcasting Channels // IEEE Transactions on Communications. 1977. Vol. 25. Iss. 1. PP. 117–128. DOI:10.1109/TCOM.1977.1093713

17. Banzal S. Data and Computer Network Communication. Boston: Firewall Media, 2007.

18. Paramonov A., Koucheryavy A. M2M Traffic Models and Flow Types in Case of Mass Event Detection // Proceedings of the 14th International Conference on Next Generation Wired/Wireless Networking (NEW2AN) and 7th Conference on Internet of Things and Smart Spaces (ruSMART), St. Petersburg, Russia, 27–29 August 2014. Lecture Notes in Computer Science. Cham: Springer, 2014. Vol. 8638. PP. 294–300. DOI:10.1007/978-3-319-10353-2_25

19. Бородин А.С., Парамонов А.И. Маршрутизация трафика в сети беспроводной связи, построенной на базе D2D-технологий // Электросвязь. 2019. № 2. С. 38–44.

20. Contiki: The Open Source OS for the Internet of Things. URL: http://www.contiki-os.org/start.html (дата обращения: 18.07.2019)

* * *

TRAFFIC ROUTING METHOD FOR THE INTERNET OF THINGS BASED ON THE MINIMUM OF COLLISIONS PROBABILITY

A. Koucheryavy[1], **O.A. Mahmood**[1], **A. Paramonov**[1]

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

Article info
The article was received 31 May 2019

For citation: Koucheryavy A., Mahmood O.A., Paramonov A. Traffic Routing Method for the Internet of Things Based on the Minimum of Collisions Probability. *Proceedings of Telecommunication Universities*. 2019;5(3):37–44. (in Russ.) Available from: https://doi.org/10.31854/1813-324X-2019-5-3-37-44

Abstract: *The article discusses the analysis of the main approaches to the route choices in the networks of the Internet of Things and suggests a method of choosing routes taking into account the probability of collisions, which allows to create a logical network structure. The proposed method is based on the seeking algorithm of the quickest route on the graph. This method was implemented by means of simulation modeling, with the help of which was estimated the effectiveness for networks with high density of units comparing with the methods, which are based on the evaluation of the length of the route.*

Keywords: *Internet of things, collision, route, self-similar traffic, simple flow, simulation.*

References

1. Koucheryavy A.E., Paramonov A.I., Koucheryavy E.A. *Seti sviazi obshchego polzovaniia. Tendentsii razvitiia i metody rascheta* [Public Communication Networks. Development Trends and Calculation Methods]. Moscow: Central Research Institute of Communications Publ.; 2008. (in Russ.)
2. Koucheryavy A.E. Internet Veshchei [Internet of Things]. *Electrosvyaz*. 2013;1:21–24. (in Russ.)
3. Koucheryavy A.E., Prokopiev A.V., Koucheryavy Y.A. *Samoorganizuiushchiesia seti* [Self-Organizing Network]. St. Petersburg: Lyubavich Printing House; 2011. 312 p. (in Russ.)
4. Muthanna A., Prokopiev A., Koucheryavy A. The mixed telemetry/image USN in the overload conditions. *Proceedings of the 16th International Conference on Advanced Communication Technology (ICACT), 16–19 February 2014, Pyeongchang, South Korea*. Piscataway, NJ: IEEE; 2014. Available from: https://doi.org/10.1109/ICACT.2014.6779006
5. Muthanna A., Prokopiev A., Koucheryavy A. The RPL and AODV Routing Protocol Features Comparison. *Proceedings of the IId International Conference on Infotelecommunications in Science and Education, 27–28 February 2013, St. Petersburg, Russia*. St. Petersburg: The Bonch-Bruevich Saint-Petersburg State University of Telecommunications Publ.; 2013. p.167–171. (in Russ.)
6. Hoang T., Kirichek R., Paramonov A., Houndonougbo F., Koucheryavy A. Adaptive routing in wireless sensor networks under electromagnetic interference. *Proceedings of the 31st International Conference on Information Networking, ICOIN, 11–13 January 2017, Da Nang, Vietnam*. Piscataway, NJ: IEEE; 2017. p.76–79. Available from: https://doi.org/10.1109/ICOIN.2017.7899479
7. Hoang L.T., Kirichek R.V., Paramonov A.I., Koucheryavy A.E. Development of Methods to Maintain the Functionality of Wireless Sensor Networks Under Intentional Electromagnetic Interference Conditions. *Electrosvyaz*. 2017;3:32–38.
8. Paramonov A., Nurilloev I., Koucheryavy A. Provision of Connectivity for (Heterogeneous) Self-organizing Network Using UAVs. *Proceedings of the 17th International Conference on Next Generation Wired/Wireless Networking (NEW2AN), 10th Conference on Internet of Things and Smart Spaces (ruSMART), IIId Workshop on Nano-scale Computing and Communications (NsCC), 28–30 August 2017, St. Petersburg, Russia. Lecture Notes in Computer Science*. Cham: Springer; 2017. vol.10531. p.569–576. Available from: https://doi.org/10.1007/978-3-319-67380-6_53
9. Paramonov A., Hussain O., Samouylov K., Koucheryavy A., Kirichek R., Koucheryavy Y. Clustering Optimization for Out-of-Band D2D communications. *Wireless Communications and Mobile Computing*. 2017. vol.2017. Available from: https://doi.org/10.1155/2017/6747052
10. Makolkina M., Vikulov A., Paramonov A. The Augmented Reality Service Provision in D2D Network. *Proceedings of the 20th International Conference on Distributed Computer and Communication Networks (DCCN), 25–29 September 2017, Moscow, Russia. Communications in Computer and Information Science*. Cham: Springer; 2017. vol.700. p.281–290. Available from: https://doi.org/10.1007/978-3-319-66836-9_24
11. Nurilloev I., Paramonov A., Koucheryavy A. Connectivity Estimation in Wireless Sensor Networks. *Proceedings of the 16th International Conference on Next Generation Wired/Wireless Networking (NEW2AN) and 9th Conference on Internet of Things and Smart Spaces (ruSMART), 26–28 September 2016, St. Petersburg, Russia. Lecture Notes in Computer Science*. Cham: Springer; 2016. vol.9870. p.269–277. Available from: https://doi.org/10.1007/978-3-319-46301-8_22
12. Muthanna A., Masek P., Hosek J., Fujdiak R., Hussein O., Paramonov A., Koucheryavy A. Analytical Evaluation of D2D Connectivity Potential in 5G WIRELESS Systems. *Proceedings of the 16th International Conference on Next Generation Wired/Wireless Networking (NEW2AN) and 9th Conference on Internet of Things and Smart Spaces (ruSMART), 26–28 September 2016, St. Petersburg, Russia. Lecture Notes in Computer Science.* Cham: Springer; 2016. vol.9870. p.395–403. Available from: https://doi.org/10.1007/978-3-319-46301-8_33
13. Dao N., Koucheryavy A., Paramonov A. Analysis of Routes in the Network Based on a Swarm of UAVs. In: Kim K. J., Joukov N. (eds.) *Information Science and Applications (ICISA). Lecture Notes in Electrical Engineering.* Singapore: Springer; 2016. vol.376. p.1261–1271. Available from: https://doi.org/10.1007/978-981-10-0557-2_119
14. Kirichek R., Paramonov A., Vladyko A., Borisov E. Implementation of the Communication Network for the Multi-Agent Robotic Systems. *International Journal of Embedded and Real-Time Communication Systems*. 2016;7(1):48–63. Available from: https://doi.org/10.4018/IJERTCS.2016010103
15. Abramson N. THE ALOHA SYSTEM: Another Alternative for Computer Communications. *Proceedings of the American Federation of Information Processing Societies (AFIPS) Fall Joint Computer Conference, 17–19 November 1970, Houston, USA*. New York: ACM; 1970. p.281–285. Available from: https://doi.org/10.1145/1478462.1478502
16. Abramson N. The Throughput of Packet Broadcasting Channels. *IEEE Transactions on Communications.* 1977;25(1): 117–128. Available from: https://doi.org/10.1109/TCOM.1977.1093713
17. Banzal S. *Data and Computer Network Communication*. Boston: Firewall Media; 2007.
18. Paramonov A., Koucheryavy A. M2M Traffic Models and Flow Types in Case of Mass Event Detection. *Proceedings of the 14th International Conference on Next Generation Wired/Wireless Networking (NEW2AN) and 7th Conference on Internet of Things and Smart Spaces (ruSMART), 27–29 August 2014, St. Petersburg, Russia. Lecture Notes in Computer Science*. Cham: Springer; 2014. vol.8638. p.294–300. Available from: https://doi.org/10.1007/978-3-319-10353-2_25
19. Borodin A.S., Paramonov A.I. Routing of traffic in D2D wireless network. *Electrosvyaz*. 2019;2:38–44. (in Russ.)
20. *Contiki: The Open Source OS for the Internet of Things*. Available from: http://www.contiki-os.org/start.html [Accessed 18th Jule 2019]

ANALYSIS OF QOS DELIVERED TO USERS OF WCDMA BAND IN DIFFERENT LOCATIONS: CASE STUDY OF UNIVERSITY OF ILORIN, NIGERIA

O.A. Tiamiyu[1*]

[1]University of Ilorin
Ilorin, PMB 1515, Nigeria,
*Correspondence Address: ozutiams@yahoo.com

Article info
The article was received 03 June 2019

For citation: Tiamiyu O.A. Analysis of QOS Delivered to Users of WCDMA Band in Different Locations: Case Study of University of Ilorin, Nigeria. *Proceedings of Telecommunication Universities*. 2019;5(3):45–56. Available from: https://doi.org/10.31854/1813-324X-2019-5-3-45-56

Abstract: *Since 2001, which marked the advent of modern telephony in Nigeria, there is a significant increase in the capacity of the Mobile Network Operators (MNOs). Total connected active lines were quite over a hundred million according to the reports by Nigeria Communications Commission (NCC), the regulatory body in Nigeria. However, mobile telephone users in the country are experiencing poor quality of service at different locations in the country. Thus, NCC has set benchmark values for various keys performance Indicator. In this study, findings on the quality of service delivered to users of WCDMA Band by the MNOs in different locations within University of Ilorin will be made.*

Keywords: *Mobile Network Operators, capacity, WCDMA, QoS, keys performance Indicator, users' location, University of Ilorin.*

1. INTRODUCTION

The history of mobile communication in Nigeria is traceable to the deregulation of the traditional means of communication under the civilian rule of the then president of the federal republic of Nigeria in person on President Olusegun Obasanjo (GCFR). This deregulation gave birth to GSM revolution in 2001. Before the advent of mobile communication in Nigeria, Nigeria Telecommunication Limited (NITEL) was saddled with the responsibility of managing the telecommunications sector, which was via Landline referred to as Fixed Telephony [1]. The first Mobile Network Operator (MNO) that came on board was ECONET (now Airtel), launched on August 6, 2001; MTN followed suit almost immediately.

The Nigerian Telecommunication Industry is said to be the fastest growing telecommunication industry in the world with current teledensity of 108 % and the biggest telecom industry in the world. It represents the largest provider of job opportunity in the country and contributes greatly to the country's GDP [2].

Before 2001, which marked the advent of modern telephony in Nigeria, teledensity in the country was at a very low level. 13 years down the line, Nigeria's telecommunication, the total connected active lines were quite over a hundred million with a teledensity above 90 according to the reports by NCC in 2013 [3]. This implies that there was a significant increase in the capacity of the Mobile Network Operators (MNOs). This necessitated adoption of better system, like Universal Mobile Telecommunications System (UMTS) that uses Wideband Code Division Multiple Access (WCDMA) for its transmission network.

Users embraced UMTS as it is backward compatible with the already existing network architecture, which is General Packet Radio System (GPRS) or Enhanced Data rates for Global Evolution (EDGE) network. This has minimized the investment required to set up 3G network. In addition, the regular SIM is upgradable to Universal SIM (USIM) that enables it to communicate over the UMTS network. UMTS specifies the Universal Terrestrial Radio Access Network (UTRAN), which is composed of multiple Node-Bs in place of base stations using different terrestrial air interface standards and frequency bands [4].

As seen in Figure 1, UMTS network architecture indicates that the GPRS or EDGE Core Network (CN) remains the same. This shows its Inter-Radio Access Technology (IRAT) interoperability [2, 5, 6]. 3G Architecture has three (3) main parts, the Core Network, UMTS Terrestrial Radio Access Network (UTRAN) and user equipment (UE). The CN performs the function of switching, transit, and routing of traffic between nodes (packet or circuit switched); the UTRAN (also referred to as Radio Access Technologies) has two parts, namely Radio Network Controller (RNC) and Node-Bs. RNC performs handover functions, ciphering of data in the network, Radio Resource Control, Power Management

and control, Channel allocation among other functions. Node-Bs perform the functions of the Base station in 2G network, which is to provide the air interface to the User Equipment and also modulation and demodulation of traffic.

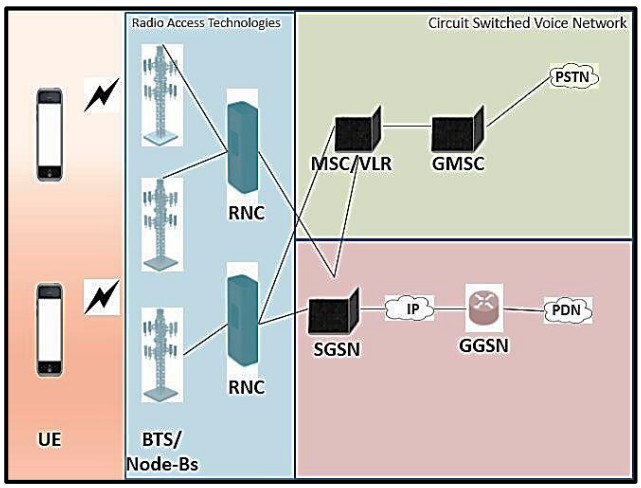


Fig. 1. UMTS Network Architecture

UE, which comprises the USIM as well as the Mobile Station of the user, has various identities assigned to it on the network such as IMSI, MSISDN, TMSI, IMEI and so on [7].

Though UMTS has better capacity than the predecessors do, yet mobile telephone users in the country are experiencing and complaining about poor QoS at different locations in the country. There have been complaining over the QoS delivered by service providers in the country continuously over the last few years that the MNOs had to pay fines billed on them by NCC in 2013 and 2014 for poor service delivery [8, 9]. Furthermore, there were reports in the Guardian newspaper from individuals complaining about poor service from MNOs. A consumer living in Lagos complained that he hardly had successful conversations without three to four breaks in transmission. He further stressed that sometimes when he called; he hardly heard the user on the other side. According to the consumer, this got worse with time.

There was also a report from a subscriber to service providers, the subscriber who was supposed to receive a notification message from a company about an interview but could not receive the message on time due to poor signal reception. The subscriber lost the job [9].

Among the complaints is the receipt of unsolicited messages by subscribers [8]. In the Guardian Newspapers in their technology section, it was reported that NCC affirmed that mobile telephone users in the country had experienced poor QoS in Q4 of 2016 and Q1 of 2017. The poor services range from drop calls, call setup failure, poor call retention, weak signals, cross-talk, and unsolicited text messages among others [10].

As each of the MNOs is not having optimum service delivery in every location in the country, most mobile subscribers do subscribe to more than one MNO, thereby having to switch Subscriber Identity Module (SIM) from a location to another; or being forced to use more than one mobile equipment.

Thus, considering that subscribers of the MNOs in Nigeria is increasing at a very high rate, there is a need for the various MNOs to check their coverage rate and see their overall network performance meets the needs of the subscribers to their network. Moreover, the regulatory body in Nigeria, Nigeria Communications Commission (NCC) has set benchmark values for various Key Performance Indicator (KPI) (Table 1) [11].

Hence, this has prompted researchers to make findings on the QoS delivered by the MNOs in different locations and areas of the country.

In this study, KPI for voice communication in the 3G UMTS network of the four different Mobile Network Operators (MNO) in Nigeria, tagged as operator A, B, C and D respectively will be checked.

The KPIs to check include:
– Network Accessibility (Call Setup Success Rate);
– Coverage Voice Quality (–10dB ≤ Ec/No < 0 dB);
– Handover Success Rate (HOSR);
– Coverage Reliability (% RSCP > –85 dbm);
– Speech Quality Index;
– Call Setup Time;
– Network Retain ability (dropped call rate).

As a means of informing people and the MNOs themselves, there is a company, OpenSignal, which monitors signal level on daily basis. This company produces reports on their website about network providers worldwide.

Thus, for a start in this study, below are the results considering the scope of this project as provided on this company's website as at July 27, 2017. The points Painted Red are reports of poor QoS area while those painted green are areas with good QoS as depicted in the Figure 2-6 [12].

The report for MNO A shows that there are no reported data (signal) on Jalala and Senior Staff Quarters that are located within the university of Ilorin campus, unlike within its Permanent Site where QoS is high according to the report (Figure 2 and 3). Figure 4–6 depicts the report by Open Signal for signal quality of MNO B.

TABLE 1. Some NCC Set KPI Threshold Values

KPI	Call Setup Success Rate	Call Setup Time	Call Drop Rate	Handover Success Rate	Received Signal Code Power	Ec/No	Call Completion Success Rate
NCC defined benchmark	≥ 98%	≤ 6 sec	≤ 1%	≥ 98 %	≥ –85 dBm	≥ –9 dBm	≥ 97 %

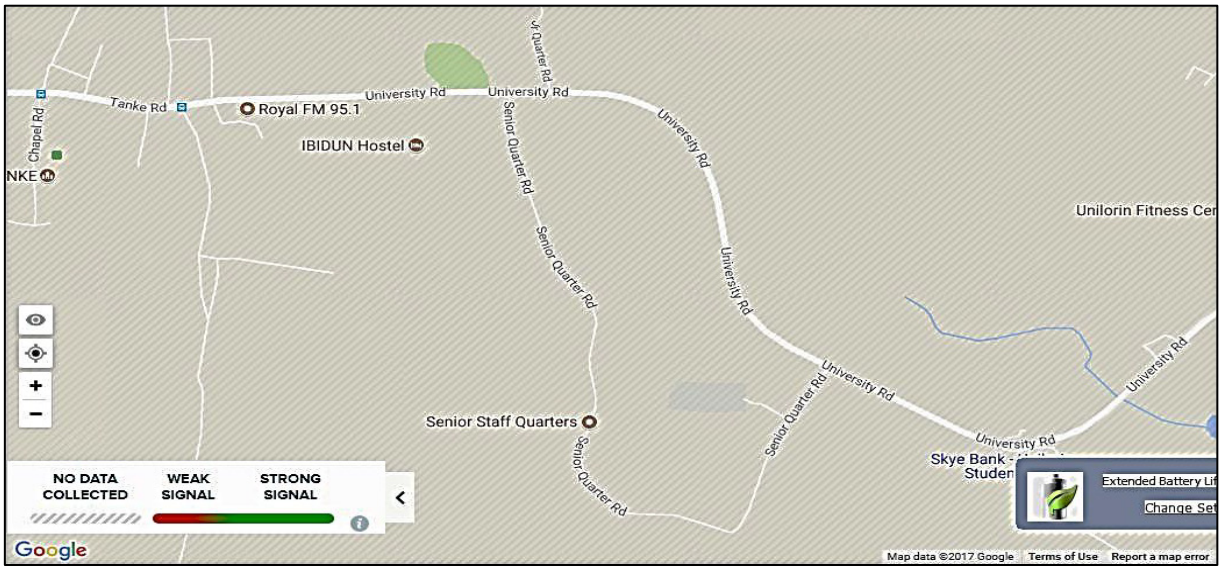


Fig. 2. Open Signal MNO A Report for Jalala and Senior Staff Quarters [12]

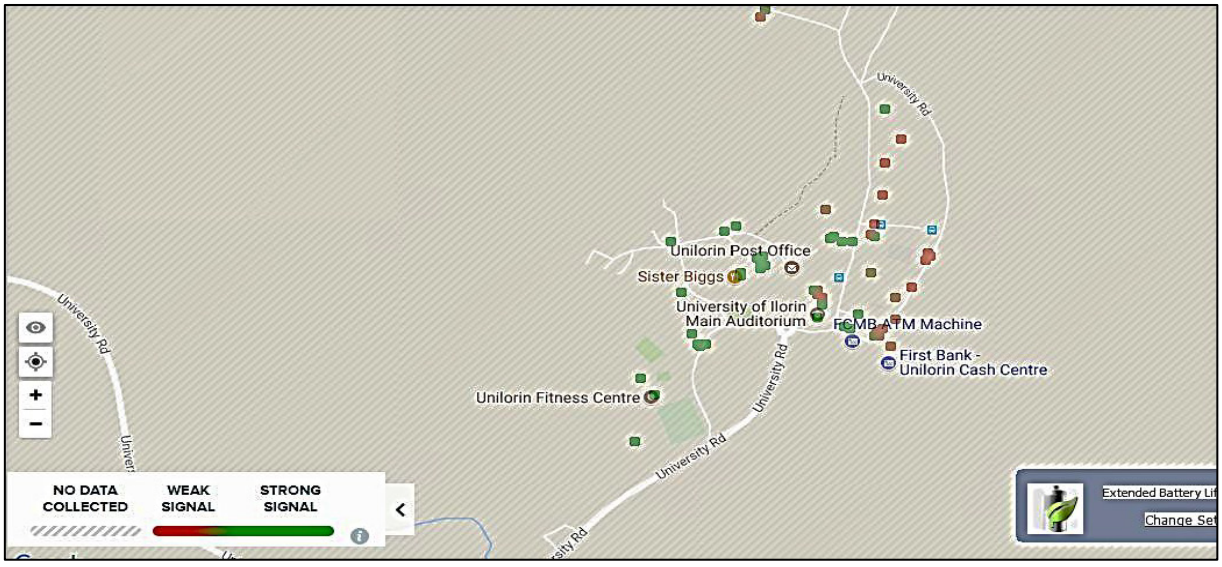


Fig. 3. Open Signal MNO A Report for Permanent Site [12]

Fig. 4. Open Signal Report for MNO B Signal Quality in Jalala [12]

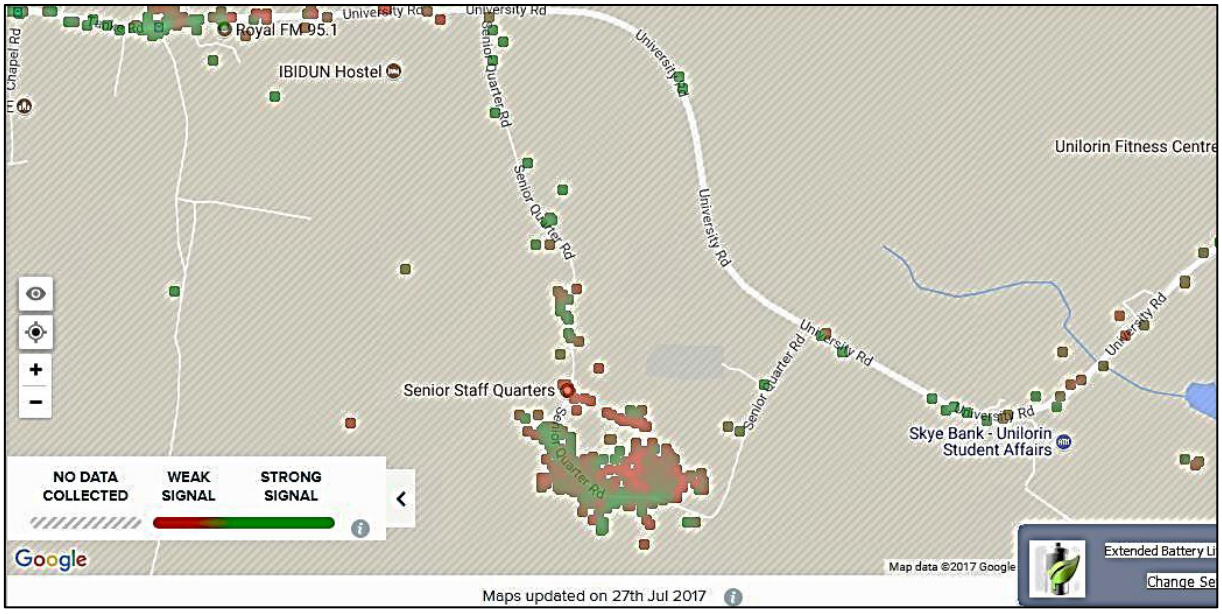


Fig. 5. Open Signal Report for MNO B Signal Quality in Staff Quarters [12]

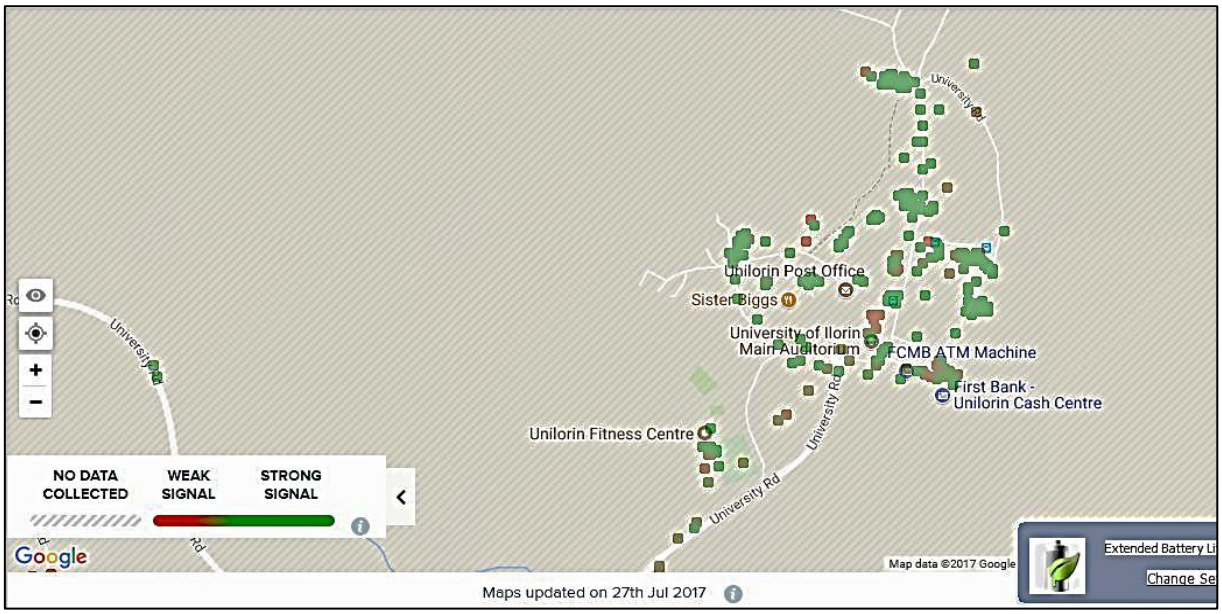


Fig. 6. Open Signal Report for MNO B Coverage in Permanent Site

2. LITERATURE REVIEW

The P3 connect mobile test company based in the United Kingdom stated in their 2016 report that the results got from their test in the United Kingdom that the service providers all comply with the standard set for them by the regulatory body in the country [13]. The benchmark test was carried out for the following network service providers: EE, Three, O_2 and Vodafone. They gave a summary report of the general test then further broke down the results based on voice and data communication separately. At the end of their report, they compared the result for 2016 with those they have gathered in past years and it was evident that the four major Network operators that were tested had improved in the overall quality of service they provide to the subscribers of their respective networks.

In Bangkok, two Authors came together to compare the performance of Third generation technologies for Internet services provided by the major network operators in Thailand. The paper focused on developing a conceptual framework for performance testing as well as Network Optimization, and performance comparison of 3G operations on 850/900 MHz and 2100 MHz bands in Thailand. The KPIs used during the course of their analyses were Throughput, Latency and data rates [14].

The authors in [15] examined the QoS of GSM network offered by four major network providers in Nigeria taking Ikorodu Axis as their case study. They studied the quality of service in voice call only over the four service providers; MTN, AIRTEL, GLOBACOMM and ETISALAT in some parts of Ikorodu Local Government Area,

Lagos State, Nigeria. They made use of TEMS 9.1 as their data collection software, Sony Ericsson C-702 and MapInfo Professional 11.0. Each mobile station was set to call for 90 seconds and a waiting period of 10 seconds was included in the control script. The authors analyzed their collected data using MapInfo and plotted graphs for the various KPIs and they did an analysis of bad patches.

The authors of [16] did an Evaluation and Optimization of the QoS that the mobile cellular networks in Nigeria are providing to the subscribers. They used an application called QVOICE with a pre-configured Nokia 6270i phone to collect necessary data. Five KPIs were the basis of the desired result for analysis, and they were Call Setup Success Rate (CSSR), Call Completion Rate (CCR), Call Handover Success Rate, Call Drop Rate and Standalone Dedicated Control Channel (SDCCH). The data collected was analyzed and Chi-test was performed to know the deviation from the set value by the NCC, and then transferred through SQL server for post-processing analysis. A conceptual framework was presented for Optimization using Adaptive Network-Based Fuzzy interference System (ANFIS).

A report was published in the International Journal of Research in Engineering and Technology by four authors on Optimizing radio frequency for improved QoS in Abeokuta, Nigeria [17]. The authors who carried out this research work collected data such as signal integrity, signal quality, interference, dropped calls, blocked calls, call statistics, service level statistics, QoS information and handover info among other data that were needed for thorough analysis to achieve their defined aim. They carried out drive test in defined areas to cover the Abeokuta metropolis using TEMS 9.0 and four TEMS enabled Sony Ericsson k800i. They divided the result type into two for Short and Long Calls. The short calls were used to check for Accessibility and Mobility while the Long calls were used to check retainablity and sustainability of calls.

3. METHODOLOGY

This study covered the analysis of real-time data recorded with the aid of a drivetest application while driving along the vehicle paths in the three selected locations within the University of Ilorin campus. The selected areas were Jalala Junior Staff Quarters (Jalala), University of Ilorin Senior Staff quarters and the University of Ilorin Main Campus (Permanent Site).

After the drivetest, post processing of the collected data was done and results discussed. Areas with bad coverage were highlighted and some possible reasons for the bad coverage were made known.

Data was collected with the aid of a drivetest and then saved as log files for further analysis to get desired results after the parameters have been defined.

Parameters that were considered in the course of this study include Call Setup Success Rate, call setup time, handover attempt, handover failure, HOSR, call attempt, Speech Quality Index (SQI), call drop, Received Signal Code Power (RSCP), Energy per Chip to Noise Ratio (Ec/No) and Received Signal Strength Indicator (RSSI).

The software that was used in the course of the study was licensed TEMS Investigation 15.2.2, MapInfo Professional 12.0, Snipping tool and Microsoft Excel.

The hardware or devices used were a laptop with Windows 7 Professional (Service Pack 1), a Global Positioning Service (GPS) device, four (4) Sony Ericsson W995 TEMS phone, USB hub, a car and a car Inverter for constant power supply to the laptop during the course of the drive.

It was noted that the total received signal power, i.e. RSSI, could not be considered as an indication of coverage in a WCDMA system. The RSCP value and the Ec/No are the values to put into consideration when working on the analysis of a WCDMA data.

The parameters recorded and evaluated that were used in measuring the QoS delivered were generally referred to as KPI.

3.1. KPIs Used and their Definitions

Call Setup Success Rate: Often referred to Accessibility KPI. It is a measure of the amount of calls that are successfully setup after attempt has been made on the call. If a call has been setup and later drops, the call has been successfully setup and connection has been made. When calls are not successfully setup, it is called Call block. Call could be blocked because of abnormal RRC (Radio Resource Control) connection release, no alerting/connection, no Radio bearer setup, and timer expiration among others. CSSR is It is expressed as a percentage of the ratio of Call Setup to the number of Call attempts.

Mathematically, $CSSR = \frac{Call\ Setup}{Call\ Attempt} \times 100$.

Call Drop Rate (CDR): Also referred to as Network retainability. The call drop rate is the rate at which calls drop after setup and assignment of channel has taken place. The rate at which calls drop depends on various factors such as failure to reestablish connection or other unspecified reasons. It is expressed as a percentage of the ratio of call drop to call setup.

Mathematically, $CDR = \frac{Call\ drop}{Call\ Setup} \times 100$.

Soft Handover Success Rate: This is the successful rate at which Radio Link is added, removed or replaced. It is the ratio of success of these to the failures expressed in percentage.

Call Setup Time: This is the time taken to setup the call after the attempt has been successfully made. Taking into consideration the benchmark set by the NCC for this KPI, which is that it must be less than 6secods. Hence, to include it in the calculation, the amount of call setup time less than 6 sec was expressed as a percentage of the total number of call setup time.

Coverage Reliability: The coverage reliability can be expressed as the reliability of the network for connection at any time. Connection is reliable at the Received Signal Code Power (RSCP) value. The benchmark set for this value by the NCC is –85dBm. Thus, the percentage coverage reliability was calculated as the sum of RSCP values greater than the set benchmark expressed as a percentage of the total.

The ranges used were as follows:
Min $\le x <$ –95
–95 $\le x <$ –85
–85 $\le x <$ –75
–75 $\le x <$ –65
–65 $\le x <$ –55
–55 $\le x <$ Max

Coverage Quality: This is the value of Energy per chip to Noise Ratio (Ec/No) greater than a desired value that guarantees optimum connectivity and quality. The coverage quality can be expressed in value as the percentage of number of values above the set threshold to the total number of values. For this project, a threshold of –10dBm was used.

The ranges used were as follows:
–34 $\le x <$ –10 (Bad)
–10 $\le x <$ –7 (Acceptable)
–7 $\le x <$ 0 (Good)

Speech Quality Index (SQI): It is a special attribute incorporated into the KPI value and being checked by TEMS for complete and efficient evaluation of the quality of voice signals heard or passed across a communication link during a particular call. It ranges from 0 to 30 with 0 been the poorest and 30 been the best.

–20 $\le x <$ 1 (Bad)
1 $\le x <$ 19 (Acceptable)
19 $\le x <$ 30 (Good)

The test was carried out in two phases, which were:
1) Data Collection phase;
2) Data Analysis phase.

In data collection phase, drivetest was performed and the software, TEMS Investigation, was used for the collection of data. TEMS Investigation is an active E2E test system, being used for verification, troubleshooting and optimization of services delivered in Radio Access Networks (RAN). It enables MNOs and infrastructure suppliers to test the quality of service they are delivering to subscribers. It covers in-vehicle, in-building, as well as the service quality received by pedestrians [18]. TEMS combines two key attributes – Speed and simplicity, to help in responding quickly to customer's complaints, while offering an unequalled ease of operation to users. TEMS Investigation 15.3 was installed on the laptop used for the study, as well as MapInfo Professional 12.0 and Microsoft Office Excel, 2016 edition for data analysis. The test could as well be carried out using a motorcycle or bicycle. Instead of drivetest, walktest could also be carried out.

The connections were made to a laptop with necessary software installed and TEMS License Key (Dongle) attached. A GPS device and Mobile stations were connected via USB. The GPS device connected to the laptop was placed on top of the car during the course of the drivetest to enable it to have a clearer view of the sky for more accurate results.

The collected data during drivetest data could be analyzed in real time during the test or after the test.

3.2. Drivetest Routes

Drivetest routes that indicated where testing would occur was defined based on several factors, mainly related to the purpose of the test. The drive routes showed the essential part of the area that must be covered, being the guide as to know which part had been covered and which part had not. Other places in the area might be tested as well based on the discretion.

Google Earth application was used in creating a drive route. The final image for drive route was taken to guide during drive test. Drivetest route chosen for this project were the Senior Staff Quarters of University of Ilorin (Figure 7), the University of Ilorin Main Campus Permanent Site (Figure 8) and the Jalala Junior Staff Quarters University of Ilorin (Figure 9).

3.3. The Drivetest

The drivetest was performed using two phones (one was making calls (CALL) from a specific number from time to time, while the other was maintained in IDLE mode). Thus, data were collected in IDLE and CALL modes for the network. The CALL duration were for short (30–60 seconds) and long (up to 180 seconds or more). Short calls checked the rate at which calls were successfully established and completed, while long calls checked the retainability of the network. Figure 10 shows a snippet of the voice call.

3.4. Data Collection Process

Before starting the drivetest, the worksheet to be used in monitoring the devices connected during the drive was created after launching TEMS Investigation 15.3, then the voice scripts to be used during the course of the drives.

The Road Map to use in knowing the path taken during the project and the cell file, which is the information about the BTS in the environment, were loaded and data were collected.

While driving, voice prompt on any activity was carefully attended to as it might had occurred as a result of disconnection of any of the devices, in which case the test would have to be rerun. Ongoing calls were allowed to end or stop the running script before stopping recording the logfile because the interruption might cause the call to be interpreted erroneously as dropped call.

Fig. 7. Staff Quarters Drive Route [18]

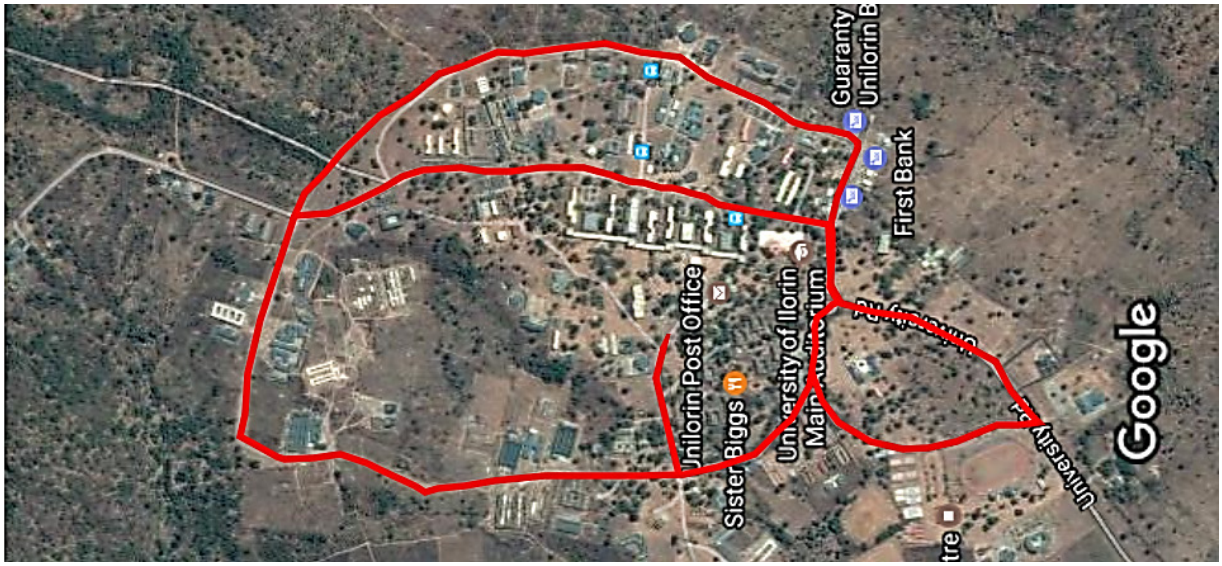


Fig. 8. Permanent Site Drive Route [18]

Fig. 9. Junior Staff Quarters Drive Route [18]

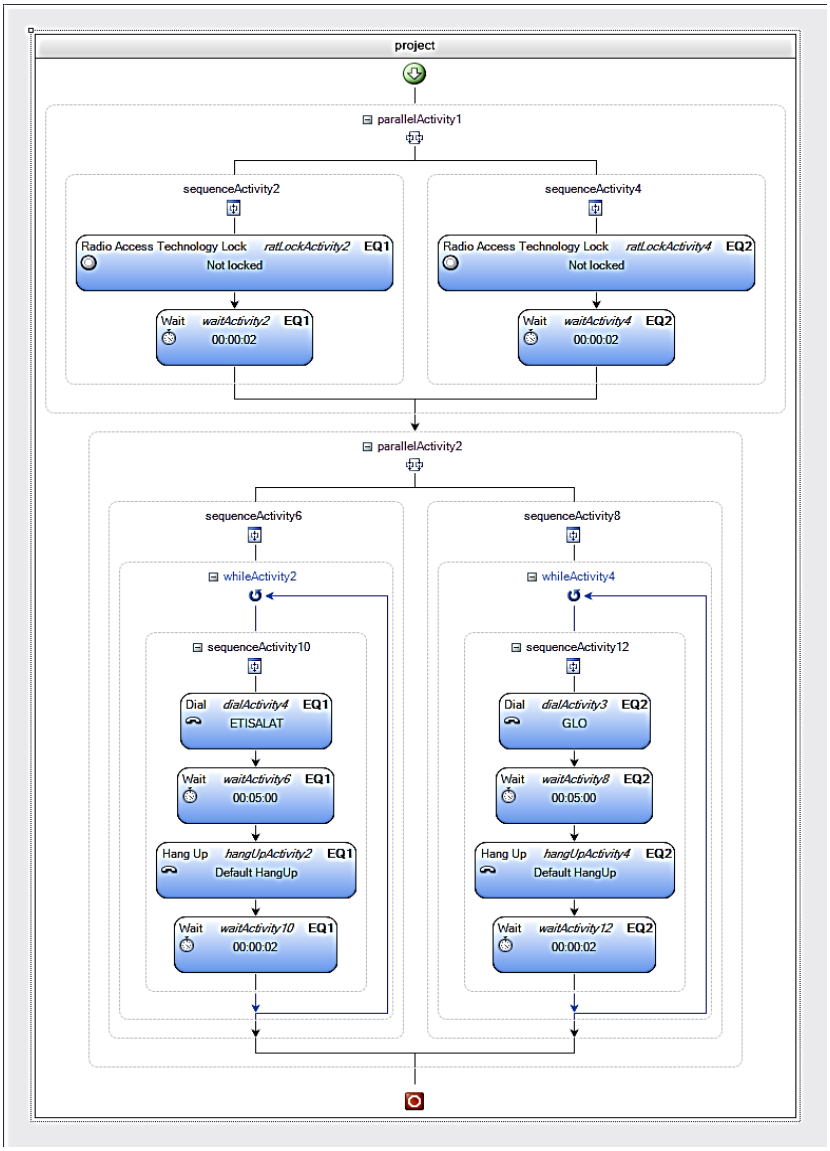


Fig. 10. Voice Call Snippet

4. RESULTS AND ANALYSIS

After the drivetest, the values of the RSCP, Ec/No, and SQI per location and per type of call for each MNO were plotted in MapInfo. For all Networks, there was 100 % success rate in the handover at all locations. Summary based on various KPI values, for all MNOs, were as seen in the Table 2.

TABLE 2. Summary KPI Values

PROVIDERS		MTN	Etisalat	Airtel	Glo	MTN	Etisalat	Airtel	Glo	MTN	Etisalat	Airtel	Glo
№	KPI	*JALALA Long Call*				*JALALA Short Call*				*Permanent Site Long Call*			
1	% Call Setup Time MOC < 6 sec	25,00	0,00	100,00	0,00	75,00	50,00	100,00	8,33	92,31	81,82	100,00	50,00
2	% Coverage Reliability RSCP > –85dbm	53,41	52,35	60,24	41,49	57,21	65,04	75,28	25,42	89,79	69,22	93,85	90,62
3	% Coverage Quality (–10 ≤ Ec/No < 0 dB)	21,49	37,70	31,06	51,18	60,74	65,43	25,49	37,18	21,49	37,70	31,06	51,18
4	Accessibility (CSSR)	85,71	50,00	75,00	80,00	85,71	50,00	88,89	85,71	100,00	100,00	100,00	73,33
5	Retainability (100-Call Drop Rate)	33,33	100,00	100,00	50,00	83,33	100,00	87,50	83,33	92,31	100,00	100,00	72,73
6	Handover Success Rate	100,00	100,00	100,00	100,00	100,00	100,00	100,00	100,00	100,00	100,00	100,00	100,00
7	SQI	86,45	0,00	24,80	67,70	37,45	0,00	65,77	66,99	84,05	0,00	55,22	67,47

CONTINUE TABLE 2

	MTN	Etisalat	Airtel	Glo	MTN	Etisalat	Airtel	Glo	MTN	Etisalat	Airtel	Glo
№	*Staff Quarters Short Call*				*Staff Quarters Long Call*				*Permanent Site Short Call*			
1	85,71	0,00	N/A	20,00	80,00	100,00	100,00	40,00	100,00	71,43	100,00	29,17
2	58,96	53,69	99,51	42,66	57,55	62,34	76,86	88,77	99,92	70,58	91,08	86,29
3	57,65	54,20	95,19	84,51	61,48	63,57	55,71	84,68	58,15	39,47	51,34	51,34
4	100,00	66,67	0,00	100,00	100,00	100,00	100,00	100,00	12,96	89,47	6,25	76,67
5	100,00	100,00	0,00	100,00	92,31	100,00	100,00	72,73	100,00	100,00	100,00	78,26
6	100,00	100,00	N/A	100,00	100,00	100,00	100,00	100,00	100,00	100,00	100,00	100,00
7	74,97	0,00	0,00	77,92	82,63	0,00	50,40	87,45	17,05	0,00	0,00	61,27

4.1. Junior Staff Quarters

As obvious from the Table 2 as well Figure 11a and 11b, at Junior Staff Quarters, all the networks had poorer accessibility (accessibility is a measure of the CSSR for Short calls) compared to the benchmark set by NCC, which is 98 %. MNO A had 88 %, which was the highest value recorded. In this location, MNO B had the least Accessibility.

On the measure of how well a network retains connections without leading to a drop in the call, i. e. retainability, NCC set benchmark for this is that the drop call rate has to be less than or equal to 1 %. MNO B led here followed by MNO A then MNO C. MNO D retainability for this area is the poorest.

Combining results for the Long and Short calls, MNO C led in the quality of voice sent over link. MNO D came second; followed by MNO A. MNO B had the poorest SQI in this location as they had 0 % values in the acceptable range of SQI.

For both types of call, MNO D had the highest call setup time and MNO A had the least. Overall, MNO A came first with all its calls setup time taking less than 6 seconds. MNO D came second here; followed by MNO B. MNO C came last in this category.

Coverage category of the KPI is of two types, which are coverage reliability and quality. In reliability, MNO A led when the result of both call types were combined together, followed closely by MNO B. MNO D and MNO C were in 3rd and 4th positions respectively. As for the coverage quality, which is the Ec/No, MNO B led, followed by MNO C. MNO A had the least coverage quality.

Summary of the calls, considering KPI 1–7 values, were done for both senior Staff Quarters (Figure 11c and 11d) and the Permanent Site (Figure 11e and 11f) as well.

4.2. Senior Staff Quarters

Accessibility: MNO D and MNO C networks had 100 % accessibility for their subscribers. MNO A was least accessible.

Retainability: MNO D had the best retainability, followed by MNO C and MNO B. However, accessing MNO A was difficult; its retainability was 100 % once the call was setup.

SQI: In this environment, MNO C had the best speech quality from the calls. MNO D was close to MNO C in speech quality. MNO B's speech quality was poorest as there was no value greater than the acceptable KPI value for the network.

Call Setup time: Talking about the time taken to setup call on network in this location, MNO D was the best; followed by MNO A. MNO C was the worst among as a very low percentage of its calls took less than 6 seconds for setup.

Coverage: MNO C had the best coverage followed by MNO D and MNO B. The most reliable here was MNO A network, while MNO C had the best quality of coverage followed by MNO D.

4.3. Permanent Site

Accessibility: MNO B network was best accessible for the location, followed closely by MNO C. MNO D and MNO A had poor accessibility (MNO A had the poorest).

Retainability: MNO B and MNO A Networks were leading in this KPI in the Permanent Site environment. Though MNO D followed them closely, yet MNO C network also had an equally good retainability but are far from the NCC set benchmark. It had up to 11 % dropped call rate instead of 1 % specified.

SQI: MNO C led with the highest number of its SQI value in the acceptable range. MNO D followed MNO C network, though MNO D was having a widely varying value recorded. MNO B came last in the hierarchy of value.

Call Setup time: MNO A had the best call setup time, always less than 6 seconds. MNO D followed closely while MNO C had the lowest call setup duration.

Coverage: MNO D network had the best network coverage reliability followed by MNO A. In this category of KPI, MNO B had the least. The coverage quality was generally low across all networks. MNO C led followed by MNO A. MNO D was in the 3rd place.

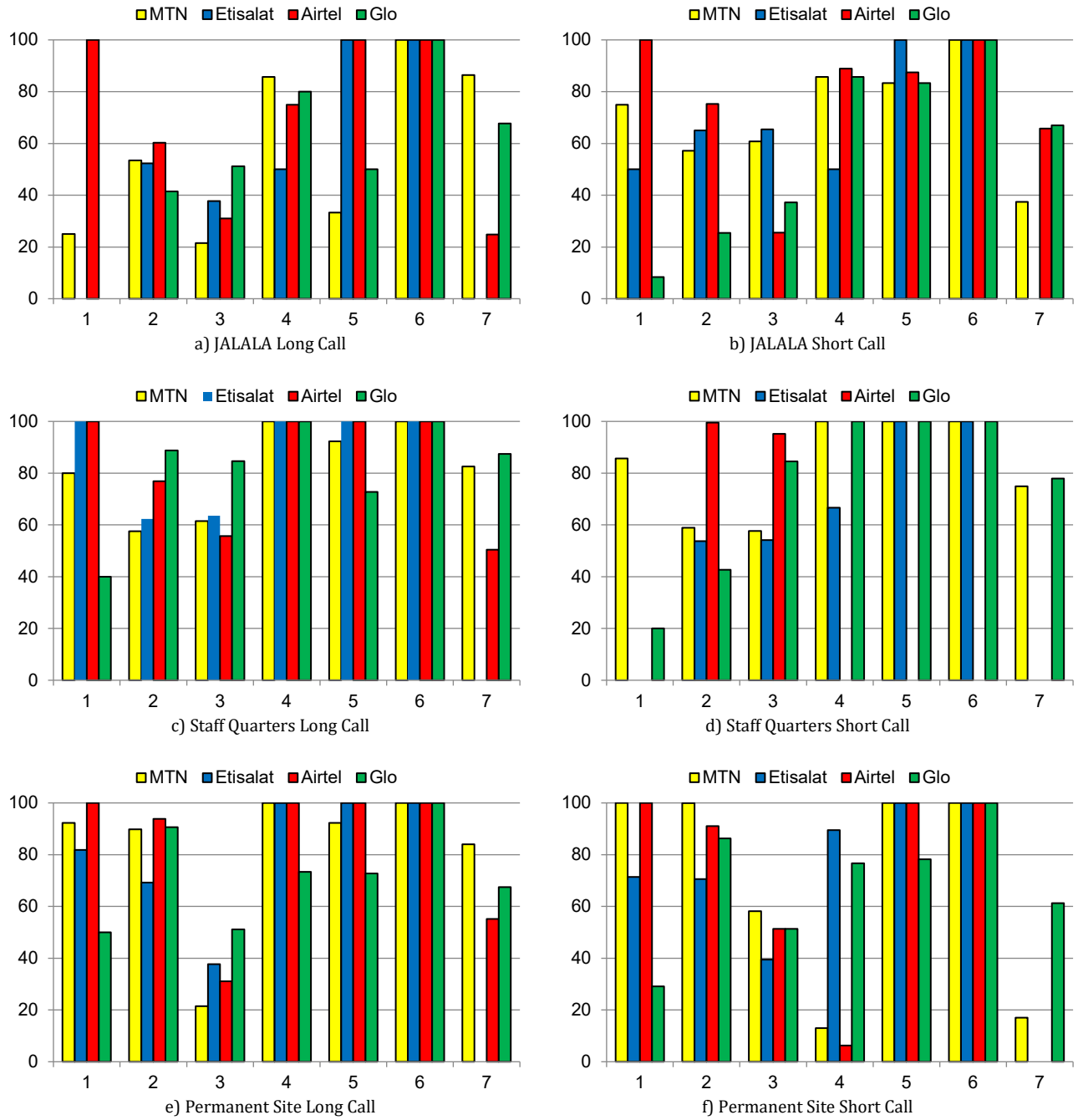


Fig. 11. Graphical Summary of the Calls

5. CONCLUSION

Evaluating the QoS delivered by the MNOs to the subscribers is as important as checking an area for the history of natural disaster before constructing a structure there. After evaluation and results provided, the MNOs that are rendering services in the area in question would be eager to improve on QoS in those areas should it be necessary. Naturally, MNOs should do random check in various areas to check the QoS they are providing to the populace as well as trying, in the least, conforming to the benchmark set by the NCC.

This study carried out created awareness about the QoS being rendered by various MNOs in the environs being considered. The results aid in deciding which of the MNOs to use in those locations.

Furthermore, the results buttressed the complaints by the subscribers. The results showed that the overall Network Quality index is poor because of the deviation from the benchmark set by the NCC is high in most cases of the network locations of the MNOs. There were also areas with “no service mode” reported as well as “limited service mode”. Therefore, there is need for government and the regulatory body to improve on monitoring and enforce compliance of MNOs to meet up with already set benchmark values.

References

1. Global Technology Archive. *History of Global System for Mobile Communication in Nigeria (GSM).* 2012. Available from: http://www.onlinenaijatech.blogspot.in/2012/06/history-of-global-system-for-mobile.html?m=1 [Accessed 25th September 2019]
2. Chindo S. Assessing the Impact of GSM Sub-Telecommunication Sector on the Teledensity Rate and Economic Growth in Nigeria: Time Series Analysis. *International Journal of Business and Social Science*. 2013;4(3).
3. Nigerian Communications Commission. *2013 Year End Subscriber/Network Data Report for Telecommunications Operating Companies in Nigeria.* 2013. Available from: https://www.ncc.gov.ng/docman-main/industry-statistics/research-reports/563-2013-year-end-subscriber-network-data-report/file [Accessed 25th September 2019]
4. Pesavento M., Mulder W. LTE Tutorial part 1. LTE Basics. *Proceedings of the Femto Forum Plenary, Reading, UK, June 2010*.
5. Laiho J., Wacker A., Novosad T. *Radio Network Planning and Optimisation for UMTS*. Chichester: John Wiley & Sons; 2006.
6. Chevallier C., Brunner C., Garavaglia A., Murray K.P., Baker K.R. *WCDMA (UMTS) Deployment Handbook. Planning and Optimization Aspects*. Chichester: John Wiley & Sons; 2006.
7. Holma H., Toskala A. *WCDMA for UMTS. Radio access for Third Generation Mobile Communications*. Chichester: John Wiley & Sons; 2005.
8. Ajibola A. *Nigerian Telecoms Firms Frustrate Subscribers*. 2015. Available from: https://iwpr.net/global-voices/nigerian-telecoms-firms-frustrate-subscribers [Accessed 25th September 2019]
9. Naij.com. *READ What Nigerians are Saying about MTN, GLO, AIRTEL and Others*. Available from: https://www.legit.ng/64171.html [Accessed 25th September 2019]
10. Adeyemi A., Nkechi O.U. NCC decries telecoms firms quality of service. *The Guardian*. 2017. Available from: https://m.guardian.ng/technology/ncc-decries-telecoms-firms-quality-of-service [Accessed 25th September 2019]
11. The Federal Government Printer. Nigerian Communications Act: Quallty of Service Regulations. *Federal Republic of Nigeria Official Gazette.* 2013:B133–B166.
12. Opensignal. *Coverage Maps*. Available from: https://opensignal.com/networks/nigeria/airtel-coverage [Accessed 25th September 2019]
13. P3 Connect. *The 2016 Mobile Network Test in the United Kingdom.* Available from: https://www.p3-group.com/en/wp-content/uploads/2016/11/Report-UK-2016.pdf [Accessed 25th September 2019]
14. Chimmanee S., Jantavongso S. The performance comparison of third generation (3G) technologies for internet services in Bangkok. *J. Inf. Commun. Technol.* 2016;15:1–31.
15. Ogunleye A.O., Soewu A., Makanjuola N.T. QoS – Comparative Management and Evaluation of GSM Telephone System in Nigeria. *The Pacific Journal of Science and Technology (PJST).* 2016;17(2):134–163.
16. Alexander N.N., Anthony U.O., Emmanuel O.I., Davies K.N. Evaluation and Optimization of Quality of Service (QoS) of Mobile Cellular Networks in Nigeria. *International Journal of Information and Communication Technology Research.* 2013:3(9): 277–282.
17. Oseni O.F., Popoola S.I., Enumah H., Gordian A. Radio frequency optimization of mobile networks in Abeokuta, Nigeria for improved quality of service. *International Journal of Research in Engineering and Technology.* 2014;3(8):174–180.
18. *Google Maps* (n.d.). Available from: http://www.maps.google.com [Accessed 25th September 2019]

* * *

АНАЛИЗ КАЧЕСТВА ОБСЛУЖИВАНИЯ ПОЛЬЗОВАТЕЛЕЙ WCDMA ПРИ РАЗЛИЧНОЙ ДИСЛОКАЦИИ: ПОИСКОВОЕ ИССЛЕДОВАНИЕ УНИВЕРСИТЕТА ИЛОРИНА, НИГЕРИЯ

О.А. Тиамийу[1]

[1]Университет Илорина
1515, Илорин, Нигерия

Информация о статье
УДК 621.39.82
Статья поступила в редакцию 03.06.2019

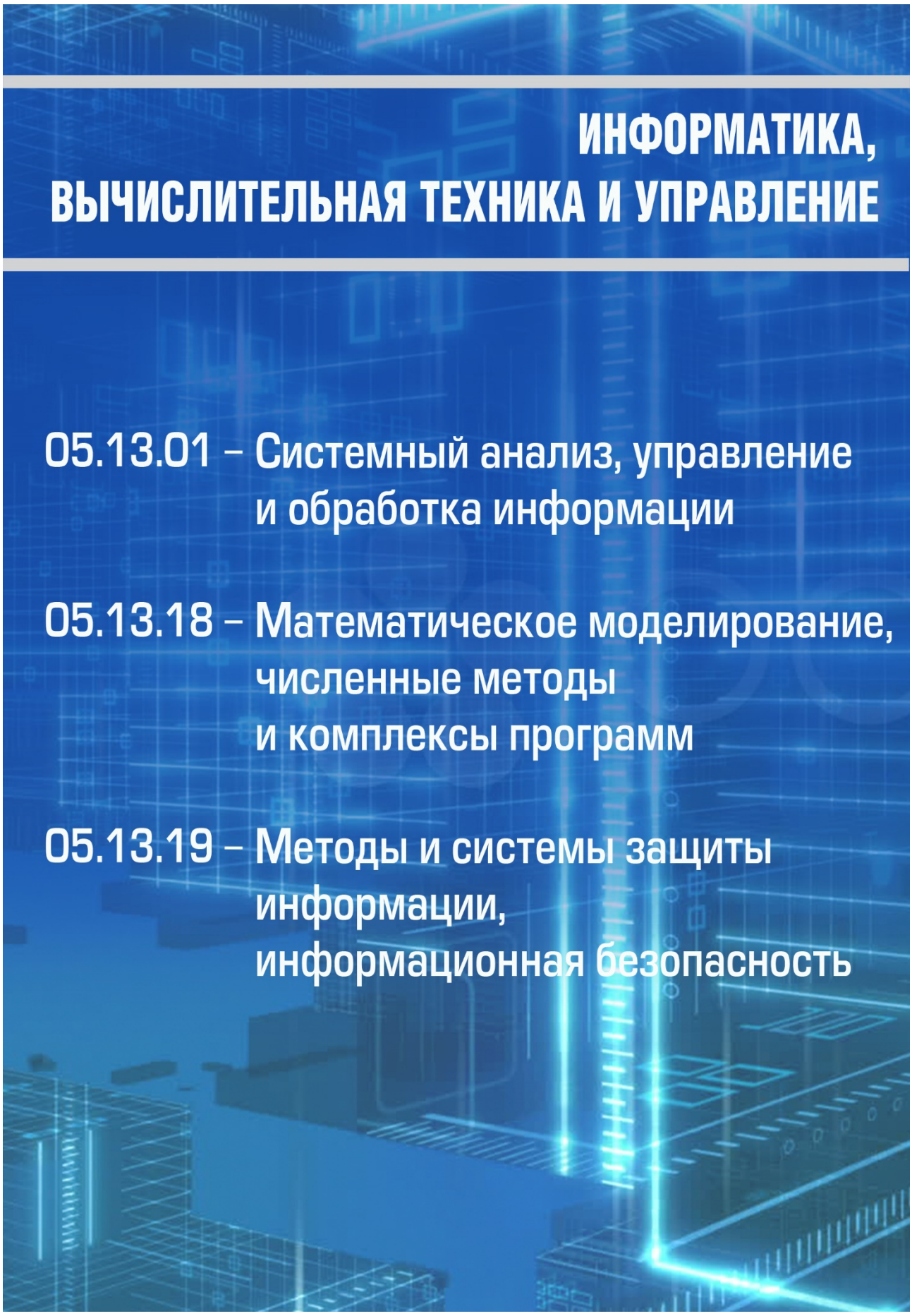
Ссылка для цитирования: Тиамийу О.А. Анализ качества обслуживания пользователей WCDMA при различной дислокации: поисковое исследование университета Илорина, Нигерия // Труды учебных заведений связи. 2019. Т. 5. № 3. С. 45–56. DOI:10.31854/1813-324X-2019-5-3-45-56

Аннотация: *С 2001 года, ознаменовавшего появление современной телефонии в Нигерии, наблюдается значительное увеличение пропускной способности операторов мобильных сетей. Согласно отчетам Нигерийской комиссии по связи (NCC), регулирующего органа в Нигерии, общее количество подключенных активных линий составило более ста миллионов. Тем не менее, пользователи мобильных телефонов в стране получают низкое качество обслуживания в разных местах страны. Таким образом, NCC установил контрольные значения для различных показателей. В этом исследовании, проведенном в университете Илорина, будут сделаны выводы о качестве услуг, предоставляемых пользователям диапазона WCDMA операторами мобильной связи при различной дислокации пользователей.*

Ключевые слова: *операторы сетей мобильной связи, пропускная способность, WCDMA, качество обслуживания, дислокация пользователей, университет Илорина*

Список используемых источников

1. History of Global System for Mobile Communication in Nigeria (GSM) // Global Technology Archive. 2012. URL: http://www.onlinenaijatech.blogspot.in/2012/06/history-of-global-system-for-mobile.html?m=1 (дата обращения 25.09.2019)
2. Chindo S. Assessing the Impact of GSM Sub-Telecommunication Sector on the Teledensity Rate and Economic Growth in Nigeria: Time Series Analysis // International Journal of Business and Social Science. 2013. Vol. 4. Iss. 3.
3. *2013 Year End Subscriber/Network Data Report for Telecommunications Operating Companies in Nigeria* // Nigerian Communications Commission. 2013. URL: https://www.ncc.gov.ng/docman-main/industry-statistics/research-reports/563-2013-year-end-subscriber-network-data-report/file (дата обращения 25.09.2019)
4. Pesavento M., Mulder W. LTE Tutorial part 1. LTE Basics // Proceedings of the Femto Forum Plenary, Reading, UK, June 2010.
5. Laiho J., Wacker A., Novosad T. Radio Network Planning and Optimisation for UMTS. Chichester: John Wiley & Sons, 2006.
6. Chevallier C., Brunner C., Garavaglia A., Murray K.P., Baker K.R. WCDMA (UMTS) Deployment Handbook. Planning and Optimization Aspects. Chichester: John Wiley & Sons, 2006.
7. Holma H., Toskala A. WCDMA for UMTS. Radio access for Third Generation Mobile Communications. Chichester: John Wiley & Sons, 2005.
8. Ajibola A. Nigerian Telecoms Firms Frustrate Subscribers. 2015. URL: https://iwpr.net/global-voices/nigerian-telecoms-firms-frustrate-subscribers (дата обращения 25.09.2019)
9. READ What Nigerians are Saying about MTN, GLO, AIRTEL and Others // Naij.com. URL: https://www.legit.ng/64171.html (дата обращения 25.09.2019)
10. Adeyemi A., Nkechi O.U. NCC decries telecoms firms quality of service. *The Guardian*. 2017. Available from: https://m.guardian.ng/technology/ncc-decries-telecoms-firms-quality-of-service (дата обращения 25.09.2019)
11. The Federal Government Printer. Nigerian Communications Act: Quality of Service Regulations // *Federal Republic of Nigeria Official Gazette.* 2013. PP. B133–B166.
12. Coverage Maps // Opensignal. URL: https://opensignal.com/networks/nigeria/airtel-coverage (дата обращения 25.09.2019)
13. The 2016 Mobile Network Test in the United Kingdom // P3 Connect. URL: https://www.p3-group.com/en/wp-content/uploads/2016/11/Report-UK-2016.pdf (дата обращения 25.09.2019)
14. Chimmanee S., Jantavongso S. The performance comparison of third generation (3G) technologies for internet services in Bangkok // J. Inf. Commun. Technol. 2016. Vol. 15. PP. 1–31.
15. Ogunleye A.O., Soewu A., Makanjuola N.T. QoS – Comparative Management and Evaluation of GSM Telephone System in Nigeria // The Pacific Journal of Science and Technology (PJST). 2016. Vol. 17. Iss. 2. PP. 134–163.
16. Alexander N.N., Anthony U.O., Emmanuel O.I., Davies K.N. Evaluation and Optimization of Quality of Service (QoS) of Mobile Cellular Networks in Nigeria // International Journal of Information and Communication Technology Research. 2013. Iss. 3(9). PP. 277–282.
17. Oseni O.F., Popoola S.I., Enumah H., Gordian A. Radio frequency optimization of mobile networks in Abeokuta, Nigeria for improved quality of service // International Journal of Research in Engineering and Technology. 2014. Vol. 3. Iss. 8. PP. 174–180.
18. Google Maps (n.d.). URL: http://www.maps.google.com (дата обращения 25.09.2019)



DOI:10.31854/1813-324X-2019-5-3

МЕТОДИКА МНОГОАСПЕКТНОЙ ОЦЕНКИ И КАТЕГОРИЗАЦИИ ВРЕДОНОСНЫХ ИНФОРМАЦИОННЫХ ОБЪЕКТОВ В СЕТИ ИНТЕРНЕТ

А.А. Браницкий[1*], **И.Б. Саенко**[1]

[1]Санкт-Петербургский институт информатики и автоматизации Российской академии наук, Санкт-Петербург, 199178, Российская Федерация
*Адрес для переписки: alexander.branitskiy@gmail.com

Информация о статье
УДК 004.056
Статья поступила в редакцию 30.04.2019

Ссылка для цитирования: Браницкий А.А., Саенко И.Б. Методика многоаспектной оценки и категоризации вредоносных информационных объектов в сети Интернет // Труды учебных заведений связи. 2019. Т. 5. № 3. С. 58–65. DOI:10.31854/1813-324X-2019-5-3-58-65

Аннотация: *В условиях быстрого развития информационных технологий возникает задача, связанная с обнаружением источников вредоносной информации в сети Интернет. Для ее решения могут применяться методы машинного обучения как один из наиболее популярных и мощных инструментов, предназначенных для выявления зависимостей между входными (наблюдаемыми) данными и выходными (желаемыми) результатами. В данной статье представлена методика, направленная на многоуровневую обработку входных данных о вредоносных информационных объектах в сети Интернет и обеспечивающая их многоаспектную оценку и категоризацию с использованием методов машинного обучения. Цель исследования заключается в повышении эффективности процесса обнаружения вредоносной информации в сети Интернет на примере задачи классификации веб-страниц.*

Ключевые слова: *информационные объекты, вредоносная информация, классификаторы, веб-страницы, многоуровневая схема комбинирования.*

Введение

Современная глобальная сеть содержит огромное количество разнородной информации, которая по своему содержанию может рассматриваться как вредоносная. Обнаружение источников является важной задачей, поскольку их распространение и использование может приводить к серьезным негативным последствиям как на локальном уровне, затрагивающем интересы и права отдельных лиц, так и на глобальном уровне, находящем отражение в международных разногласиях и конфликтах.

В качестве примера обнаружения вредоносных информационных объектов (ИО), можно привести системы родительского контроля. В роли ИО в таких системах выступает информация, предоставляемая такими Интернет-сервисами, как веб-сайты, социальные сети, онлайн-чаты, игровые и медиапорталы и другие. В этом случае запрещение доступа к ИО выполняется на основе анализа потоков данных, передаваемых от соответствующего Интернет-ресурса к конечному пользователю. Признаком для такого запрета может являться наличие вредоносной информации, содержащей, например, ненормативную лексику, призывы к противоправным действиям или указания, пропагандирующие нездоровый образ жизни.

Саму задачу обнаружения вредоносной информации можно рассматривать как задачу категоризации ИО, в которой заранее определены нелегитимные категории. Системы, предназначенные для решения этой задачи, могут быть основаны как на ручном построении классификационных правил, так и с привлечением автоматических средств их генерации. Именно последний тип подобных систем представляет наибольший интерес со стороны исследователей в связи с постоянным ростом, развитием и популяризацией такого перспективного научного направления, как машинное обучение.

В статье рассматривается вопрос повышения показателей эффективности обнаружения вредоносных ИО на примере задачи классификации веб-страниц с использованием различных методов машинного обучения и их комбинирования.

Релевантные работы

Задача обнаружения вредоносной информации в сети Интернет может быть сведена к классификации веб-страниц, в которой ряд категорий заранее определен системным администратором как содержащий нелегитимный контент. В этой области существует множество работ, посвященных построению, как экспертных систем, так и полностью автоматических систем.

Представленная в [1] система CONSTRUE основана на продукционных правилах, создаваемых вручную оператором-экспертом. Данная система предназначена для классификации экономических и финансовых новостей и соотнесения анализируемого текста к одной из 674 категорий. Точность классификации для системы CONSTRUE составляет более 90 %. Недостаток такой системы заключается в том, что ее поддержание в консистентном состоянии требует регулярного привлечения специалистов, выполняющих добавление и корректирование продукционных правил.

Подход к категоризации содержимого с автоматической генерацией правил классификации рассматривается исследователями C. Apté, F. Damerau и S.M. Weiss [2]. Предлагаемый ими формат правил – дизъюнктивная нормальная форма (ДНФ). Алгоритм формирования правил основан на последовательной замене одного из конъюнктов и дальнейшем добавлении нового конъюнкта до тех пор, пока не будет построено стопроцентное покрытие обучающей выборки (т. е. такой набор правил, которые будут обеспечивать безошибочную классификацию обучающих элементов). Данный алгоритм выполняет эвристический поиск таких правил: алгоритм не обеспечивает нахождение минимальной по количеству конъюнктов ДНФ. Кроме того, в отличие от дерева решений конъюнкты, объединенные одним правилом при помощи этого алгоритма, не являются взаимоисключающими.

В качестве элементарных конъюнктов (атомов) использовались предикаты, отражающие признаки:

1) вхождения определенного слова (или словосочетания) из локального словаря (набора слов, содержащего специфичные для одной категории понятия) в анализируемый текст;

2) превышения частоты встречаемости определенного выражения внутри анализируемого текста на указанное пороговое значение.

Предложенный подход позволяет сохранить представление правил в формате, удобном для анализа экспертами. В то же время при описанном способе генерации правил теряются обобщающая способность системы и способность обработки зашумленных данных.

Авторы статьи [3] предлагают принять анализируемый документ как массив вещественнозначных коэффициентов, которые представляют собой относительные и абсолютные частоты вхождения определенных слов в классифицируемый текст. Среди таких коэффициентов были выделены:

– частота слова (TF, *от англ.* Term Frequency);

– обратная частота документа (IDF, *от англ.* Inverse Document Frequency);

– важность слова (TD, *от англ.* Term Discrimination), где TD = TF × IDF;

и некоторые другие.

В [4] изложен подход, который позволяет приписывать каждому слову его интегральный вес, включающий вероятность появления этого слова, как в рамках определенной категории, так и внутри всей коллекции документов, и с учетом остальных категорий.

Сравнение двух методов машинного обучения, а именно байесовского классификатора и дерева решений, в рамках задачи категоризации текста выполнено в [5]. Авторы этой статьи подчеркивают, что на крупных наборах обучающих данных лучшую производительность демонстрирует дерево решений, а на более мелких наборах данных – байесовский классификатор. Причем для байесовского классификатора с увеличением числа обрабатываемых признаков наблюдается ситуация переобучения (на контрольном множестве производительность классификатора снижается), а для дерева решений при этих же условиях и достаточном объеме обучающей выборки происходит увеличение показателей эффективности классификации.

Применимость другого популярного метода машинного обучения, а именно машины опорных векторов (МОВ), к задаче классификации текстов исследуется в статье T. Joachims [6], где автор выделяет способность МОВ обучаться как на высокоразмерных, так и на разреженных векторах признаков. Решение задачи классификации текстов в большинстве случаев имеет вид линейно разделимых областей, для обособления которых может использоваться МОВ.

В статье R. Johnson и T. Zhang [7] описываются два типа конволюционных нейронных сетей: прямое распространение сигнала и с преобразованием «мешка» слов (bag-of-words) на конволюционном слое. В результате экспериментов авторами было выявлено, что первый тип нейронной сети демонстрирует бóльшую производительность в терминах показателей классификации по сравнению со вторым типом нейронной сети.

В [8] представлен метод для извлечения признаков в рамках задачи категоризации текста. Предложенная модификация генетического алгоритма, как показывают эксперименты, позволяет добиться более компактного представления обучающих векторов в терминах их размерности и повысить качество классификации анализируемого текста.

Общим ограничением для вышеупомянутых работ, посвященных приложению методов машинного обучения к решаемой задаче, является приме-

нение односоставных классификаторов, что приводит к невозможности обучения модели по частям и, в свою очередь, затрудняет возможность распараллеливания этого процесса.

Анализ работ в данной предметной области показывает актуальность рассматриваемой темы. В то же время, несмотря на их разнообразие, задача разработки методики, предназначенной для обнаружения вредоносных ИО в сети Интернет и сочетающей в себе методы машинного обучения и их комбинирования, остается по-прежнему высокоприоритетным направлением в научно-исследовательском сообществе.

Многоаспектная оценка и категоризация вредоносных информационных объектов в сети Интернет

В разработанной авторами методике выделяется пять шагов (рисунок 1).

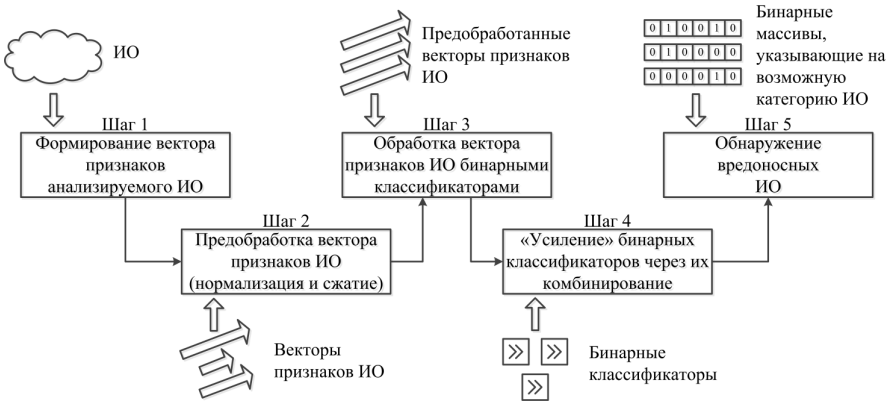


Рис. 1. Пошаговая схема методики многоаспектной оценки и категоризации вредоносных ИО в сети Интернет

На *первом шаге* осуществляется формирование вектора признаков ИО. *Второй шаг* направлен на выполнение процедуры предобработки созданного вектора признаков при помощи его покомпонентной нормализации и уменьшения размерности. На *третьем шаге* вектор признаков анализируемого ИО обрабатывается бинарными классификаторами. *Четвертый шаг*, «усиление» бинарных классификаторов, характеризуется их комбинированием в единый высокоуровневый классификатор, который предоставляет данные, необходимые на *пятом шаге* для формирования окончательного решения о наличии вредоносного содержимого внутри ИО. Вредоносность содержимого ИО задается через принадлежность ИО к одной из тех категорий, которые заранее были определены оператором системы как содержащие нелегитимную информацию.

На рисунке 2 представлена многоуровневая схема комбинирования классификаторов, покрывающая шаги 2, 3 и 4 в системе многоаспектной оценки и категоризации вредоносных ИО. Шаги 1 и 5 рассмотрены ниже в разделе «Эксперименты».

В рамках этой схемы выделяется три уровня:

1) предобработка входного объекта при помощи минимаксной (min-max) нормализации и метода главных компонент (МГК);

2) обработка входного объекта при помощи разнообразных базовых классификаторов, построенных на основе методов машинного обучения;

3) агрегирование базовых классификаторов через их композицию, представленную как метод взвешенного голосования (МВГ).

Первый уровень выполняет роль начальной подготовки обучающих и тестовых данных, подаваемых на вход базовых классификаторов. Каждый компонент обрабатываемого вектора масштабируется до неотрицательного значения, не превосходящего 1. Затем извлекаются наиболее информативные признаки. Они получаются как линейная комбинация обрабатываемого вектора и собственных векторов матрицы ковариации, сформированной на основе обучающего набора данных.

Второй уровень содержит пять базовых классификаторов: МОВ, метод k-ближайших соседей (МБС), наивный байесовский классификатор (НБК), линейную регрессию (ЛР) и дерево решений (ДР). Каждый из этих классификаторов является бинарным, т. е. предназначен для обособления объектов только одного фиксированного класса от других. Посредством использования таких классификаторов становится возможным легко и эффективно выполнять их параллельное обучение.

Предположим, что обучающий набор данных содержит m классов и представляется как набор пар:

$$(\boldsymbol{X}, \Omega) = \{(\boldsymbol{x_k}, c_k)\}_{k=1}^{M},$$

где $\boldsymbol{x_k} = (x_{k1}, \dots, x_{kn})^T \in \boldsymbol{X}$ – вектор признаков; c_k – присвоенная вектору $\boldsymbol{x_k}$ метка класса, такая, что $\exists \omega_j \in \Omega = \{\omega_1, \dots, \omega_m\}: \boldsymbol{x_k} \in \omega_j \wedge j = c_k$.

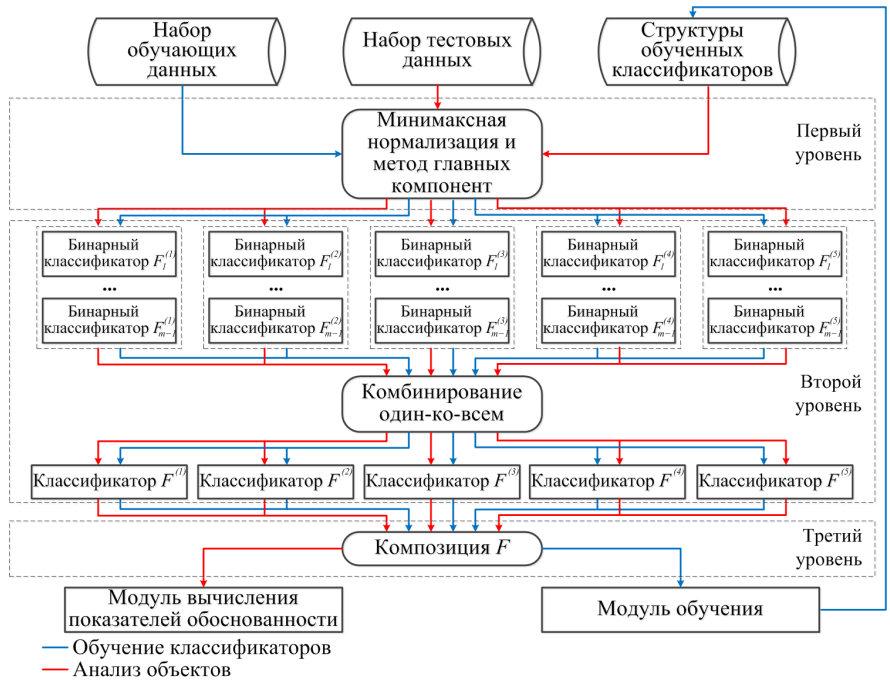


Рис. 2. Многоуровневая схема комбинирования классификаторов в системе многоаспектной оценки и категоризации вредоносных ИО в сети Интернет

В рамках схемы «один-ко-многим» бинарный классификатор $F_j^{(i)}: R^n \to \{0,1\}, (j = 1, \dots, m-1, m \geq 2; i = 1, \dots, 5)$, являющийся частью составного классификатора $F^{(i)}: R^n \to 2^{\{1,\dots,m\}}$, обучается на элементах $\{(\boldsymbol{x_k}, I(c_k = j))\}_{k=1}^{M}$, где I обозначает логическую функцию.

Функционирование составного классификатора $F^{(i)}$ может быть описано следующим образом:

$$F^{(i)}(\boldsymbol{z}) = \begin{cases} \{m\}, \text{если } \forall j \in \{1, \dots, m-1\}\, F_j^{(i)}(\boldsymbol{z}) = 0 \\ \left\{j \middle| F_j^{(i)}(\boldsymbol{z}) = 1\right\}_{j=1}^{m-1}, \text{иначе.} \end{cases}$$

В данной формуле первые $(m-1)$ бинарных классификаторов подвергаются объединению. Бинарные классификаторы $F_j^{(i)}$ настраиваются таким образом, чтобы их выходы равнялись 1, если индекс j соответствует метке класса c_k.

Объект $\boldsymbol{z}$ распознается как принадлежащий классу, промаркированному меткой m, если выходы всех $(m-1)$ бинарных классификаторов установлены в 0. В противном случае выход составного классификатора $F^{(i)}$ представляет собой множество тех меток классов, которые соответствуют индексам бинарных классификаторов с ненулевыми выходами.

Выбор схемы комбинирования «один-ко-многим» обусловлен тем фактом, что она направлена на объединение классификаторов, число которых прямо пропорционально количеству классов. В отличие от других популярных схем [9], таких как «один-к-одному» или направленный ациклический граф, которые обладают квадратичной зависимостью между указанными параметрами, схема «один-ко-многим» является особенно выигрышной в случае нескольких десятков классов.

Третий уровень – это композиция F, которая выражается как МВГ. Настроенный в процессе обучения этой композиции коэффициент w_i отражает вклад соответствующего составного классификатора $F^{(i)}$ в финальное решение о принадлежности анализируемого ИО к тому или иному классу.

Для систем, обеспечивающих поддержку предложенной методики, выделяется два режима: обучение классификаторов и анализ объектов. Первый начинается с загрузки обучающих данных и заканчивается сериализацией структур обученных классификаторов. Второй начинается с загрузки тестовых данных и структур обученных классификаторов и заканчивается вычислением показателей эффективности классификаторов. На рисунке 2 эти режимы обозначены синими (обучение классификаторов) и красными (анализ объектов) стрелками.

Эксперименты

В таблице 1 представлены размеры исследуемого набора данных [10] для каждой из 19 категории. Суммарная мощность исследуемого набора составляет 74893 записи, которые предварительно были разбиты по 19 категориям. Некоторые из них содержат вредоносный контент (например, marijuana, adult, violence) с точки зрения содержания. Сами записи представляют собой веб-страницы, доступные в сети Интернет (см. таблицу 2).

ТАБЛИЦА 1. Категории экспериментального набора и их мощность

№	Категория	Количество
1.	Adult / для взрослых	6748
2.	Alcohol / спиртные напитки	2802
…	…	…
9.	Jew Related / антисемитизм	3446
10.	Marijuana / марихуана	5365
…	…	…
17.	Violence / насилие	1892
18.	Weapon / оружие	2448
…	…	…

Формируемый вектор признаков содержит 402 компонента. При их вычислении использовались три типа исходных данных: URL-строка (адрес Интернет-ресурса), структура документа (статистические данные по HTML-тегам), извлеченный текст (полученный после удаления HTML-тегов).

В качестве показателей эффективности применялись следующие параметры: точность (PR, *от англ.* Precision,); полнота (RC, *от англ.* Recall); *F*-мера (FM, *от англ.* F-measure); аккуратность (AC, *от англ.* Accuracy). На рисунке 3 представлены значения этих показателей, вычисленные для каждого классификатора с использованием данных, не встречавшихся в процессе обучения. Для обучения использовалась выборка, размером приблизительно ¼ от всего набора данных. За счет комбинирования классификаторов при помощи МВГ показатель AC вырос более, чем на 1,5 % по сравнению с наибольшим значением аналогичного показателя, демонстрируемым среди базовых классификаторов, а именно ЛР. Кроме того, значения остальных показателей также увеличились: PR – на 2,63 %; RC – на 2,66 %; FM – на 2,65 %.

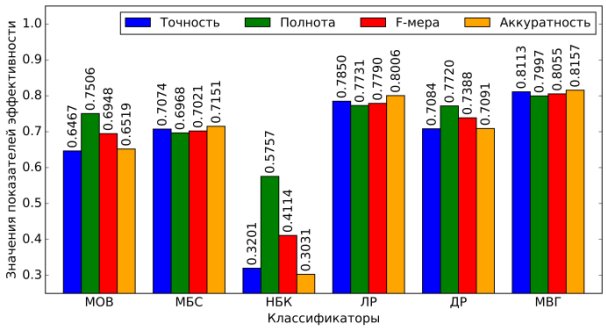


Рис. 3. Показатели эффективности, вычисленные на тестовом наборе данных

На рисунке 4 представлены временные характеристики процесса обучения для каждого классификатора и для различных размерностей входного вектора, полученного в результате сжатия при помощи МГК.

ТАБЛИЦА 2. Параметры веб-страницы

Номер	Описание	Тип исходных данных
1	Абсолютное число выбранных 15 тегов	Структура документа
2–16	Относительное число выбранных 15 тегов	Структура документа
17	Абсолютное число всех тегов	Структура документа
18	Абсолютное число атрибутов во всех тегах	Структура документа
19	Количество ссылок	Структура документа
20	Размер заголовка	Извлеченный текст
21	Размер отображаемого текста	Извлеченный текст
22	Длина комментариев	Структура документа
23–41	Логический признак вхождения имени каждой категории в заголовок	Извлеченный текст
42–60	Логический признак вхождения имени каждой категории в отображаемый текст	Извлеченный текст
61–250	Абсолютная частота вхождения каждого из 10 наиболее употребительных слов, характерных для каждой категории, в отображаемый текст	Извлеченный текст
251–269	Абсолютная суммарная частота вхождения 10 наиболее употребительных слов, характерных для каждой категории, в заголовок	Извлеченный текст
270–288	Абсолютная суммарная частота вхождения 10 наиболее употребительных слов, характерных для каждой категории, в URL	Извлеченный текст и URL-строка
289–345	Степень семантической схожести имени каждой категории с тремя наиболее употребительными словами, входящими в отображаемый текст анализируемого документа, в терминах word2vec [11]	Извлеченный текст
346–402	Степень семантической схожести словаря, состоящего из пяти наиболее употребительных слов в рамках каждой категории, с тремя наиболее употребительными словами, входящими в текст анализируемого документа, в терминах word2vec	Извлеченный текст

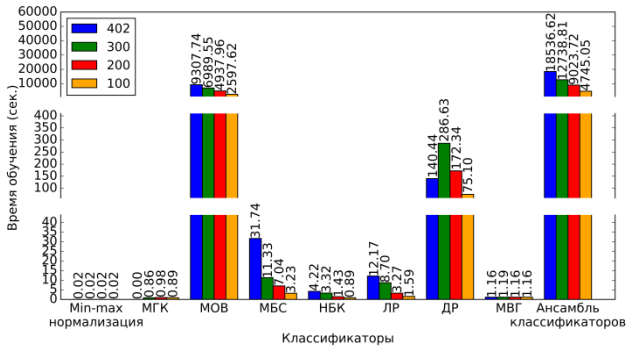


Рис. 4. Временные характеристики процесса обучения

Среди базовых классификаторов наименьшими временными затратами по обучению обладает НБК, а МОВ характеризуется наиболее длительным процессом обучения. Отметим, что изменение размерности признакового пространства прямо пропорционально влияет и на время обучения композиции классификаторов. Так, при сужении признакового пространства с 402 до 300 компонентов наблюдается уменьшение времени обучения ансамбля классификаторов в 1,46 раза, при сужении до 200 компонентов – в 2,05 раза, а до 100 компонентов – в 3,90 раза.

На рисунке 5 представлена зависимость времени, затраченного на анализ 74 893 векторов признаков при помощи каждого классификатора, от размерности обрабатываемого вектора.

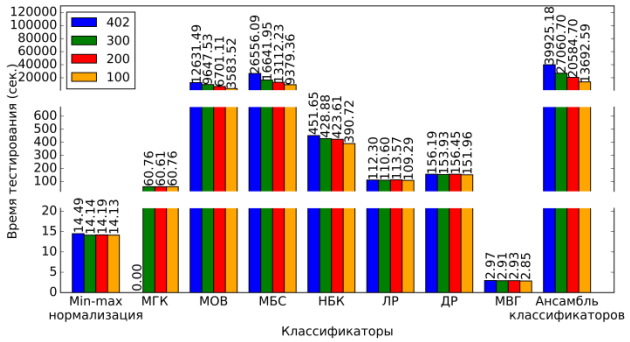


Рис. 5. Временные характеристики процесса анализа

По скорости анализа векторов среди базовых классификаторов наилучшей характеристикой обладает ЛР, на долю которой приходится от 2,8 % до 8 % времени от общего времени функционирования всего ансамбля классификаторов. Напротив, МБС является наиболее трудоемким и требует от 61,5 % до 68,5 % суммарного времени, расходуемого коллективом классификаторов (параметр k в МБС был выбран равным 10). Переход от 402-мерного к 100-мерному вектору признаков, анализируемому каждым базовым классификатором, привел к сокращению времени обработки (формирования результата классификации) этого вектора более чем в 2,9 раза. Таким образом, четырехкратное сжатие признакового пространства позволило сократить время обучения иерархического классификатора и время анализа входного вектора с его помощью почти в 4 и в 3 раза, соответственно.

На рисунке 6 представлена зависимость показателей эффективности, вычисленных для ансамбля классификаторов (композиции на основе МВГ), от размерности входного вектора признаков ИО.

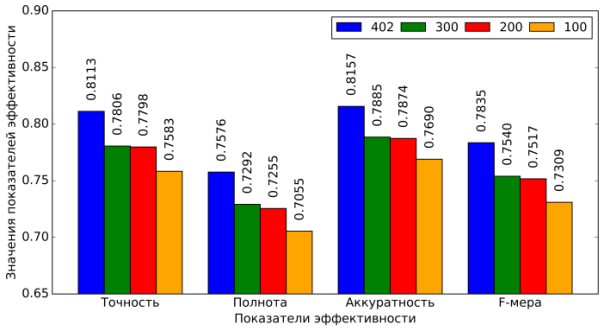


Рис. 6. Показатели эффективности, вычисленные на на основе МВГ

Как и следовало ожидать, с уменьшением размерности анализируемого вектора качество классификации по всем показателям уменьшается. Это обусловливается тем, что при переходе к суженному набору признаков теряется часть информации об исходных данных.

Для вычисления несмещенной оценки выбранных показателей эффективности использовалась пятиблочная кросс-валидация. Одновременно с этим размер обучающей выборки увеличился более чем в 3 раза, что позволило обеспечить лучшее покрытие тестового множества по сравнению со случаем, представленным на рисунке 3. На рисунке 7 представлены усредненные значения этих показателей вместе с отклонениями, обозначенными в виде вертикальных линий, пронизывающих каждый столбик гистограммы. Как видно из рисунка, наилучшими показателями эффективности обладает МВГ.

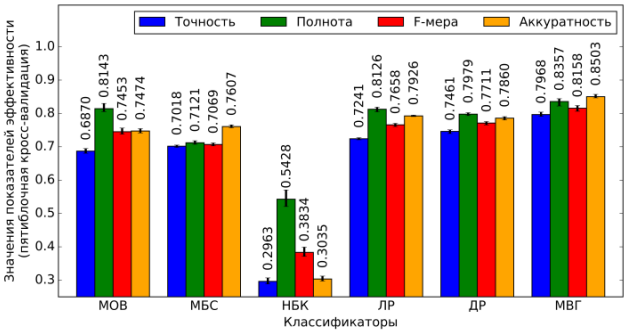


Рис. 7. Показатели эффективности, вычисленные при помощи пятиблочной кросс-валидации

На рисунке 8 показана зависимость времени обучения классификаторов и их ансамбля от числа используемых потоков. Сжатие векторов признаков осуществлялось до 100 компонент. В случае трех классификаторов (МОВ, МБС и ДР) наблюдается заметное снижение времени обучения с увеличением числа задействованных потоков.

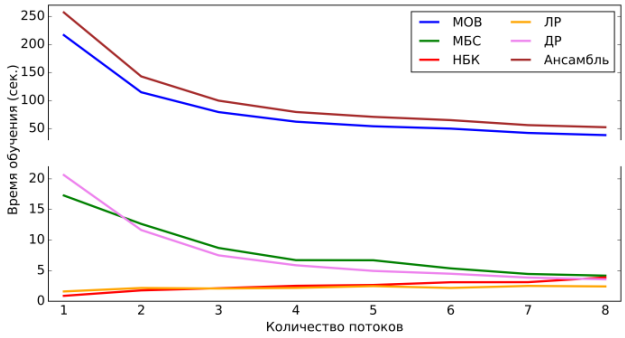


Рис. 8. Зависимость времени обучения базовых классификаторов и их коллектива от количества потоков

Для «быстро обучаемых» классификаторов (НБК и ЛР) такого существенного выигрыша нет. Это обосновывается тем, что прием распараллеливания является эффективным только тогда, когда время инициализации и планирования самого потока является несопоставимо малым по сравнению со временем выполнения самой задачи, запущенной в рамках созданного потока. Суммарное время обучения коллектива из 5 базовых классификаторов с использованием 8 потоков сократилось более чем в 4,9 раза по сравнению с однопоточным режимом.

Заключение

Представленная в статье методика отличается от существующих наличием многоуровневой схемы комбинирования бинарных классификаторов, а также сочетает в себе механизмы ускорения процесса обучения за счет распараллеливания и сжатия признакового пространства.

Многоаспектная категоризация обеспечивается за счет разностороннего анализа веб-документа согласно трем типам исходных данных, а именно URL-строки, структуры документа и извлеченного текста. Многоаспектность оценки обеспечивается за счет проведения разнообразных экспериментов, покрывающих как вычисление показателей эффективности, так и временных показателей, затраченных в процессе обучения классификаторов и анализа объектов. Показатель аккуратности был увеличен более чем на 1,5 % по сравнению с аналогичным показателем, демонстрируемым лучшим базовым классификатором, а именно ЛР. Использование 8 потоков привело к сокращению времени обучения коллектива классификаторов почти в 5 раз по сравнению однопоточным режимом. По скорости анализа векторов среди базовых классификаторов наилучшей характеристикой обладает ЛР. Напротив, МБС является наиболее трудоемким.

БЛАГОДАРНОСТИ

Работа выполнена при финансовой поддержке проекта РНФ № 18-11-00302 в СПИИРАН.

Список используемых источников

1. Hayes P.J., Andersen P.M., Nirenburg I.B., Schmandt L.M. TCS: a shell for content-based text categorization // Proceedings of the Sixth Conference on Artificial Intelligence Applications (Santa Barbara, USA, 5–9 May 1990). Piscataway, NJ: IEEE, 1990. Vol. 1. PP. 320–326. DOI:10.1109/CAIA.1990.89206

2. Apté C., Damerau F., Weiss S.M. Automated learning of decision rules for text categorization // ACM Transactions on Information Systems (TOIS). 1994. Vol. 12. Iss. 3. PP. 233–251. DOI:10.1145/183422.183423

3. Salton G., Buckley C. Term-weighting approaches in automatic text retrieval // Information Processing & Management. 1988. Vol. 24. Iss. 5. PP. 513–523. DOI:10.1016/0306-4573(88)90021-0

4. Fattah M.A. A Novel Statistical Feature Selection Approach for Text Categorization // Journal of Information Processing Systems. 2017. Vol. 13. Iss. 5. PP. 1397–1409.

5. Lewis D.D., Ringuette M. A Comparison of Two Learning Algorithms for Text Categorization // In: Third Annual Symposium on Document Analysis and Information Retrieval. 1994. PP. 81–93.

6. Joachims T. Text categorization with Support Vector Machines: learning with many relevant features // Proceedings of the 10th European Conference on Machine Learning (ECML, Chemnitz, Germany, 21–23 April 1998). Lecture Notes in Computer Science (Lecture Notes in Artificial Intelligence). Berlin, Heidelberg: Springer, 1998. Vol. 1398. PP. 137–142. DOI:10.1007/BFb0026683

7. Johnson R., Zhang T. Effective Use of Word Order for Text Categorization with Convolutional Neural Networks // Proceeding of the Annual Conference of the North American Chapter of the Association for Computational Linguistics "Human Language Technologies" (Denver, USA, 31 May – 5 June 2015). Stroudsburg: Association for Computational Linguistics, 2015. PP. 103–112. DOI:10.3115/v1/N15-1011

8. Ghareb A.S., Bakar A.A., Hamdan A.R. Hybrid feature selection based on enhanced genetic algorithm for text categorization // Expert Systems with Applications. 2016. Vol. 49. Iss. C. PP. 31–47. DOI:10.1016/j.eswa.2015.12.004

9. Lorena A.C., De Carvalho A.C., Gama J.M.P. A review on the combination of binary classifiers in multiclass problems // Artificial Intelligence Review. 2008. Vol. 30. Iss. 1–4. DOI:10.1007/s10462-009-9114-9

10. Kotenko I., Chechulin A., Shorov A., Komashinsky D. Analysis and Evaluation of Web Pages Classification Techniques for Inappropriate Content Blocking // Proceeding of the 14th Industrial Conference on Data Mining "Advances in Data Mining. Applications and Theoretical Aspects" (ICDM, St. Petersburg, Russia, 16–20 July 2014). Lecture Notes in Computer Science. Cham: Springer, 2014. Vol. 8557. PP. 39–54. DOI:10.1007/978-3-319-08976-8_4

11. Mikolov T., Chen K., Corrado G., Dean J. Efficient Estimation of Word Representations in Vector Space. 2013. URL: https://arxiv.org/pdf/1301.3781 (дата обращения 10.04.2019)

* * *

THE TECHNIQUE OF MULTI-ASPECT EVALUATION AND CATEGORIZATION OF MALICIOUS INFORMATION OBJECTS ON THE INTERNET

A. Branitskiy[1], **I. Saenko**[1]

[1]Saint-Petersburg Institute for Informatics and Automation of the Russian Academy of Sciences,
St. Petersburg, 193232, Russian Federation

Article info
The article was received 30 April 2019

For citation: Branitskiy A., Saenko I. The Technique of Multi-aspect Evaluation and Categorization of Malicious Information Objects on the Internet. *Proceedings of Telecommunication Universities*. 2019;5(3):58–65. (in Russ.) Available from: https://doi.org/10.31854/1813-324X-2019-5-3-58-65

Abstract: *Under the influence of rapid development in the sphere of information technologies, rises the challenge related to detection of malicious information sources on the Internet. To solve this we can use machine learning methods as one of the most popular and powerful tools designed to identify dependencies between input (observed) data and output (desired) results. This article presents a methodology which is aimed at multi-level processing of input data about malicious information objects on the Internet and providing their multi-aspect assessment and categorization using machine learning methods. The purpose of the investigation is to improve the efficiency of the detecting process of malicious information on the Internet using the examples of Web-pages classification..*

Keywords: *information objects, malicious information, classifiers, Web-pages, multi-level combination scheme.*

References

1. Hayes P.J., Andersen P.M., Nirenburg I.B., Schmandt L.M. TCS: a shell for content-based text categorization. *Proceedings of the Sixth Conference on Artificial Intelligence Applications, 5–9 May 1990, Santa Barbara, USA*. Piscataway, NJ: IEEE; 1990. vol.1. p.320–326. Available from: https://doi.org/10.1109/CAIA.1990.89206

2. Apté C., Damerau F., Weiss S.M. Automated learning of decision rules for text categorization. *ACM Transactions on Information Systems (TOIS)*. 1994;12(3):233–251. Available from: https://doi.org/10.1145/183422.183423

3. Salton G., Buckley C. Term-weighting approaches in automatic text retrieval. *Information Processing & Management*. 1988;24(5):513–523. Available from: https://doi.org/10.1016/0306-4573(88)90021-0

4. Fattah M.A. A Novel Statistical Feature Selection Approach for Text Categorization. *Journal of Information Processing Systems.* 2017;13(5):1397–1409.

5. Lewis D.D., Ringuette M. A Comparison of Two Learning Algorithms for Text Categorization. In: *Third Annual Symposium on Document Analysis and Information Retrieval*. 1994. p.81–93.

6. Joachims T. Text categorization with Support Vector Machines: learning with many relevant features. *Proceedings of the 10th European Conference on Machine Learning, ECML, 21–23 April 1998, Chemnitz, Germany. Lecture Notes in Computer Science (Lecture Notes in Artificial Intelligence).* Berlin, Heidelberg: Springer; 1998. vol.1398. p.137–142. Available from: https://doi.org/10.1007/BFb0026683

7. Johnson R., Zhang T. Effective Use of Word Order for Text Categorization with Convolutional Neural Networks. *Proceeding of the Annual Conference of the North American Chapter of the Association for Computational Linguistics " Human Language Technologies", 31 May – 5 June 2015, Denver, USA*. Stroudsburg: Association for Computational Linguistics; 2015. p.103–113. Available from: https://doi.org/10.3115/v1/N15-1011

113. Ghareb A.S., Bakar A.A., Hamdan A.R. Hybrid feature selection based on enhanced genetic algorithm for text categorization. *Expert Systems with Applications*. 2016:49(C):31–47. Available from: https://doi.org/10.1016/j.eswa.2015.12.004

9. Lorena A.C., De Carvalho A.C., Gama J.M.P. A review on the combination of binary classifiers in multiclass problems. *Artificial Intelligence Review*. 2008;30(1-4). Available from: https://doi.org/10.1007/s10462-009-9114-9

10. Kotenko I., Chechulin A., Shorov A., Komashinsky D. Analysis and Evaluation of Web Pages Classification Techniques for Inappropriate Content Blocking. *Proceeding of the 14th Industrial Conference on Data Mining "Advances in Data Mining. Applications and Theoretical Aspects", ICDM, 16–20 July 2014, St. Petersburg, Russia. Lecture Notes in Computer Science.* Cham: Springer; 2014. vol.8557. p.39–54. Available from: https://doi.org/10.1007/978-3-319-08976-8_4

11. Mikolov T., Chen K., Corrado G., Dean J. *Efficient Estimation of Word Representations in Vector Space.* 2013. Available from: https://arxiv.org/pdf/1301.3781 [Accessed 10th April 2019]

ПРЕДСТАВЛЕНИЕ СОВМЕСТНЫХ РАСПРЕДЕЛЕНИЙ НА ОСНОВЕ ПОКАЗАТЕЛЬНОГО И СТЕПЕННОГО ПРЕОБРАЗОВАНИЙ ПЛОТНОСТИ ИХ ЭНЕРГИИ В ЧАСТОТНО-ВРЕМЕННОМ ПРОСТРАНСТВЕ (завершение обзора)

С.В. Дворников[1*]

[1]Военная академия связи имени Маршала Советского Союза С.М. Буденного,
Санкт-Петербург, 194064, Российская Федерация
*Адрес для переписки: practicdsv@yandex.ru

Информация о статье
УДК 621.391
Статья поступила в редакцию 09.06.2019

Ссылка для цитирования: Дворников С.В. Представление совместных распределений на основе показательного и степенного преобразований плотности их энергии в частотно-временном пространстве: завершение обзора // Труды учебных заведений связи. 2019. Т. 5. № 3. С. 66–74. DOI:10.31854/1813-324X-2019-5-3-66-74

Аннотация: *Представлен аналитический обзор оригинальных методов повышения контрастности матриц совместных распределений за счет применения показательных и степенных преобразований плотности их энергии в частотно-временно́м пространстве. Приведены примеры моделирования, определяющие практическую направленность разработанных подходов. Даны рекомендации по их практическому применению.*

Ключевые слова: *частотно-временны́е распределения, степенные и показательные преобразования, методы вторичной обработки совместных распределений.*

Введение

Несмотря на то, что теорию билинейных распределений можно рассматривать как самостоятельное направление науки, ее методы продолжают совершенствоваться в соответствии с требованиями, определяемыми их практическим приложением. В их основе по-прежнему лежит методология совместной обработки плотности распределения энергии анализируемых процессов в частотновременно́й области, предложенная Cohen L. [1].

Следует отметить, что теоретическая база, разработанная в [2–13], достаточно активно используется в прикладных задачах радиотехники [14–34]. Вместе с тем исследования по вторичной обработке матриц совместных распределений энергии [6, 12, 13, 29] определили новое направление совершенствования форм их совместных представлений в частотно-временно́м пространстве, связанное с повышением контрастности компонент полезного сигнала. В частности, предложенную в [25] модификацию частотно-временны́х описаний нестационарных процессов на основе показательных и степенных функций.

Методы усовершенствования представлений сигналов на основе показательного и степенного преобразований совместных распределений плотности их энергии

В общем случае возможности псевдораспределений, описанные в работе Claasen T.A.C.M. и Meclenbrauker W.F.G. [30], не позволяют в полной мере обеспечить точное оценивание характеристик быстро изменяющихся процессов.

Прежде всего, это обусловлено тем, что в соответствии с принципом неопределенности Гейзенберга [5] уменьшение размера временно́го окна так, чтобы оно позволяло локализовать быстрые изменения сигналов, неизбежно приводит к снижению локализации плотности энергии вдоль линии их мгновенных частот. В результате, в условиях шумов инструментальная чувствительность псевдораспределений как инструмента анализа снижается и становится не пригодной к исследованию тонкой структуры обрабатываемых сигналов и энергетических процессов, поскольку возникающая при этом погрешность измерений превышает дисперсию разброса оцениваемой величины.

В целях борьбы с указанным негативным проявлением в [31, 32] предложены интересные подходы к улучшению в частотно-временны́х распределениях свойств локализации энергии сигналов вдоль линий мгновенных частот. В частности, в [17] для количественной оценки качества частотно-временны́х описаний предлагается использовать такие показатели, как глобальный и локальный разбросы энергии.

Однако их аналитическое вычисление является достаточно сложной задачей. Более того, даже для одного и того же совместного частотно-временно́го представления расчетные выражения и конечные значения этих показателей будут различаться в зависимости от вида сигнала [6].

Существенного улучшения характеристик частотно-временны́х описаний удалось достичь за счет применения методов совершенствования масштабно-временных распределений, использующих различные формы вейвлет-преобразований [34]. Более интересным в этом плане видится использование частотно-временны́х распределений (ЧВР) с адаптивным порогом отображения сигнальным компонентов [16]. Однако практическое применение такого подхода связано с определенными сложностями выбора уровня порога в условиях априорной неопределенности о значениях сигнальных и шумовых компонентов в матрице распределения.

Вместе с тем результаты исследования возможностей улучшения свойств совместных ЧВР по локализации энергии полезного сигнала в частотно-временно́м пространстве, проведенные в [1, 3, 23, 25, 29], показали, что в формируемой матрице распределения доминирующими являются сигнальные компоненты. Это явление объясняется корреляционной природой формирований ЧВР. Поскольку шумы не коррелированы, то на плоскости матрицы совместных представлений их компоненты распределяются равномерно, в то время как сигнальные компоненты локализуются вдоль линий их мгновенных частот.

Базируясь на указанных свойствах, желательно получить такое частотно-временно́е представление распределения энергии, которое позволило бы усилить доминирующие значения матрицы, принадлежащие полезным сигналам. Другими словами, целесообразно увеличить абсолютную разность между сигнальными и шумовыми компонентами на обрабатываемых формах ЧВР. В радиотехнике аналогичные функции выполняет операция нелинейного усиления.

Среди известных математических операций, позволяющих осуществить требуемое нелинейное усиление, можно выделить преобразования на основе степенных и показательных функций [25]. Аналитическое представление операции показательного преобразования имеет следующий вид:

$$\mathbf{W}_{\text{ПП}} = A^{\mathbf{W}}, \qquad (1)$$

где $\mathbf{W}$ – исходная матрица ЧВР; $\mathbf{W}_{\text{ПП}}$ – матрица ЧВР, усовершенствованная за счет применения операции показательного преобразования; A – основание преобразования.

Операции имеют следующий вид:

$$\mathbf{W}_{\text{СП}} = \mathbf{W}^{A}, \qquad (2)$$

где $\mathbf{W}_{\text{СП}}$ – матрица, усовершенствованная за счет применения операции степенного преобразования.

В общем случае методы усовершенствования равно обусловлены и их применение определяется конкретными условиями. В связи с этим рассмотрим особенности реализации указанных операций. Так, усовершенствование матриц на основе степенного преобразования позволяет получить большее различие между соседними компонентами (числовыми значениями) в области величин, близких к единице. Причем этот эффект усиливается при возрастании абсолютного значения основания преобразования.

В то же время для разделения близлежащих членов в области нулевого значения матрицы предпочтителен метод усовершенствования на основе показательного преобразования (рисунок 1).

Рис. 1. Нормированные функции степенного и показательного преобразование эталонного ряда

На рисунке 1 показаны функции, полученные на основе степенного и показательного преобразований с равным основанием эталонного ряда чисел $x = \{0;\ 0{,}1;\ \ldots;\ 0{,}9\}$. Применительно к частотно-временно́му анализу указанные функции можно рассматривать как результаты усовершенствования временного среза матрицы ЧВР. Тогда по оси абсцисс представлены элементы среза матрицы до усовершенствования $x = \{0;\ 0{,}1;\ \ldots;\ 0{,}9\}$, а по оси ординат – значения усовершенствованного ряда y после процедур степенного и показательного преобразований.

В интересах сравнения возможностей методов конечные результаты после операций усовершенствования дополнительно нормировались относительно своих максимальных значений. При усовершенствовании рассматривалось значение оснований $A = 10$.

Заметим, что выбор A близким к 1000 позволяет получить для функций показательного преобразования результат, сопоставимый со степенным преобразованием при $A = 10$. Однако применение больших величин для оснований A при степенных преобразованиях обосновано только в случае предварительного временно́го нормирования матриц [25]. Особую роль в указанных процедурах усовершенствования играет операция временно́го нормирования, заключающаяся в нормировании всех элементов матрицы ЧВР по частоте для каждого ее среза по времени.

В реальных каналах всегда присутствуют различного рода неоднородности, приводящие к искажению АЧХ тракта. Следовательно, амплитудные значения сигнала даже на несущей частоте в различные моменты времени будут иметь различные величины. Особенно это характерно для каналов с различного рода замираниями. Поэтому применение к такой матрице ЧВР-процедур степенного или показательного преобразования только усугубит имеющиеся различия между сигнальными компонентами, находящимися на различных позициях временны́х интервалов.

Во избежание указанных проблем в [25] предложено использовать процедуры временно́го нормирования матриц ЧВР. Применение указанной процедуры позволит обеспечить на энергетической плоскости распределений одинаковый уровень для максимальных компонент на каждом временно́м срезе. Таким образом, процедуры реализации метода можно свести к реализации следующих процедур:

– формирование (синтез) требуемого (заданного) ЧВР от обрабатываемой реализации;

– временно́е нормирование матрицы распределения энергии синтезированного ЧВР;

– вычисление степенного (показательного) преобразования над матрицей ЧВР обрабатываемого сигнала (процесса).

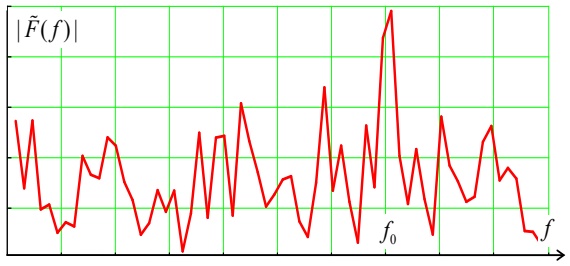
Результаты моделирования по реализации методов усовершенствования матриц ЧВР

Для демонстрации возможностей методов усовершенствования матриц ЧВР на основе применения к ним степенного и показательного преобразований проведено моделирование различных тестовых сигналов в условиях аддитивных шумов.

В качестве примера на рисунке 2 изображены спектры тестового сигнала $s(t)$, представляющего собой гармонический радиоимпульс. В частности, на рисунке 2а показан спектр тестового сигнала без шумов $|F(f)|$, а на рисунке 2б – спектр сигнала в шумах $|\tilde{F}(f)|$, из которого видно, что отношение сигнал/шум составило 8 дБ.

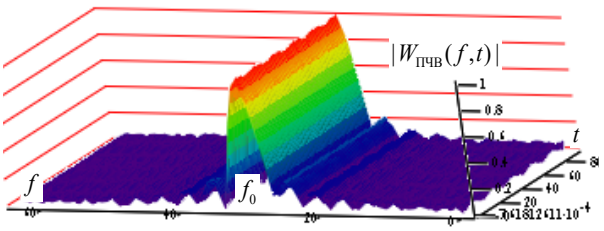
На рисунке 3 представлены ЧВР тестового сигнала в тех же условиях без шумов $W_{\text{ПЧВ}}(f,t)$ и в шумах $\tilde{W}_{\text{ПЧВ}}(f,t)$. В качестве ЧВР при моделировании использовано псевдочастотно-временно́е распределение (псевдо-ЧВР) Вигнера [30]. Очевидно, что при таком уровне шума линия мгновенной частоты в значительной степени неравномерна, что не позволяет на ее основе измерить значение несущей частоты даже на основе псевдо-ЧВР.

а)

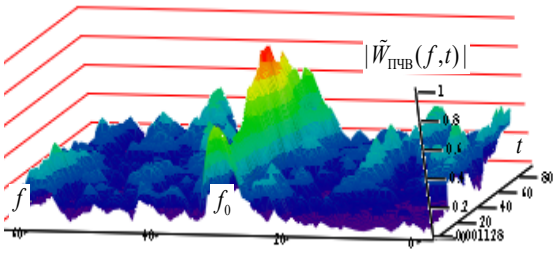


б)

Рис. 2. Спектр тестового сигнала без шумов (а) и в шумах (б)



а)



б)

Рис. 3. Псевдо-ЧВР Вигнера тестового сигнала без шумов (а) и в шумах (б)

Далее матрица псевдо-ЧВР Вигнера тестового сигнала была усовершенствована путем применения процедур временно́го нормирования (рисунок 4а) и затем дополнительно модифицирована за счет степенного преобразования (рисунок 4б). Даже визуальный анализ показывает, что применение процедур временно́го нормирования в значительной мере выровняло по уровню сигнальные компоненты вдоль линии мгновенной частоты (см. рисунок 4а), тем самым, обеспечив возможность проведения ее измерений на матрице псевдо-ЧВР.

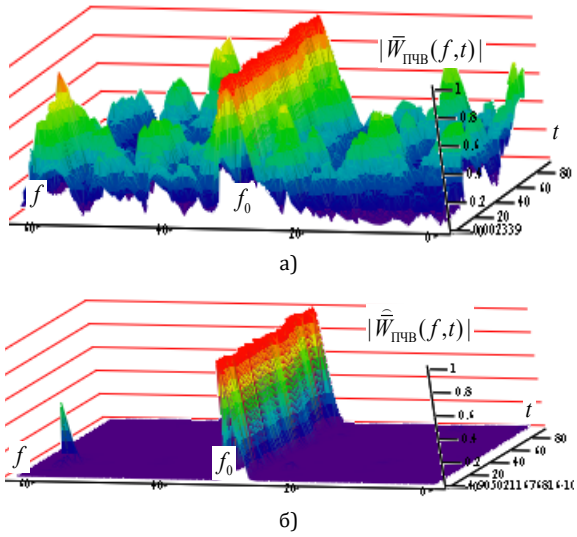


Рис. 4. Псевдо-ЧВР Вигнера тестового сигнала после процедур временно́го нормирования (а) и после процедур временно́го нормирования и степенного преобразования (б)

Следует отметить, что значения шумовых составляющих на матрице псевдо-ЧВР все еще велико и, следовательно, они будут затруднять выбор порога принятия решения при реализации более тонких процедур обработки. В то же время, последующие процедуры модифицирования усовершенствованной матрицы псевдо-ЧВР за счет процедур степенного преобразования (см. рисунок 4б) фактически полностью подавили шумовой фон.

В качестве примера на рисунке 5 изображены гистограммы распределений вдоль линий мгновенных частот (по оси *x* частотные значения представлены в виде дискретных отсчетов) абсолютных значений модифицированной усовершенствованной матрицы псевдо-ЧВР (по оси *y* представлены нормированные амплитудные значения матрицы в процентах от максимальной величины), превысивших порог по уровню 0,7 от наибольшего значения (истинное положение компонент тестового сигнала вдоль линии дискретных отсчетов $x = 30$.

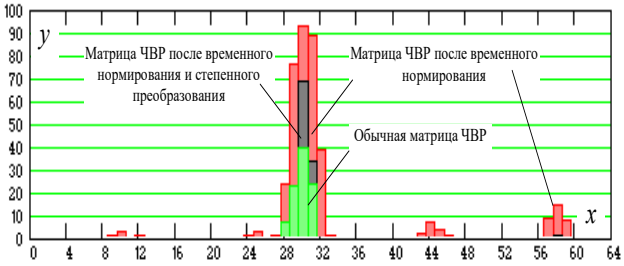


Рис. 5. Распределение сигнальных компонент тестового сигнала вдоль линий мгновенных частот

Теоретические предположения о положительных свойствах процедур степенных и показательных преобразований подтверждаются результатами практических экспериментов в [25]. При этом следует отдельно подчеркнуть значимость проведения процедур предварительного временно́го нормирования матриц распределений энергии. Именно данная процедура позволяет выровнять по уровню сигнальные компоненты вдоль линий мгновенных частот. Физическая сущность указанной операции аналогична работе автоматической регулировки усиления в каналах радиотехнических устройств с замираниями.

Вместе с тем, негативным моментом операции временно́го нормирования является значительная величина дисперсии в пределах каждого временно́го среза, что нежелательно при измерении и оценке спектральных компонентов. Для снижения негативных последствий применения процедур временно́го нормирования, целесообразно повышать уровень порога отображения результирующих значений, но при этом уменьшается и общая энергия сигнальных компонент.

Для демонстрации эффекта предложенных процедур модифицирования и усовершенствования матриц распределений энергии показаны двумерные (рисунки 6а, 6в и 6д) и трехмерные матрицы (рисунки 6б, 6г и 6е), полученные автором в [25].

Представленные результаты моделирования (матрицы распределения энергии) нормировались относительно их полной энергии. Основание степени преобразования в эксперименте выбиралось из условия:

$$\widetilde{W}_{\text{ПЧВ}}(f,t), \qquad (3)$$

при $A = 1000$.

Следует отметить, что для приведения матриц распределения энергии к условию (3) может потребоваться проведение дополнительных операций над каждым $K_{f,t}$-элементом матрицы. В частности, выполнения операции взятие модуля и умножения на число, которые в целом не искажают общей картины распределения энергетических компонент на матрице ЧВР.

Для оценки эффективности рассмотренных процедур модификации в качестве критерия степени различия/схожести с «идеальным ЧВР» в [25] предложен двумерный коэффициент корреляции $r_{\text{к}}$:

$$r_{\text{к}} = \frac{\sum_{m=1}^{M}\sum_{n=1}^{N}(w_{m,n}-\bar{w})\,(v_{m,n}-\bar{v})}{\sqrt{\left(\sum_{m=1}^{M}\sum_{n=1}^{N}(w_{m,n}-\bar{w})^2\right)\left(\sum_{m=1}^{M}\sum_{n=1}^{N}(v_{m,n}-\bar{v})^2\right)}}, \qquad (4)$$

где $\bar{w}$ и $\bar{v}$ – математические ожидания элементов матриц.

Использование критерия (4) позволяет достаточно отобразить продуктивность модифицирования. Так, на рисунке 7 представлены результаты сравнения различных видов частотно-временны́х преобразований с «идеальным ЧВР», где КПФ – кратковременное (оконное) преобразование Фурье; ПВ – псевдораспределение Вигнера; НВП – непрерывное вейвлет-преобразование; ПФС = A – модифицированная спектрограмма на основе показательного преобразования при A = 2, 10, 100 и 1000.

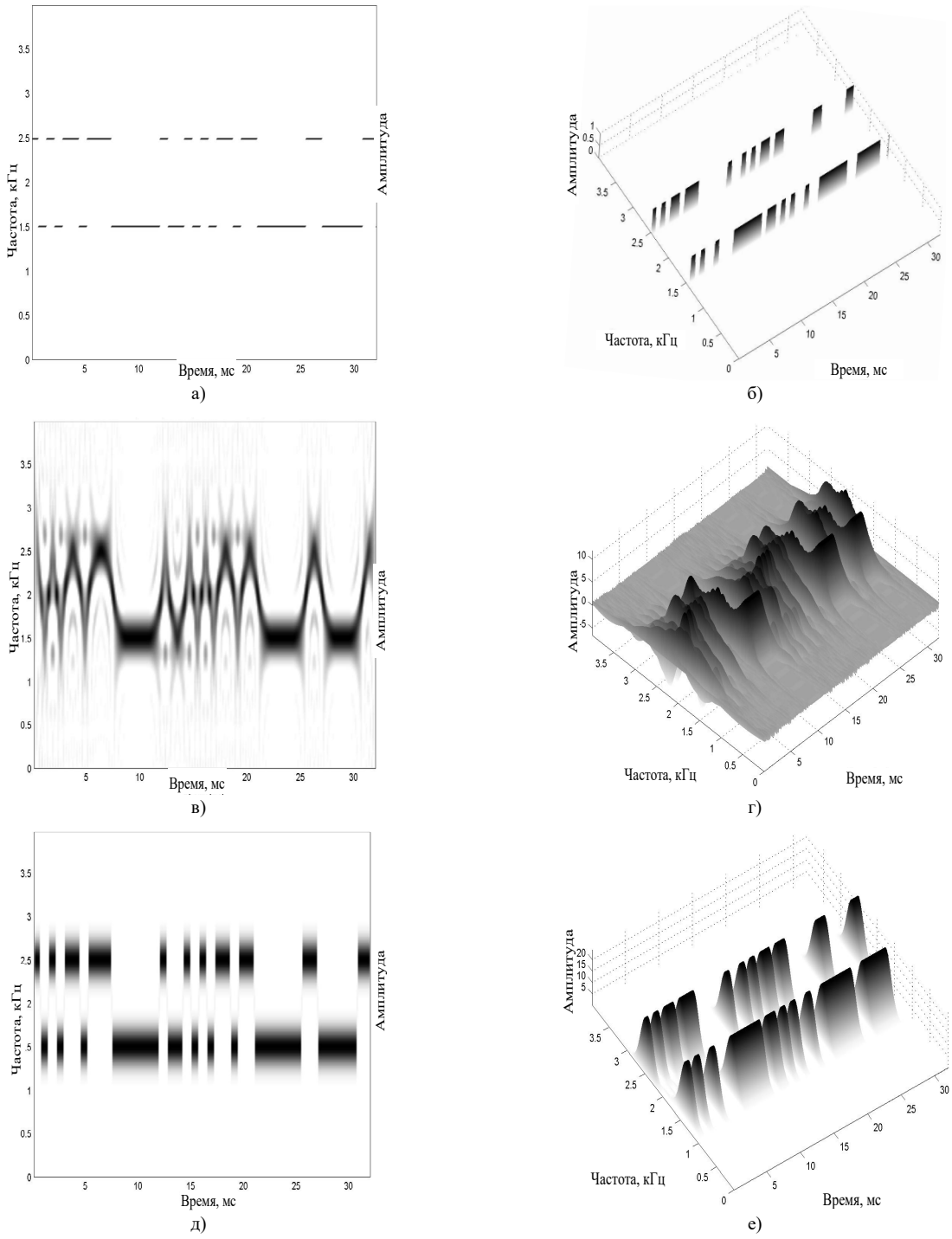


Рис. 6. Представление тестового сигнала ЧМн-2 на основе на основе «идеального ЧВР» (а, б), псевдо-ЧВР Вигнера (в, г) и модифицированной спектрограммы после временно́го нормирования (д, е)

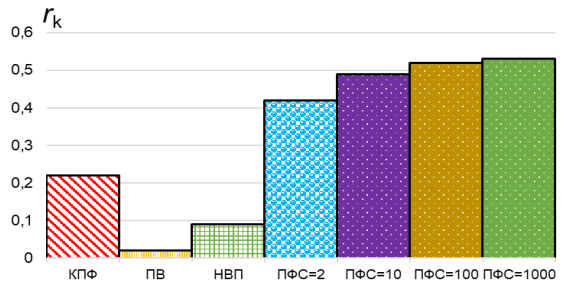


Рис. 7. Соответствие различных ЧВР «идеальному ЧВР» по метрике $r_к$

Визуальный анализ представленных результатов (см. рисунок 7) позволяет заключить, что наибольшая целесообразность применения процедур модификации обоснована к распределениям, имеющим низкий (подавленный) интерференционный фон, то есть к различным формам сглаженных и псевдо-ЧВР.

Среди прочих, авторами в [25] выделены спектрограммы, в общем случае представляющими собой простейшую форму ЧВР, недостатком которых является значительный дисперсионный разброс

энергии вдоль линии мгновенной частоты. Однако применение процедур модификаций на основе степенных и показательных преобразований позволило существенно уменьшить характер негативных проявлений. С учетом указанных обстоятельств спектрограммы можно рассматривать как наиболее эффективный инструмент анализа нестационарных процессов со сложной частотно-временной структурой.

Очевидно, что степенные и показательные преобразования достаточно трудоемки в вычислительном плане. Причем аналитическая сложность вычислений возрастает с повышением основания *A*. Вместе с тем анализ представленных результатов показывает, что для получения приемлемых значений по точности и качеству представления матриц распределения энергии достаточно использовать $A = 10$, что позволяет на практике ограничится данным основанием.

Дальнейшее усовершенствование матриц распределения энергии имеет смысл лишь при условии проведения дополнительных процедур временно́го нормирования.

Заключение

Формализация представления совместных ЧВР как инструмента анализа тонкой частотно-временно́й структуры параметров энергетических процессов с высокой нестационарностью их изменения на интервале обработки позволяет определить основные направления дальнейшего развития теории билинейных распределений.

В рамках настоящей статьи рассмотрены лишь некоторые аспекты, связанные с непосредственным применением процедур степенного и показательного преобразований. Вместе с тем поиск приемлемых форм, основанный на анализе существующих знаний, наверняка позволит определить перспективные направления дальнейших исследований в этом вопросе. Немаловажным аспектом является практическая составляющая приложения методов совместного анализа, в частности, в процедурах принятия решения [35–40].

Разработанные подходы к модификации матриц распределения энергии универсальны и дают возможность осуществлять быстрый синтез инструмента анализа с требуемыми характеристиками. Очевидно, что будущее за применением совместной обработки в задачах радиотехники определено метрологическими возможностям модифицированных матриц по измерению тонкой структуры энергетических процессов. Также можно предположить возможность их применения и в интересах повышения помехоустойчивости передачи информации [41–44], о чем уже указывалось ранее. Большое будущее видится и у метода временно́го нормирования. В настоящее время эти вопросы активно изучаются.

Список используемых источников

1. Cohen L. Time-Frequency Distribution – a Review // Proceedings of the IEEE. 1989. Vol. 77. Iss. 7. PP. 941–981. DOI:10.1109/5.30749

2. Boashash B. Time-Frequency Signal Analysis // In: Advances in Spectrum Estimation and Array Processing. N. J.: Prentice Hall, 1990. PP. 418–517.

3. Hlawatsch F., Krattenthaler W. Bilinear signal synthesis // IEEE Transactions on Signal Processing. 1992. Vol. 40. Iss. 2. PP. 352–363. DOI:10.1109/78.1249454

4. Cohen L. The scale representation // IEEE Transactions on Signal Processing. 1993. Vol. 41. Iss. 12. PP. 3275–3292. DOI:10.1109/78.258073

5. Cohen L. Time-Frequency Analysis. Englewood Cliffs, NJ: Prentice-Hall, 1995. 299 p.

6. Дворников С.В. Теоретические основы синтеза билинейных распределений. СПб.: Издательство Политехнического университета, 2007. 268 с.

7. Flandrin P. Time-Frequency / Time-Scale Analysis. San Diego: Academic Press, 1999 (translated by Stöckler from the French editions, Temps-frequency. Paris: Hermes, 1993).

8. Дворников С.В. Теоретические основы синтеза билинейных распределений энергии нестационарных процессов в частотно-временном пространстве: обзор // Труды учебных заведений связи. 2018. Т. 4. № 1. С. 47–60. DOI:10.31854/1813-324X-2018-1-47-60

9. Дворников С.В. Билинейные распределения с пониженным уровнем интерференционного фона в частотно-временном пространстве: продолжение обзора // Труды учебных заведений связи. 2018. Т. 4. № 2. С. 69–81. DOI:10.31854/1813-324X-2018-2-69-81

10. Дворников С.В. Билинейные масштабно-временные распределения энергии аффинного класса в частотно-временно́м пространстве: продолжение обзора // Труды учебных заведений связи. 2018. Т. 4. № 3. С. 26–44. DOI:10.31854/1813-324X-2018-4-3-26-44

11. Дворников С.В. Обобщенные гибридные масштабно-частотно-временные распределения в частотно-временном пространстве: продолжение обзора // Труды учебных заведений связи. 2018. Т. 4. № 4. С. 20–35. DOI:10.31854/1813-324X-2018-4-4-20-35

12. Дворников С.В. Методология совершенствования форм представления совместных распределений в частотно-временном пространстве: продолжение обзора // Труды учебных заведений связи. 2019. Т. 5. № 1. С. 96–106. DOI:10.31854/1813-324X-2019-5-1-96-106

13. Дворников С.В. Совместные распределения с повышенной контрастностью сигнальных компонент в частотно-временном пространстве: продолжение обзора // Труды учебных заведений связи. 2019. Т. 5. № 2. С. 117–125. DOI:10.31854/1813-324X-2019-5-2-117-125

14. Дворников С.В. Теоретические основы синтеза частотно-временных представлений класса Коэна // Информация и космос. 2008. № 3. С. 16–24.
15. Дворников С.В., Кудрявцев А.М. Теоретические основы частотно-временного анализа кратковременных сигналов: монография. СПб.: ВАС, 2010. 240 с.
16. Дворников С.В., Алексеева Т.Е. Распределение Алексеева и его применение в задачах частотно-временной обработки сигналов // Информация и космос. 2006. № 3. С. 9–20.
17. Алексеев А.А., Кириллов А.Б. Технический анализ сигналов и распознавание радиоизлучений. СПб.: ВАС, 1998. 368 с.
18. Дворников С.В. Проблема поиска сигналов источников информации при радиомониторинге // Мобильные системы. 2007. № 4. С. 33–35.
19. Дворников С.В., Бородин Е.Ю., Маджар Х., Махлуф Ю.Х. Частотно-временное оценивание параметров сигналов на основе функций огибающих плотности распределения их энергии // Информация и космос. 2007. № 4. С. 41–45.
20. Дворников С.В., Яхеев А.Ф. Метод измерения параметров кратковременных сигналов на основе распределения Алексеева // Информация и космос. 2011. № 1. С. 66–74.
21. Дворников С.В., Железняк В.К., Храмов Р.Н., Желнин С.Р., Медведев М.В., Симонов А.Н., Сауков А.М. Метод обнаружения радиоизлучений на основе частотно-временного распределения Алексеева // Научное приборостроение. 2006. Т. 16. № 1. С. 107–115.
22. Дворников С.В., Осадчий А.И., Дворников С.С., Родин Д.В. Демодуляция сигналов на основе обработки их модифицированных распределений // Контроль. Диагностика. 2010. № 10. С. 46–54.
23. Яхеев А.Ф., Дворников С.В. Измерение параметров сигналов на основе оптимизации формы распределения Алексеева // Наукоемкие технологии. 2009. Т. 10. № 1. С. 25–28.
24. Дворников С.В. Демодуляция сигналов на основе обработки их модифицированных частотно-временных распределений // Цифровая обработка сигналов. 2009. № 2. С. 7–11.
25. Дворников С.В., Сауков А.М. Модификация частотно-временных описаний нестационарных процессов на основе показательных и степенных функций // Научное приборостроение. 2004. Т. 14. № 3. С. 76–85.
26. Дворников С.В., Дворников С.С., Спирин А.М. Синтез манипулированных сигналов на основе вейвлет-функций // Информационные технологии. 2013. № 12. С. 52–55.
27. Дворников С.В. Теоретические основы представления сигнала в аналитическом виде функциями его огибающей и полной фазы // Научное приборостроение. 2006. Т. 16. № 4. С. 106–111.
28. Дворников С.В., Желнин С.Р., Медведев М.В. Метод формирования признаков распознавания сигналов диапазона декаметровых волн по их вейвлет-коэффициентам, рассчитанным на основе лифтинговой схемы // Информация и космос. 2006. № 2. С. 68–73.
29. Auger F., Flandrin P. Improving the readability of time-frequency and time-scale representation by the reassignment method // IEEE Transactions on Signal Processing. 1995. Vol. 43. Iss. 5. PP. 1068–1089. DOI:10.1109/78.382394
30. Claasen T.A.C.M., Meclenbrauker W.F.G. The Wigner Distribution – a Tool for Time-Frequency Signal Analysis. Part 1, 2, 3 // Philips Journal of Research. 1980. Vol. 35. PP. 217–250, 276–300, 372–389.
31. Hou T.Y., Shi Z. Data-driven time-frequency analysis // Applied and Computational Harmonic Analysis. 2013. Vol. 35. Iss. 2. PP. 284–308. DOI:10.1016/j.acha.2012.10.001
32. Renyi A. On Measures of Entropy and Information // Proceedings of the 4th Berkeley Symposium on Mathematical Statistics and Probability (20 June – 30 July 1960). Berkeley: University of California Press, 1961. Vol. 1. PP. 547–561.
33. Baraniuk R.G., Flandrin P., Janssen A.J.E.M., Michel O.J.J. Measuring time-frequency information content using the Renyi entropies // IEEE Transactions on Information Theory. 2001. Vol. 47. Iss. 4. PP. 1391–1409. DOI:10.1109/18.923723
34. Чуи Ч. Введение в вейвлеты. М.: Мир, 2001. 412 с.
35. Дворников С.В. Метод обнаружения сигналов диапазона ВЧ на основе двухэтапного алгоритма принятия решения // Научное приборостроение. 2005. Т. 15. № 3. С. 114–119.
36. Дворников С.В. Методика оценки имитоустойчивости каналов управления роботизированных устройств // Радиопромышленность. 2016. № 2. С. 64–69.
37. Дворников С.В., Дворников А.С., Желнин С.Р., Оков И.Н., Сауков А.М., Симонов А.Н., Яхеев А.Ф. Способ распознавания радиосигналов. Патент на изобретение RUS 2356064 от 24.04.2007. Опубл. 20.05.2009. Бюл. 14. 16 с.
38. Вознюк М.А., Дворников С.В., Винокуров М.Е., Петросян А.П., Романенко П.Г. Работа линий радиосвязи с ППРЧ в условиях преднамеренных помех // Информационные технологии. 2012. № 10. С. 64–67.
39. Дворников С.В., Устинов А.А., Пшеничников А.В., Борисов В.В., Москалец А.Г., Бурыкин Д.А. Демодуляция сигналов ОФТ на основе адаптивного порога // Вопросы радиоэлектроники. Серия: Техника телевидения. 2013. № 2. С. 90–97.
40. Дворников С.В. Цифровой синтез спектрально-эффективных сигналов телевидения // Вопросы радиоэлектроники. Серия: Техника телевидения. 2015. № 6. С. 168–173.
41. Дворников С.В., Пшеничников А.В., Манаенко С.С., Бурыкин Д.А., Кузнецов Д.А. Теоретические положения повышения помехоустойчивости сигнально-кодовых конструкций квадратурных сигналов // Информация и космос. 2015. № 3. С. 13–16.
42. Дворников С.В., Дворников С.С., Спирин А.М. Синтез манипулированных сигналов на основе вейвлет-функций // Информационные технологии. 2013. № 12. С. 52–55.
43. Дворников С.В., Пшеничников А.В., Манаенко С.С. Помехоустойчивая модель сигнала КАМ-16 с трансформированным созвездием // Информационные технологии. 2015. Т. 21. № 9. С. 685–689.
44. Дворников С.В., Манаенко С.С., Дворников С.С., Погорелов А.А. Синтез фазоманипулированных вейвлет-сигналов // Информационные технологии. 2015. Т. 21. № 2. С. 140–143.

* * *

PRESENTATION OF JOINT TIME-FREQUENCY DISTRIBUTIONS ON THE BASIS OF INDICATIVE AND POWER-TRANSFORMATION OF THEIR DENSITY OF THEM IN TIME-FREQUENCY SPACE (completion of review)

S. Dvornikov[1]

[1]Telecommunications Military Academy,
St. Petersburg, 194064, Russian Federation

Article info
The article was received 09 June 2019

For citation: Dvornikov S. Presentation of Joint Time-Frequency Distributions on the Basis of Indicative and Power-Transformation of their Density of them in Time-Frequency Space: Completion of Review. *Proceedings of Telecommunication Universities*. 2019;5(3):66–74. (in Russ.) Available from: https://doi.org/10.31854/1813-324X-2019-5-3-66-74

Abstract: *In this article it is presented an analytical overview of original methods for increasing the contrast of joint distribution matrices using the demonstrative and exponential transformations of their energy density in a frequency-time space. We see the examples of modelling, which define the focus of developed approaches. We are given the practical recommendations how to use them.*

Keywords: *time-frequency distributions, power and exponential transformations, methods of secondary processing of joint distributions.*

References

1. Cohen L. Time-Frequency Distribution – a Review. *Proceedings of the IEEE*. 1989;77(7):941–981. Available from: https://doi.org/10.1109/5.30749
2. Boashash B. Time-Frequency Signal Analysis. In: Haykin S. (eds.) *Advances is Spectrum Estimation and Array Processing*. N. J., USA: Prentice Hall; 1990. p.418–517.
3. Hlawatsch F., Krattenthaler W. Bilinear signal synthesis. *IEEE Transactions on Signal Processing*. 1992;40(2):352–363. Available from: https://doi.org/10.1109/78.124945
4. Cohen L. The scale representation. *IEEE Transactions on Signal Processing*. 1993;41(12):3275–3292. Available from: https://doi.org/10.1109/78.258073
5. Cohen L. *Time-Frequency Analysis.* Englewood Cliffs, NJ: Prentice-Hall; 1995. 299 p.
6. Dvornikov S.V. *Teoreticheskie osnovy sinteza bilineinykh raspredelenii* [Theoretical Basis for the Synthesis of Bilinear Distributions]. St. Petersburg: Izdatelstvo Politekhnicheskogo universiteta Publ.; 2007. 268 p. (in Russ.)
7. Flandrin P. *Time-Frequency / Time-Scale Analysis*. San Diego: Academic Press; 1999. 386 p. (Translated by Stöckler from the French ed.: *Temps-frequency*. Paris: Hermes; 1993)
8. Dvornikov S. Theoretical Foundations of the Synthesis of Bilinear Energy Distributions of Non-Stationary Processes in the Frequency-Temporary Space: Review. *Proceedings of Telecommunication Universities*. 2018;4(1):47–60. (in Russ.) Available from: https://doi.org/10.31854/1813-324X-2018-1-47-60
9. Dvornikov S. Bilinear Time-Frequency Distributions with a Lowered Level of the Interference Background in the Frequency-Temporary Space: Continued Review. *Proceedings of Telecommunication Universities*. 2018;4(2):69–81. (in Russ.) Available from: https://doi.org/10.31854/1813-324X-2018-2-69-81
10. Dvornikov S. Bilinear Scale-Temporary Distributions of Energy of the Affine Class in the Frequency-Temporary Space: Continued Review. *Proceedings of Telecommunication Universities*. 2018;4(3):26–44. (in Russ.) Available from: https://doi.org/10.31854/1813-324X-2018-4-3-26-44
11. Dvornikov S. Generalized Hybrid Scale-Frequency-Time Distributions in Time-Frequency Space: Continued Review. *Proceedings of Telecommunication Universities*. 2018;4(4):20–35. (in Russ.) Available from: https://doi.org/10.31854/1813-324X-2018-4-4-20-35
12. Dvornikov S. Methodology of Improving Forms of Representation of Joint Distributions in the Time-Frequency Space: Continued Review. *Proceedings of Telecommunication Universities*. 2019;5(1):96–106. (in Russ.) Available from: https://doi.org/10.31854/1813-324X-2019-5-1-96-106
13. Dvornikov S. Joint Distributions with Improved Contrast of Signal Components in Time-Frequency Space: Continued Review. *Proceedings of Telecommunication Universities*. 2019;5(2):117–125. (in Russ.) Available from: https://doi.org/10.31854/1813-324X-2019-5-2-117-125
14. Dvornikov S.V. *Teoreticheskie osnovy sinteza chastotno-vremennykh predstavlenii klassa Koena* [Theoretical Foundations of the Synthesis of Time-Frequency Representations of the Cohen Class]. *Informatsiia i kosmos*. 2008;3:16–24. (in Russ.)

15. Dvornikov S.V., Kudryavtsev A.M. *Teoreticheskie osnovy chastotno-vremennogo analiza kratkovremennykh signalov: monografiia* [Theoretical Foundations of Time-Frequency Analysis of Short-Term Signals. Monograph]. St. Petersburg: Telecommunications Military Academy Publ.; 2010. 240 p. (in Russ.)

16. Dvornikov S.V., Alekseeva T.E. Raspredelenie Alekseeva i ego primenenie v zadachakh chastotno-vremennoi obrabotki signalov [Alekseev Distribution and Its Application in Frequency-Time Signal Processing Tasks]. *Informatsiia i kosmos.* 2006;3:9–20. (in Russ.)

17. Alekseev A.A., Kirillov A.B. *Tekhnicheskii analiz signalov i raspoznavanie radioizluchenii* [Technical Analysis of Signals and Recognition of Radio Emission]. St. Petersburg: Telecommunications Military Academy Publ.; 1998. 368 p. (in Russ.)

18. Dvornikov S.V. Searching of information sources in radio-monitoring. *Mobilnye sistemy*. 2007;4:33–35. (in Russ.)

19. Dvornikov S.V., Borodin E.I., Madzhar K., Makhluf I.K. Chastotno-vremennoe otsenivanie parametrov signalov na osnove funktsii ogibaiushchikh plotnosti raspredeleniia ikh energii [Frequency-Time Estimation of Signal Parameters Based on Envelope Functions of Their Energy Distribution Density]. *Informatsiia i kosmos*. 2007;4:41–45. (in Russ.)

20. Dvornikov S.V., Jakheev A.F. Metod izmereniia parametrov kratkovremennykh signalov na osnove raspredeleniia Alekseeva [Method for Measuring Short-Term Signal Parameters Based on Alekseev Distribution]. *Informatsiia i kosmos*. 2011;1:66–74. (in Russ.)

21. Dvornikov S.V., Zheleznyak V.K., Khramov R.N., Zhelnin S.R., Medvedev M.V., Simonov A.N., et al. Method of radio signal detection based on alexeev's time-frequency distribution [Method of Detection of Radio Emissions Based on the Time-Frequency Distribution of Alekseev]. *Nauchnoe Priborostroenie (Scientific Instrumentation)*. 2006;16(1):107–115. (in Russ.)

22. Dvornikov S.V., Osadchy A.I., Dvornikov S.S., Rodin D.V. Demodulation Based on Processing the Modified Distributions. *Testing. Diagnostics*. 2010;10:46–54. (in Russ.)

23. Jakheev A.F., Dvornikov S.V. Measurement of Signals' Parameters on the Basis of Advanced Alekseev's Distribution Form. *Science Intensive Technologies*. 2009;10(1):25–28. (in Russ.)

24. Dvornikov S.V. Demoduliatsiia signalov na osnove obrabotki ikh modifitsirovannykh chastotno-vremennykh raspredelenii [Demodulation of Signals Based on the Processing of Their Modified Time-Frequency Distributions]. *Digital Signal Processing*. 2009;2:7–11. (in Russ.)

25. Dvornikov S.V., Saukov A.M. Modification of time-frequency descriptions of non-stationary processes Based on Exponential and Power functions. *Nauchnoe Priborostroenie (Scientific Instrumentation)*. 2004;14(3):76–85. (in Russ.)

26. Dvornikov S.V., Dvornikov S.S., Spirin A.M. Syntheses of Manipulated Signals on the Base of Wavelet-Functions. *Information Technology*. 2013;12:52–55. (in Russ.)

27. Dvornikov S.V. Theory of analytic signal presentation by functions of signal envelope and total phase. *Nauchnoe Priborostroenie (Scientific Instrumentation)*. 2006;16(4):106–111. (in Russ.)

28. Dvornikov S.V., Zhelnin S.R., Medvedev M.V. Metod formirovaniia priznakov raspoznavaniia signalov diapazona dekametrovykh voln po ikh veivlet-koeffitsientam rasschitannym na osnove liftingovoi skhemy [The method of Forming Signs of Recognition of Signals in the Range of Decameter Waves by Their Wavelet Coefficients, Calculated on the Basis of a Lifting Scheme]. *Informatsiia i kosmos*. 2006;2:68–73. (in Russ.)

29. Auger F., Flandrin P. Improving the readability of time-frequency and time-scale representation by the reassignment method. *IEEE Transactions on Signal Processing*. 1995;43(5):1068–1089. Available from: https://doi.org/10.1109/78.382394

30. Claasen T.A.C.M., Meclenbrauker W.F.G. The Wigner Distribution – a Tool for Time-Frequency Signal Analysis. Part 1, 2, 3. *Philips Journal of Research*. 1980;35:217–250,276–300,372–389.

31. Hou T.Y., Shi Z. Data-driven time-frequency analysis. *Applied and Computational Harmonic Analysis*. 2013;35(2):284–308. Available from: https://doi.org/10.1016/j.acha.2012.10.001

32. Renyi A. On Measures of Entropy and Information. *Proceedings of the 4th Berkeley Symposium on Mathematical, Statistics and Probability, 20 June – 30 July 1960*. Berkeley: University of California Press; 1961. vol.1. p.547–561.

33. Baraniuk R.G., Flandrin P., Janssen A.J.E.M., Michel O.J.J. Measuring time-frequency information content using the Renyi entropies. *IEEE Transactions on Information Theory*. 2001;47(4):1391–1409. Available from: https://doi.org/10.1109/18.923723

34. Chui Ch. *Vvedenie v veivlety* [Introduction to Wavelets]. Moscow: Mir Publ.; 2001. 412 p. (in Russ.)

35. Dvornikov S.V. HF Signal Detection Method Based on the Two-Phase Decision Making Algorithm. *Nauchnoe Priborostroenie (Scientific Instrumentation)*. 2005;15(3):114–119. (in Russ.)

36. Dvornikov S.V. Procedure of Evaluation of Imitation Stability of Robotic Devices Control Channels. *Radio industry*. 2016;2:64–69. (in Russ.)

37. Dvornikov S.V., Dvornikov A.S., Zhelnin S.R., Okov I.N., Saukov A.M., Simonov A.N., et al. *Sposob raspoznavaniia radiosignalov*. [Method of Recognition of Radio Signals]. Patent RF, no. 2356064, 24.04.2007. (in Russ.)

38. Voznjuk M.A., Dvornikov S.V., Vinokurov M.E., Petrosyan A.P., Romanenko P.G. Operation of Lines of a Radio Communication with PROF in the Conditions of Deliberate Noises. *Information Technology*. 2012;10:64–67. (in Russ.)

39. Dvornikov S.V., Ustinov A.A., Pshenichnikov A.V., Borisov V.V., Moskalets A.G., Burykin D.A. Demodulation of PSK signals based on adaptive threshold. *Voprosy radioelektroniki. Seriia: Tekhnika televideniia.* 2013;2:90–97. (in Russ.)

40. Dvornikov S.V. Digital synthesis of spectral-effective television signals. *Voprosy radioelektroniki. Seriia: Tekhnika televideniia*. 2015;6:168–173. (in Russ.)

41. Dvornikov S.V., Pshenichnicov A.V., Manaenko S.S., Burikin D.A., Kuznetsov D.A. Teoreticheskie polozheniia povysheniia pomekhoustoichivosti signalno-kodovykh konstruktsii kvadraturnykh signalov [Theoretical Provisions for Improving the Noise Immunity of Signal-Code Designs of Quadrature Signals]. *Information and Space*. 2015;3:13–16. (in Russ.)

42. Dvornikov S.V., Dvornikov S.S., Spirin A.M. Syntheses of Manipulated Signals on the Base of Wavelet-Functions. *Information Technology*. 2013;12:52–55. (in Russ.)

43. Dvornikov S.V., Pshenichnicov A.V., Manaenko S.S. Increased Noise Immunity Signal 16-QAM Constellation with Transformed. *Information Technology*. 2015;21(9):685–689. (in Russ.)

44. Dvornikov S.V., Manaenko S.S., Dvornikov S.S., Pogorelov A.A. Synthesis PSK Wavelet-Signal. *Information Technology*. 2015;21(2):140–143. (in Russ.)

СИСТЕМА ЦИФРОВЫХ ВОДЯНЫХ ЗНАКОВ С ВОЗМОЖНОСТЬЮ ИХ ИЗВЛЕЧЕНИЯ ИЗ БУМАЖНЫХ КОПИЙ ЦИФРОВЫХ ДОКУМЕНТОВ

В.И. Коржик[1*], **Д.А. Флаксман**[1]

[1]Санкт-Петербургский государственный университет телекоммуникаций им. проф. М.А. Бонч-Бруевича, Санкт-Петербург, 193232, Российская Федерация
*Адрес для переписки: val-korzhik@yandex.ru

Информация о статье
УДК 004.056.5
Статья поступила в редакцию 12.04.2019

Ссылка для цитирования: Коржик В.И., Флаксман Д.А. Система цифровых водяных знаков с возможностью их извлечения из бумажных копий цифровых документов // Труды учебных заведений связи. 2019. Т. 5. № 3. С. 75–85. DOI:10.31854/1813-324X-2019-5-3-75-85

Аннотация: *В работе предлагается система ЦВЗ для цветных изображений, главной особенностью которой является возможность их извлечения даже после печати и последующего сканирования изображения со скрытым вложением. Дается описание алгоритмов вложения и извлечения дополнительной информации, основанных на использовании широкополосных сигналов в частотной области. Описаны алгоритмы коррекции искажений, возникающих при печати и последующем сканировании бумажных копий цифровых документов. Приводятся результаты экспериментального исследования предложенной системы по объему вложения и достоверности извлечения вложенных данных.*

Ключевые слова: *цифровые водяные знаки, широкополосные сигналы, геометрические преобразования, коррекция перспективных искажений.*

ВВЕДЕНИЕ

Система цифровых водяных знаков (ЦВЗ) – это способ защиты интеллектуальной собственности и авторских прав владельцев цифровой информации. ЦВЗ являются одним из двух основных разделов стеганографии – науки о скрытой передаче информации. Стеганографию можно разделить на собственно стеганографию (СГ) (в узком смысле) и на ЦВЗ [1]. Отличием СГ от ЦВЗ является то, то в стеганографии основной целью является скрытность передачи сообщений, а в ЦВЗ – невозможность устранения вложенного сообщения.

ЦВЗ по количеству вкладываемой информации делятся на нульбитовые и многобитовые. Многобитовые системы позволяют при извлечении получить скрытое сообщение, в том время как нульбитовые позволяют осуществить только проверку наличия или отсутствия самого факта вложения. С.О. Анфиногенов в своей диссертационной работе предлагает нульбитовую систему ЦВЗ, устойчивую к случайным и преднамеренным преобразованиям [2].

ЦВЗ чаще всего применяются для защиты изображений, звука, видео и других цифровых документов, однако, в настоящее время значительный интерес стал появляться и к использованию таких «аналоговых» носителей, как бумага, пленки и другие физические объекты. Все эти объекты хотя и обладают определенной степенью защиты, (например, физические водяные знаки, контрольные суммы и использование специальных типов бумаги и пленки), нуждаются в дополнительной защите. Так, например, фотографии в бумажных документах, идентифицирующих личность (паспорта, водительские права, пропуска и т. п.), нуждаются в дополнительной защите от подмены (переделки). В некоторых случаях целесообразно использовать скрытую (т. е. невидимую для нелегитимных пользователей), идентификацию личности или товара. Это свойство может упростить нахождение нарушителей процедур идентификации при выполнении необходимого контроля.

В диссертации Ю. Ткаченко [3] предлагается система ЦВЗ для графических QR-кодов, основанная на искажении формы отдельных блоков, входящих в состав бар-кода, однако данный метод требует изменения структуры самого бар-кода.

При разработке систем ЦВЗ часто используются различные способы погружения скрытой информации: дискретное преобразование Фурье, дискретное косинусное преобразование, дискретное пре-

образование Уолша и др. Так, в работе [4] предложена система ЦВЗ для проверки подлинности пластиковых карт, в основе которой лежит преобразование Адамара.

Одним из направлений развития систем ЦВЗ является разработка систем целостности изображений. Например, на основе локальных особенностей может быть построена система хеширования изображений [5]. Однако создать систему ЦВЗ, устойчивую ко всем возможным «атакам» и преобразованиям покрывающих сообщений (ПС), достаточно сложно. Одним из решений данной проблемы является совместное использование нескольких систем ЦВЗ, устойчивых к различным наборам «атак». Такие системы называются «каскадными». В работе [6] предложена каскадная система ЦВЗ, совмещающая преимущества «нормализационного» метода [7], устойчивого к различным аффинным геометрическим атакам, и «голографического» [8], устойчивого к вырезанию фрагментов изображения.

В статье рассматривается система ЦВЗ, которая позволяет вкладывать информацию в цифровые изображения (в том числе бар-коды) и сохранять возможность достоверного извлечения вложенной информации даже после печати и последующего сканирования изображения с вложением.

В первом разделе подробно рассматривается алгоритм вложения и извлечения цифровой информации в изображение. Отдельное внимание уделяется способам устранения искажений, возникающих по время печати и последующего сканирования изображения с ЦВЗ. Во втором разделе представлены экспериментальные результаты работы предложенной системы ЦВЗ для цветных изображений. Третий раздел посвящен тем же вопросам, но применительно к изображениям в виде DataMatrix-кодов. Заключение суммирует результаты работы и формирует некоторые открытые проблемы.

1. ОПИСАНИЕ АЛГОРИТМА ВЛОЖЕНИЯ ЦИФРОВОЙ ИНФОРМАЦИИ В ПОКРЫВАЮЩЕЕ ИЗОБРАЖЕНИЕ И ЕЕ ИЗВЛЕЧЕНИЯ

Алгоритм вложения

Рассмотрим подробно алгоритм вложения скрытого сообщения в покрывающее изображение. Отметим, что сообщением может быть любая цифровая информация. Блок-схема работы алгоритма представлена на рисунке 1.

Для работы алгоритма вложения требуется одноканальное изображение, при этом оригинальное изображение может быть как в градациях серого, так и цветным (в формате RGB). В случае цветного изображения для вложения будет использоваться только синий канал изображения, так как человеческий глаз менее восприимчив к искажениям в нем.

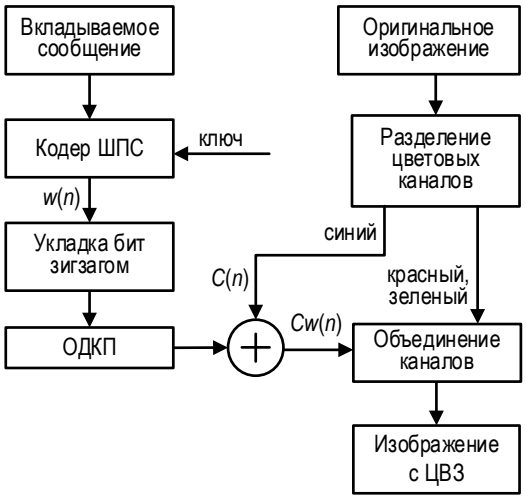


Рис.1. Блок-схема алгоритма вложения

Для вложения была выбрана область средних частот дискретно-косинусного преобразования (ДКП), что позволяет сделать вложение устойчивым не только к сжатию, но и к потере части покрывающего изображения. А для кодирования вкладываемого сообщения был выбран метод, основанный на использовании широкополосных сигналов (ШПС) [1], так как данный метод позволяет извлекать вложенные данные даже при больших искажениях и высоком уровне шума.

Для получения ШПС сначала необходимо подготовить псевдослучайную последовательность (ПСП), получить которую можно с помощью линейного рекуррентного регистра (ЛРР) [9]. Для работы ЛРР необходимо выбрать два числа и длину регистра. Первое число – это ключ, второе – начальное заполнение. Надо понимать, что чем больше длина ЛРР, тем больше будет период ПСП. Для большей стойкости вместо ЛРР может быть использован потоковый шифр [9].

На основе полученной ПСП и вкладываемых бит создается новая последовательность (ШПС), полученная по следующему правилу:

$$W(n) = \alpha(-1)^b \pi(n), \qquad n = 1, 2, \dots, N, \qquad (1)$$

где α – глубина вложения; N – длина ПСП, на которой вкладывается один бит (b = 1 или 0) информации; $\pi(n)$ – отсчет ПСП (±1); $b \in (0,1)$ – бит вкладываемого сообщения.

От параметра N зависят два важнейших свойства вложения. С одной стороны, чем больше N, тем надежнее будет извлекаться информация. С другой стороны, чем больше N, тем меньше бит можно будет вложить в изображение.

Далее из полученной ШПС-последовательности необходимо получить матрицу, размеры которой должны совпадать с размером оригинального изображения. Однако при этом надо учитывать, что следующим шагом будет обратное дискретно-косинусное преобразование (ОДКП), то есть полученная матрица является частотной матрицей. При

этом верхний левый угол – это область наиболее низких частот, а нижний правый – наиболее высоких. Оптимальной областью для укладки ШПС-последовательности является область средних частот, так как изменение низких частот сильно повлияет на качество полученного изображения с вложением, а область высоких частот больше всего подвержена искажениям. Укладывать последовательность необходимо зигзагом, начиная с верхнего левого угла, пропустив при этом область низких частот. Пример укладки бит зигзагом в область средних частот показан на рисунке 2.

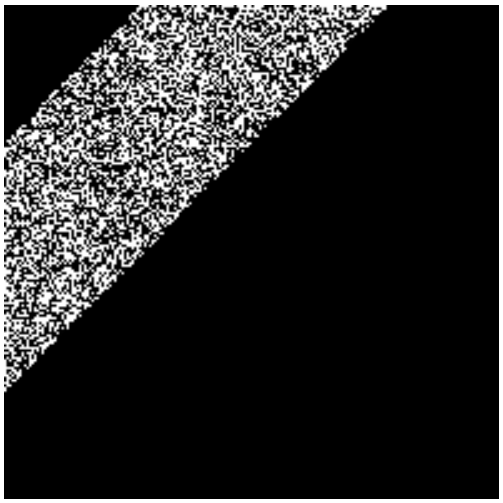


Рис. 2. Область средних частот при ДКП

Далее к полученной частотной матрице применяется ОДКП, которое описывается следующим уравнением:

$$p(x,y) = \sum_{u=0}^{W-1}\sum_{v=0}^{H-1} C(u)\cdot C(v)\cdot F(u,v)\times \\ \times \cos\left(\frac{\pi\cdot(2x+1)\cdot u}{2\cdot W}\right)\cdot\cos\left(\frac{\pi\cdot(2y+1)\cdot v}{2\cdot H}\right), \quad (2)$$

где

$$C(u) = \begin{cases} \frac{1}{\sqrt{W}}, & u = 0 \\ \sqrt{\frac{2}{W}}, & 1 \le u \le W-1 \end{cases};$$

$$C(v) = \begin{cases} \frac{1}{\sqrt{H}}, & v = 0 \\ \sqrt{\frac{2}{H}}, & 1 \le v \le H-1 \end{cases};$$

$F(u, v)$ – изображение; W – ширина изображения в точках; H – высота изображения в точках.

После ОДКП полученную матрицу необходимо сложить с выделенным ранее синим каналом оригинального изображения. Полученное в результате изображение готово к печати на физический носитель и последующему извлечению информации.

Алгоритм извлечения

Система ЦВЗ предполагает печать и последующее сканирование изображения, из-за чего возникают серьезные искажения. Для устойчивой работы алгоритма извлечения и устранения возникающих искажений необходимо добиться того, чтобы размер и геометрическое положение изображения, из которого будет осуществляться извлечение, и оригинала точно соответствовали друг другу. Блок-схема работы алгоритма извлечения представлена на рисунке 3. Стоит заметить, что процесс извлечения может быть осуществлен как при наличии оригинального изображения, так и при его отсутствии. В первом случае декодер называется информированным, во втором случае – слепым.

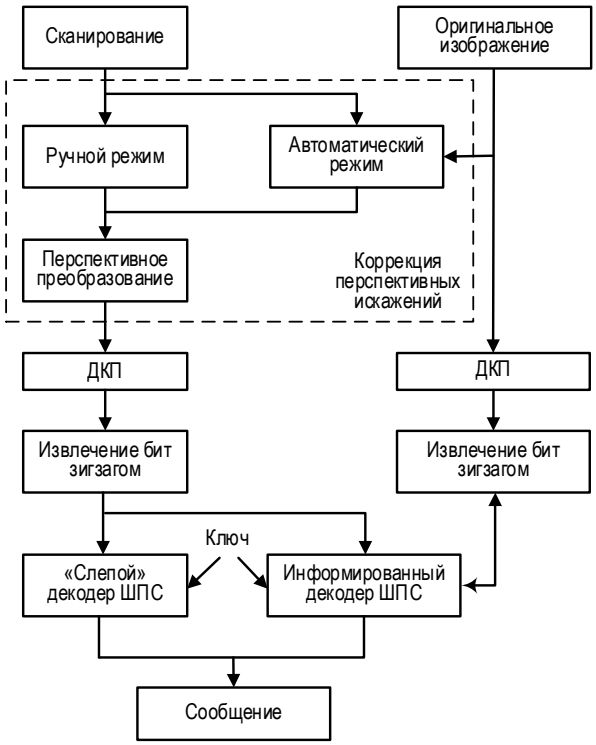


Рис. 3. Блок-схема алгоритма извлечения

Для извлечения вложения сначала нужно отсканировать распечатанное изображение с ЦВЗ, при этом следует выбирать такое разрешение сканирования, чтобы размер отсканированного изображения был больше, чем размер оригинального изображения. Иначе говоря, на одну точку оригинального изображения должно приходиться несколько точек на отсканированном изображении. Если не соблюдать данного правила, то произойдет ухудшение качества изображения и потеря части информации о нем, что негативно скажется на процессе извлечения вложенного сообщения.

После того как изображение было отсканировано, необходимо устранить возникшие геометрические искажения, основными из которых являются поворот, сдвиг и изменение масштаба. А если вместо сканера был применен фотоаппарат, то появятся «перспективные» искажения. Поэтому мы

будем рассматривать более общий случай – устранение «перспективных» искажений, используя перспективное преобразование.

Рассмотрим перспективное (проективное, гомографическое) преобразование подробнее. Важным аспектом перспективного преобразования является то, что при нем сохраняется коллинеарность точек, то есть три точки, лежащие на одной прямой (коллинеарные), останутся лежать на одной прямой и после преобразования, но при этом может не сохраниться параллельность линий, как это происходит при аффинном преобразовании (аффинное преобразование можно считать частным случаем перспективного преобразования). Перспективное преобразование описывается следующим матричным уравнением:

$$\begin{pmatrix} \bar{x}' \\ \bar{y}' \\ w \end{pmatrix} = \begin{pmatrix} t_{11} & t_{12} & t_{13} \\ t_{21} & t_{22} & t_{23} \\ t_{31} & t_{32} & t_{33} \end{pmatrix} \begin{pmatrix} \bar{x} \\ \bar{y} \\ 1 \end{pmatrix}, \quad (3)$$

где x', y' – новые координаты точки; x, y – старые координаты точки; $t_{i,j}$ – коэффициенты матрицы преобразования; w – глубина (масштаб).

Отсюда, после нормировки по масштабу получаем:

$$x'' = \frac{t_{11}x' + t_{12}y' + t_{13}}{t_{31}x' + t_{32}y' + t_{33}}, \qquad y'' = \frac{t_{21}x' + t_{22}y' + t_{23}}{t_{31}x' + t_{32}y' + t_{33}}. \quad (4)$$

Пример перспективного преобразования для тестового изображения представлен на рисунке 4.

а) б)

Рис. 4. Пример перспективного преобразования: а) тестовое изображение «Лена»; б) изображение после перспективного преобразования

При устранении перспективных искажений может возникнуть два варианта: первый – в наличии нет оригинального изображения (известен только размер изображения); второй – когда оно есть. В первом случае искажения устраняются с участием оператора (требуется визуальный поиск границ изображения), во втором – процесс может быть произведен в автоматическом режиме.

Наиболее простым является способ ручного устранения перспективных искажений, неизбежно возникающих при печати и сканировании изображения. При этом необходимо знать только размер оригинального изображения. Сначала необходимо визуально найти четыре угловые точки изображения на отсканированном образце. По положению найденных четырех точек можно рассчитать коэффициенты перспективного преобразования, описывающего преобразование между полученным четырехугольником и прямоугольником, характеризующим размеры оригинального изображения. Для этого необходимо подставить координаты найденных четырех точек в уравнение (4). В результате подстановки получится восемь уравнений: четыре уравнения для «x» и четыре – для «y», при этом коэффициент t_{33} следует принять равным 1. В результате решения получившейся системы из восьми уравнений получится матрица искомого перспективного преобразования.

Затем необходимо применить перспективное преобразование (3) с найденными коэффициентами к отсканированному изображению с ЦВЗ, одновременно обрезав полученное изображение по размерам оригинального. Весь процесс, за исключением визуального поиска, может быть легко автоматизирован. На рисунке 5а приведено отсканированное изображение, а на рисунке 5б – то же самое изображение, но после устранения перспективных искажений. Видно, что отсканированное изображение отличается масштабом и повернуто на небольшой угол.

Имея оригинальное изображение, можно использовать другой метод, и тогда все операции могут быть произведены полностью автоматически и при этом надежнее, чем при ручной коррекции.

а) б)

Рис. 5. Устранение перспективных искажений: а) отсканированное изображение; б) восстановленное изображение

Основным принципом является поиск оригинального изображения на отсканированном, для чего используются хорошо зарекомендовавшие себя методы, применяемые в «компьютером зрении». Алгоритм поиска оригинала на отсканированном изображении можно разбить на четыре этапа.

Этап 1. Поиск локальных особенностей (ЛО) и расчет их дескрипторов с использованием алгоритма обнаружения устойчивых признаков изображения SURF (*от англ.* Speeded Up Robust Features) [10].

ЛО – это хорошо различимая область изображения, соответствующая следующим требованиям: повторяемость (не изменяет своего положения при разном освещении и угле обзора); локальность (занимает малую часть изображения); значимость (каждую ЛО можно уникально описать); компактность и эффективность (количество ЛО невелико по сравнению с количеством точек изображения). Примером ЛО могут служить углы, а наиболее распространенный детектор углов – это детектор Харриса [11]. Дескриптор ЛО – это математическая характеристика, описывающая геометрию локальной окрестности вокруг точки. Поиск ЛО выполняется отдельно для оригинального изображения и изображения, полученного от сканера.

Этап 2. Сравнение ЛО оригинального изображения и изображения, полученного от сканера. Для этого используется алгоритм быстрого сравнения FLANN (*от англ.* Fast Approximate Nearest Neighbors Search) [12]. Результатом работы данного алгоритма являются пары соответствующих друг другу дескрипторов на оригинальном и отсканированном изображении.

Этап 3. Поиск коэффициентов наиболее вероятного перспективного преобразования, описывающего трансформацию первого изображения во второе, с использованием алгоритма оценки параметров на основе случайных выборок RANSAC (*от англ.* RANdom SAmple Consensus), предложенного в 1981 г. Фишлером и Боллесом [13].

Алгоритм RANSAC в данном случае работает следующим образом. По четырем случайно выбранным парам строится гипотеза – перспективное преобразование, описывающее трансформацию отсканированного изображения, к геометрическому положению оригинального изображения. Оставшиеся пары дескрипторов проверяются на соответствие гипотезы (сочетается ли данная пара дескрипторов с предложенным преобразованием). После многократного случайного построения различных гипотез выбирается та, которой удовлетворяет наибольшее число пар дескрипторов.

Этап 4. Применение найденного перспективного преобразования к отсканированному изображению.

Для проведения экспериментов была разработана программа на языке C++ с использованием библиотек компьютерного зрения «OpenCV», в которых уже реализованы вышеприведенные алгоритмы. Иллюстрация результата работы алгоритма представлена на рисунке 6. Слева находится оригинальное изображение, справа – отсканированное. На отсканированном изображении рамкой выделено найденное изображение. Линиями сопоставлены пары наиболее явно совпадающих ЛО, по которым найдено искомое перспективное преобразование. Можно заметить, что среди пар ЛО есть также и явные выбросы. Правда, на результате это никак не сказывается, так как выбросы отсеиваются алгоритмом RANSAC [13].

После того, как отсканированное изображение приведено к размерам оригинала, можно приступать к извлечению вложенных данных. Сначала, так же, как и при вложении, необходимо выделить рабочий канал. Если изображение было цветным, то рабочим является синий, если же изображение было в градациях серого, то дальнейшие шаги будут осуществляться непосредственно с самим изображением.

Рис. 6. Автоматическая коррекция перспективных искажений

Далее, так как вложение осуществлялось в частотную область, необходимо провести ДКП. ДКП – это ортогональное преобразование, в результате которого изображение представляется в виде суммы двумерных синусов различной амплитуды и частоты. ДКП описывается следующим уравнением:

$$F(u,v) = C(u)\cdot C(v)\cdot \sum_{x=0}^{W}\sum_{y=0}^{H} p(x,y)\times \\ \times \cos\left(\frac{\pi\cdot(2x+1)\cdot u}{2\cdot W}\right)\cdot\cos\left(\frac{\pi\cdot(2y+1)\cdot v}{2\cdot H}\right), \quad (5)$$

где

$$C(u) = \begin{cases} \frac{1}{\sqrt{W}}, & u = 0 \\ \sqrt{\frac{2}{W}}, & 1 \le u \le W-1 \end{cases};$$

$$C(v) = \begin{cases} \frac{1}{\sqrt{H}}, & v = 0 \\ \sqrt{\frac{2}{H}}, & 1 \le v \le H-1 \end{cases};$$

$p(x,y)$ – изображение; W – ширина изображения в точках; H – высота изображения в точках.

На рисунке 7 представлен синий канал (отображен в градациях серого) и соответствующая ему частотная матрица. Затем из полученной частотной матрицы необходимо получить последовательность бит. Для этого необходимо применить сканирование зигзагом. При этом следует выбирать именно ту область матрицы, в которую осуществлялось вложение.

Заключительным шагом является извлечение вложенных бит. Здесь может быть два варианта в зависимости от наличия или отсутствия ПС. Если его нет, то будет использоваться «слепой» декодер, а если ПС присутствует, то будет использоваться информированный декодер, при этом для оригинального изображения необходимо будет произвести ДКП и извлечение «зигзагом».

И наконец, необходимо сгенерировать ПСП бит (если использовался ЛРР, то необходимо знать ключ и начальное заполнение).

а) б)

Рис. 7. ДКП: а) тестовое изображение; б) частотная матрица (черный – наибольшая амплитуда, белый – наименьшая)

После этого нужно провести извлечение бит с помощью корреляционного приемника [1], который работает следующим образом: для каждых N бит последовательности, отвечающих за один вложенный бит, рассчитывается следующий коэффициент:

$$\Lambda = \sum_{n=1}^{N} (C'_w(n) - C(n)) \cdot \pi(n), \qquad n = 1,2, \dots, N, \quad (6)$$

где $C'_W(n)$ – отчет последовательности отсканированного изображения; $C(n)$ – отчет последовательности оригинального изображения; $\pi(n)$ – ПСП; N – длина ПСП, на которой вкладывается один бит.

В случае «слепого» декодера, $C(n)$ принимается всегда равным «0». Определение значения бита осуществляется следующим образом:

$$b = \begin{cases} 1, \Lambda < 0 \\ 0, \Lambda \geq 0 \end{cases}. \quad (7)$$

2. ЭКСПЕРИМЕНТАЛЬНЫЕ РЕЗУЛЬТАТЫ

Для проверки работы алгоритма была разработана программа на языке C++ с использованием библиотек компьютерного зрения «OpenCV» и проведена серия экспериментов. В ходе экспериментов, которые проводились как на изображениях в градациях серого, так и на цветных, были подобраны оптимальные параметры длины и глубины ШПС.

От длины ШПС зависит надежность и количество информации, вкладываемой в изображение. Если она окажется малой, то в процессе извлечения может оказаться слишком много ошибок, однако при ее увеличении будет уменьшаться количество вкладываемых в изображение бит. От глубины ШПС зависит визуальное качество изображения.

Сначала, для подбора длины ШПС, для изображений в градациях серого было выбрано тестовое изображение «Лена» в градациях серого» (см. рисунок 4а): размер изображения – 512×512 точек, физический размер напечатанного изображения – 9×9 см, глубина вложения ШПС – 4. Печать осуществлялась на лазерном принтере «Kyocera Ecosys P6021cdn». Сканирование осуществлялось «Canon LiDE 220» с разрешением 1200 dpi.

Результаты эксперимента представлены в таблице 1. По горизонтали изменяется длина ШПС используемая при вложении, а по вертикали откладывается количество бит, используемых для вложения. При этом приведены результаты как для «информированного» декодера, так и для «слепого». По результатам эксперимента можно сделать вывод, что для изображений оптимальной является длина ШПС в диапазоне от 300 до 700, при которой достигается оптимальное соотношение надежности и количества вложенной информации.

Для цветных изображений был проведен аналогичный эксперимент. Эксперимент проводился на цветном изображении «Лена». Размер изображения 512×512 точек. Физический размер напечатанного изображения: 9×9 см. Глубина вложения ШПС: 6. Печать осуществлялась на лазерном принтере «Kyocera Ecosys P6021cdn». Сканирование осуществлялось «Canon LiDE 220» с разрешением 1200 dpi.

Результаты эксперимента представлены в таблице 2. По представленным результатам можно сделать вывод, что для цветных изображений, так же, как и для изображений в градациях серого, оптимальной длинной ШПС является значение в диапазоне от 300 до 700.

Затем был проведен эксперимент по подбору оптимальной глубины вложения ШПС для цветных изображений. Длина ШПС была выбрана равной 500. Остальные параметры остались неизменными (таблица 3).

По результатам видно, что минимальной глубиной вложения является значение, равное 5. Стоит заметить, что увеличение глубины вложения влечет за собой чрезмерное ухудшение качества изображения, поэтому оптимальным диапазоном значений глубины ШПС можно считать значения в диапазоне от 6 до 7.

Далее была проведена серия экспериментов на трех других изображениях. Все эти изображения были напечатаны струйным принтером на бумаге размером 10×15 см. Результаты экспериментов приведены в таблице 4: «Изображение 1» – изображение в градациях серого, размером 1154×904 пикселя. «Изображение 2» – цветное изображение, размером 1154×904 пикселя. «Изображение 3» – цветное изображение, размером 412×530 пикселей.

По результатам экспериментов видно, что при печати изображения важную роль играет соотношение разрешения изображения и его физического размера (разрешение печати). Так, печать изображения с ЦВЗ большого размера на маленький лист может повлечь за собой уменьшение реальной скорости вложения и увеличение вероятности ошибки.

Можно заметить, что в сериях экспериментов присутствует заметный разброс вероятности ошибок, который обусловлен тем, что при проведении каждого эксперимента производилась печать и сканирование изображения, а также поиск и устранение перспективных искажений, из-за чего может возникнуть некоторая вариативность в точности устранения возникших искажений.

ТАБЛИЦА 1. Результаты эксперимента по подбору длины ШПС для изображений в градациях серого

Декодер	Вложение, бит	Длина ШПС				
		200	300	500	700	900
		Количество ошибочных бит (красным – в %)				
Информированный / Слепой	64	12 / 14	7 / 1	3 / 6	1 / 0	2 / 1
		18 / 21	10 / 1,5	4 / 9	1,5 / 0	3 / 1,5
	128	16 / 14	8 / 1	5 / 6	3 / 2	12 / 10
		12 / 10	6 / 1,7	4 / 5	2,3 / 1,5	9 / 8
	256	42 / 37	39 / 18	27 / 33	25 / 32	81 / 79
		16 / 14	15 / 7	10 / 12	10 / 12	31 / 30

ТАБЛИЦА 2. Результаты эксперимента по подбору длины ШПС для цветных изображений

Декодер	Вложение, бит	Длина ШПС						
		100	200	300	500	700	900	1100
		Количество ошибочных бит (красным – в %)						
Информированный / Слепой	64	6 / 20	4 /10	3 / 7	0 / 4	0 / 0	0 / 0	2 / 2
		9 / 31	6 / 15	5 / 11	0 / 6	0 / 0	0 / 0	3 / 3
	128	14 /32	4 / 16	3 / 7	0 / 4	2 / 1	14 / 12	33 / 29
		10 / 5	3 / 12	2 / 5	0 / 3	1,5 / 0,7	11 / 9	25 / 22
	256	31 / 45	4 / 17	13 / 8	12 / 9	47 / 45	86 / 81	90 / 93
		12 / 17	1,5 / 6	5 / 3	5 / 4	18 / 18	34 / 31	35 / 36

ТАБЛИЦА 3. Результаты эксперимента по подбору глубины ШПС для цветных изображений

Декодер	Вложение, бит	Глубина ШПС					
		4	5	6	7	8	9
		Количество ошибочных бит (красным – в %)					
Информированный / Слепой	64	3 / 9	1 / 4	0 / 1	0 / 0	1 / 0	0 / 0
		9 / 14	1,5 / 6	0 / 1,5	0 / 0	1,5 / 0	0 / 0
	128	4 / 11	2 / 4	3 / 2	2 / 0	1 / 0	0 / 0
		3 / 8,6	1,5 / 3	2,3 / 1,5	1,5 / 0	0,7 / 0	0 / 0
	256	43 / 40	21 / 19	34 / 38	1 / 15	2 / 0	2 / 2
		17 / 16	8 / 7	13 / 14	0,4 / 6	0,7 / 0	0,7 / 0,7

ТАБЛИЦА 4. Результаты экспериментов

Размер сообщения, бит	Информированный декодер / Слепой декодер		
	Номер изображения		
	1	2	32
	Количество ошибочных бит (красным – в %)		
64	0 / 7	0 / 1	0 / 0
	0 / 11	0 / 1,6	0 / 0
128	0 / 7	0 / 1	0 / 0
	0 / 5,5	0 / 0,8	0 / 0
256	0 / 7	0 / 1	1 / 0
	0 / 2,7	0 / 0,4	1,4 / 0
512	18 / 13	25 / 23	4 / 15
	3,5 / 2,5	4,9 / 4,5	2,7 / 2,9

Для каждого эксперимента представлены результаты извлечения как с использованием оригинального изображения (информированный декодер ШПС), так и без него (слепой декодер ШПС, известен только размер изображения). Вероятность ошибки при использовании «слепого» декодера выше, хотя встречаются и отдельные исключения из этого правила.

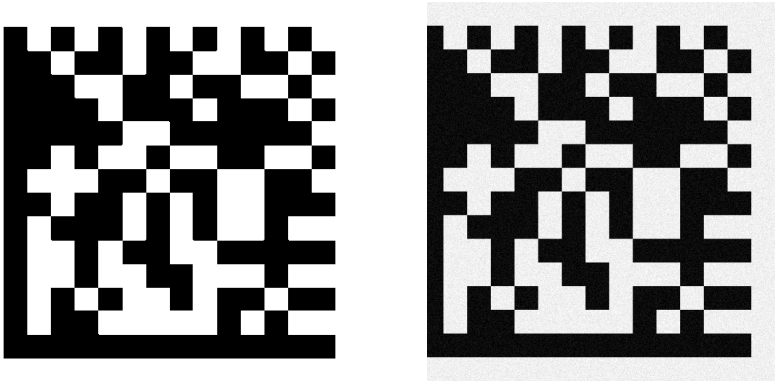
Стоит заметить, что в большинстве проведенных экспериментов видно, что количество ошибочных бит не равно 0, однако если их количество не превышает 2–3 %, то результат можно считать успешным, так как такие ошибки легко устраняются с помощью кодов с исправлением ошибок.

DOI:10.31854/1813-324X-2019-5-3-75-85

3. ИССЛЕДОВАНИЕ ВОЗМОЖНОСТИ ВЛОЖЕНИЯ ЦВЗ В DATAMATRIX-КОДЫ

Пример изображения с вложением ЦВЗ в DataMatrix-код при выбранных параметрах α = 15 и N = = 700 приведен на рисунке 8. Алгоритм вложения ЦВЗ остался таким же, каким он был для черно/белых с градациями серого и цветных фотографий. На первый взгляд, различие между рисунками 8а и 8б оказывается не заметно, однако при использовании увеличительного стекла можно заметить присутствие небольшой модуляции яркостью на черных и белых блоках DataMatrix-кода. Такое свойство может служить для скрытия дополнительно вложенной информации от технически невооруженного нарушителя.

Для данного случая так же возникает проблема устранения перспективных искажений, особенно при считывании вложения ЦВЗ при помощи мобильных средств (фотоаппаратов, смартфонов и планшетов). Решение этой проблемы упрощается для данного вида изображений ввиду того, что DataMatrix изначально разработан для подобных условий. В каждом DataMatrix-коде присутствует шаблон поиска (рисунок 9), необходимый для его обнаружения и успешного декодирования.



а) б)

Рис 8. Изображение DataMatrix-кода до (а) и после (б) вложения ЦВЗ

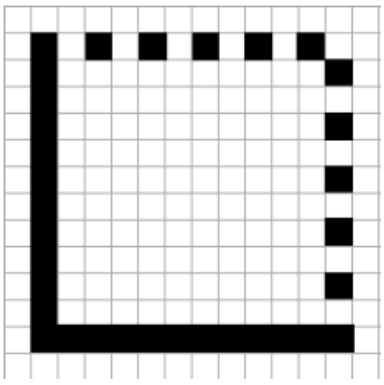


Рис 9. Шаблон поиска DataMatrix-кода

Однако широкодоступные алгоритмы позиционирования оказались недостаточно точны, так как для декодирования DataMatrix достаточно его позиционирования с точностью до модуля, поэтому пришлось дорабатывать существующие алгоритмы для получения приемлемой точности.

В таблице 5 представлены результаты эксперимента с расчетом вероятности ошибки при вложении в два DataMatrix-кода, взятых с бумажных копий размером 2×2, 3×3, 4×4, 5×5, 6×6 и 9×9 см при выборе параметров вложения α = 15, N = 700. Все изображения были напечатаны на лазерном принтере и отсканированы с разрешением 600 dpi. Результаты эксперимента показали, что, используя сканер, можно успешно извлекать до 128 бит данных из изображений размером 3×3 см. При увеличении физического размера изображения количество доступных для вложения бит увеличивается. Например, для изображения размером 4×4 см, это уже 256 бит, а для изображения 5×5 см – 320 бит.

В таблице 6 представлены результаты эксперимента для тех же изображений, однако вместо сканера была камера мобильного телефона.

ТАБЛИЦА 5. Результаты эксперимента при считывании сканером с разрешением 600 dpi

Размер сообщения, бит	Изображение 1 / Изображение 2					
	2×2	3×3	4×4	5×5	6×6	9×9
	Количество ошибочных бит (красным – в %)					
64	9 / 19	3 / 5	2 / 2	2 / 2	2 / 2	2 / 2
	14 / 29,6	4,7 / 7,8	3,13 / 3,13	3,13 / 3,13	3,13 / 3,13	3,13 / 3,13
128	40 / 52	6 / 22	3 / 2	2 / 2	2 / 2	2 / 2
	31,2 / 40,63	4,7 / 17,2	2,34 / 1,56	1,56 / 1,56	1,56 / 1,56	1,56 / 1,56
256	94 / 101	52 / 76	24 / 17	2 / 3	2 / 2	2 / 2
	36,7 / 39,5	20,3 / 29,7	9,38 / 6,64	0,78 / 1,17	0,78 / 0,78	0,78 / 0,78
320	114 / 130	75 / 95	43 / 34	5 / 9	2 / 2	2 / 2
	35,6 / 40,6	23,4 / 13,4	13,4 / 10,6	1,56 / 2,81	0,63 / 0,63	0,63 /0,63

ТАБЛИЦА 6. Результаты эксперимента при считывании телефоном (YotaPhone 2, камера 8 мегапикселей)

Размер сообщения, бит	Изображение 1 / Изображение 2			
	4×4	5×5	6×6	9×9
	Количество ошибочных бит (красным – в %)			
64	5 / 9	11 / 8	6 / 9	3 / 3
	23,4 / 10,1	17,2 / 12,5	9,38 / 14	4,69 / 4,69
128	34 / 35	30 / 35	9 / 24	3 / 4
	26,6 / 27,3	23,4 / 27,3	7,03 / 18,7	2,34 / 3,13
256	77 / 90	73 / 82	41 / 57	4 / 11
	30,1 / 35,1	28,5 / 32	16 / 22,3	1,56 / 4,3
320	98 / 108	92 / 103	69 / 79	6 / 15
	30,6 / 33,7	28,8 / 32,1	21,6 / 24,7	1,88 / 4,69

Результаты эксперимента показали, что, используя камеру телефона, успешно извлекать 128 бит данных можно только из изображений размером 6×6 см и больше, что в два раз больше, чем при использовании сканера.

ЗАКЛЮЧЕНИЕ

В работе для предложенного метода были экспериментально подобраны оптимальные параметры длины и глубины ШПС. Исходя из результатов экспериментов, можно сделать вывод о том, что наличие или отсутствие оригинального изображения при использовании данного метода в меньшей степени влияет на вероятность ошибочного извлечения сообщения, чем процесс печати и последующего сканирования изображения с ЦВЗ, приводящий к серьезным искажениям геометрии и цветового пространства изображения. Оригинальное изображение в основном нужно для его точного автоматического позиционирования. Однако если эту задачу решить альтернативным способом (например, в «ручном режиме» или методом обнаружения обводящей рамки), то можно обойтись и без оригинального изображения, а при извлечении необходимо будет знать только размер изображения, который может быть оговорен заранее.

Исследование возможности вложения ЦВЗ в баркоды, напечатанные на бумаге, показало, что успешное извлечение с использованием смартфона возможно только для их достаточно большого физического размера – не менее чем 6х6 см. В противном случае физический размер при том же объеме вложения может быть уменьшен до 3×3 см.

Следует добавить, что в настоящей статье не рассматривалась возможность использования данного метода для защиты от копирования печатных изображений. Эта проблема требует дальнейших исследований.

Список используемых источников

1. Коржик В.И., Небаева К.А., Герлинг Е.Ю., Догиль П.С., Федянин И.А. Цифровая стеганография и цифровые водяные знаки. Часть 1. Цифровая Стеганография. СПб.: СПбГУТ, 2016. 226.с.

2. Анфиногенов С.О. Разработка и исследование методов построения нульбитовой системы цифровых «водяных» знаков устойчивой к случайным и преднамеренным преобразованиям: дис. … канд. тех. наук. СПб.: СПбГУТ, 2014.

3. Tkachenko I. Generation and analysis of graphical codes using textured patterns for printed document authentication. D.Sc Thesis. Montpellier: Université de Montpellier, 2015.

4. Ho A.T.S., Shu F. A print-and-scan resilient digital watermark for card authentication // Proceedings of the 4th International Conference on Information, Communications and Signal. Formal Methods and Security (ICICS-PCM, Singapore, Singapore,15–18 December 2003). Piscataway, NJ: IEEE, 2003. DOI:10.1109/ICICS.2003.1292640

5. Monga V., Evans B.L. Perceptual Image Hashing Via Feature Points: Performance Evaluation and Tradeoffs // IEEE Transactions on Image Processing. 2006. Vol. 15. Iss. 11. PP. 3452–3465. DOI:10.1109/TIP.2006.881948

6. Кочкарев А.И. Решение проблемы извлечения информации для каскадной системы ЦВЗ при атаке вырезанием фрагментов изображения // Телекоммуникации. 2016. № 10. С. 27–38.

7. Dong P., Brankov J.G., Galatsanos N.P., Yang Y., Davoine F. Digital Watermarking Robust to Geometric Distortions // IEEE Transactions on Image Processing. 2006. Vol. 14. Iss. 12. PP. 2140–2150. DOI:10.1109/TIP.2005.857263

8. Bruckstein A.M., Richardson T.J. A Holographic Transform Domain Image Watermarking Method // Circuits, Systems, and Signal Processing. 1998. Vol. 17. Iss. 3. PP. 361–389. DOI:10.1007/BF01202298

9. Коржик В.И., Яковлев В.И. Основы криптографии: учебное пособие. СПб.: ИЦ «Интермедиа», 2016. 312 с.

10. Bay H., Tuytelaars T., Van Gool L. SURF: Speeded Up Robust Features // Proceedings of the 9th European Conference on Computer Vision (ECCV, Graz, Austria, 7–13 May 2006). Lecture Notes in Computer Science. Part 1. 2006. Vol. 3951. PP. 404–417. DOI:10.1007/11744023_32

11. Harris C., Stephens M. A Combined Corner and Edge Detector // Proceedings of the 4th Alvey Vision Conference (AVC, Manchester, UK, 31st Augusyt – 2nd September 1988). Manchester: University of Manchester Publ., 1988. PP. 23.1–23.6. DOI:10.5244/C.2.23

12. Muja M., Lowe D.G. Fast Approximate Nearest Neighbors with Automatic Algorithm Configuration // Proceedings of the International Conference on Computer Vision Theory and Applications (VISAPP, Lisboa, Portugal, 5–8 February 2009). Setubal: INSTICC Press, 2009. Vol. 1. PP. 331–340. DOI:10.5220/0001787803310340

13. Fischler M.A., Bolles R.C. Random sample consensus: a paradigm for model fitting with applications to image analysis and automated cartography // Communications of the ACM. 1981. Vol. 24. Iss. 6. PP. 381–395. DOI:10.1145/358669.358692

* * *

DIGITAL WATERMARK SYSTEM WITH AN ABILITY OF ITS EXTRACTION FROM HARD COPIES OF DATA

V. Korzhik[1], **D. Flaksman**[1]

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

Article info
The article was received 12 April 2019

For citation: Korzhik V., Flaksman D. Digital Watermark System with an Ability of its Extraction from Hard Copies of Data. *Proceedings of Telecommunication Universities*. 2019;5(3):75–85. (in Russ.) Available from: https://doi.org/10.31854/1813-324X-2019-5-3-75-85

Abstract: *In this paper it is presented Digital Watermark System for color images. The main feature of this system is an ability to extract digital watermarks even after printing and following scanning of watermarked images. There is a description of algorithms for embedding and extracting of additional information. These methods are based on the usage of spread-spectrum signals in the frequency domain. Furthermore, there is described algorithms of distortion correction after printing out and following scanning the paper copies of digital data. The results of the experimental research on evaluation of a possible embedding volume and the reliability after extraction of the embedded data are also presented.*

Keywords: *digital watermarking, spread spectrum signals, perspective distortion correction.*

References

1. Korzhik V.I., Nebaeva K.A., Gerling E.I., Dogil P.S., Fedianin I.A. *Tsifrovaia steganografiia i tsifrovye vodianye znaki. Chast 1. Tsifrovaia Steganografiia* [Digital Steganography and Digital Watermarks. Part 1. Digital Steganography.] St. Petersburg: The Bonch-Bruevich Saint-Petersburg State University of Telecommunications Publ.; 2016. 226 p. (in Russ.)
2. Anfinogenov S.O. *Razrabotka i issledovanie metodov postroeniia nulbitovoi sistemy tsifrovykh "vodianykh" znakov ustoichivoi k sluchainym i prednamerennym preobrazovaniiam* [Development and Research of Methods for Constructing a Nulbit Digital Watermark System Resistant to Random and Intentional Transformations]. PhD Thesis. St. Petersburg: The Bonch-Bruevich Saint-Petersburg State University of Telecommunications Publ.; 2014. (in Russ.)
3. Tkachenko I. *Generation and analysis of graphical codes using textured patterns for printed document authentication*. D.Sc Thesis. Montpellier: Université de Montpellier; 2015.
4. Ho A.T.S., Shu F. A print-and-scan resilient digital watermark for card authentication. *Proceedings of the 4th International Conference on Information, Communications and Signal. Formal Methods and Security, ICICS-PCM, 15–18 December 2003, Singapore, Singapore*. Piscataway, NJ: IEEE; 2003. Available from: https://doi.org/10.1109/ICICS.2003.1292640
5. Monga V., Evans B.L. Perceptual Image Hashing Via Feature Points: Performance Evaluation and Tradeoffs. *IEEE Transactions on Image Processing*. 2006;15(11):3452–3465. Available from: https://doi.org/10.1109/TIP.2006.881948
6. Kochkarev A.I. Solution of information extraction problem for concatenated digital watermarking system in case of attack by image patch cutting-out. *Telekommunikatsii*. 2016;10:27–38. (in Russ.)
7. Dong P., Brankov J.G., Galatsanos N.P., Yang Y., Davoine F. Digital Watermarking Robust to Geometric Distortions. *IEEE Transactions on Image Processing*. 2006;14(12):2140–2150. Available from: https://doi.org/10.1109/TIP.2005.857263
8. Bruckstein A.M., Richardson T.J. A Holographic Transform Domain Image Watermarking Method. *Circuits, Systems, and Signal Processing*. 1998;17(3):361–389. Available from: https://doi.org/10.1007/BF01202298
9. Korzhik V.I., Iakovlev V.I. Osnovy kriptografii: uchebnoe posobie [Cryptography Basics: Tutorial]. St. Petersburg: Intermedia Publ.; 2016. 312 p. (in Russ.)
10. Bay H., Tuytelaars T., Van Gool L. SURF: Speeded Up Robust Features. *Proceedings of the 9th European Conference on Computer Vision, ECCV, 7–13 May 2006, Graz, Austria. Lecture Notes in Computer Science. Part 1.* 2006. vol.3951. p.404–417. Available from: https://doi.org/10.1007/11744023_32
11. Harris C., Stephens M. A Combined Corner and Edge Detector. *Proceedings of the 4th Alvey Vision Conference, AVC, 31st Augusyt – 2nd September 1988, Manchester, UK*. Manchester: University of Manchester Publ.; 1988. p.23.1–23.6. Available from: https://doi.org/10.5244/C.2.23
12. Muja M., Lowe D.G. Fast Approximate Nearest Neighbors with Automatic Algorithm Configuration. *Proceedings of the International Conference on Computer Vision Theory and Applications, VISAPP, 5–8 February 2009, Lisboa, Portugal*. Setubal: INSTICC Press; 2009. vol.1. p.331–340. Available from: https://doi.org/10.5220/0001787803310340
13. Fischler M.A., Bolles R.C. Random sample consensus: a paradigm for model fitting with applications to image analysis and automated cartography. *Communications of the ACM*. 1981;24(6):381–395. Available from: https://doi.org/10.1145/358669.358692

МАСШТАБИРУЕМОЕ HONEYPOT-РЕШЕНИЕ ДЛЯ ОБЕСПЕЧЕНИЯ БЕЗОПАСНОСТИ В КОРПОРАТИВНЫХ СЕТЯХ

А.В. Красов[1], **Р.Б. Петрив**[1*], **Д.В. Сахаров**[1], **Н.Л. Сторожук**[1], **И.А. Ушаков**[1]

[1]Санкт-Петербургский государственный университет телекоммуникаций им. проф. М.А. Бонч-Бруевича, Санкт-Петербург, 193232, Российская Федерация
*Адрес для переписки: roman.petriv@mail.ru

Информация о статье
УДК 004.056
Статья поступила в редакцию 26.07.2019

Ссылка для цитирования: Красов А.В., Петрив Р.Б., Сахаров Д.В., Сторожук Н.Л., Ушаков И.А. Масштабируемое Honeypot-решение для обеспечения безопасности в корпоративных сетях // Труды учебных заведений связи. 2019. Т. 5. № 3. С. 86–97. DOI:10.31854/1813-324X-2019-5-3-86-97

Аннотация: *В статье анализируются тенденции в области применения технологий защиты сетей, использующих Honeypot-решения для выявления и исследования поведения нарушителей в целях выработки мер противодействия атакам. Предложено масштабируемое решение, протестированное на исследовательском стенде на основе технологий Microsoft Azure. Выполнен стресс-тест предложенного решения с использованием DDoS-атаки.*

Ключевые слова: *корпоративные сети, облачные вычисления, Deception Technologies (технологии «обманки»), Honeypot-решение, безопасность инфокоммуникационных сетей, киберугрозы, DDoS-атака.*

Введение

Несмотря на существенное развитие и накопленный опыт (так называемый Best Practice) применения технологий безопасности инфокоммуникационных сетей, наблюдается устойчивый рост количества, разнообразия и результативности кибератак. Многие крупные компании (Yahoo, Uber, Equifax) за последние три года столкнулись как с серьезными утечками данных, так и нарушениями в работе инфраструктуры вследствие злонамеренных действий. Согласно статистике [1], в первой половине 2019 г. только вредоносных приложений для мобильных устройств блокировалось ежедневно в среднем более 24 000, и их количество имеет тенденцию к росту. Также наблюдается устойчивый рост числа атак на IoT-инфраструктуру (более 600 % в 2017 г., 400–500 % по разным оценкам в 2018 г.), атак с помощью программ-вымогателей (в т. ч. шифровальщиков – WannaCry, Petya и др).

Масштабы кибератак продолжают расти, создавая угрозу конфиденциальности, целостности и доступности информационных активов, а также репутации организаций. «Ландшафт угроз» [2], вне всякого сомнения, станет более сложным, а атаки более целенаправленными, ориентированными на уязвимые места конкретной цели с реализацией обхода имеющихся средств защиты [3, 4].

Уже несколько лет преступные синдикаты работают подобно стартапам. Как другие успешные стартапы, они становятся более зрелыми и расширяют свои возможности. У киберпреступников уже давно есть заказчики, организована кооперация и специализация в различных областях: от написания вредоносного ПО до хостинга, тестирования, оказания курьерских услуг и т. д.

Вредоносные программы также совершенствуются их разработчиками и уже способны обходить элементы машинного обучения в развернутых системах киберзащиты [5]. Следующим шагом может стать использование передовых инструментов машинного обучения для автоматизации выбора хакерами своих целей, их наименее защищенных и оптимальных для реализации кибератак участков.

Растущее количество и разнообразие угроз требует постоянного совершенствования мер защиты, разработки и использования новых механизмов и методов противодействия кибератакам. Актуальной является задача разработки гибких унифицированных решений. Безусловно, выработка эффективных решений в значительной степени зависит от того, насколько исследованы и могут быть спрогнозированы действия нарушителей.

Анализ инцидентов безопасности является чрезвычайно важным источником информации для формирования мер противодействия, однако не может в достаточной мере обеспечивать своевременность, адекватность и эффективность (в том числе экономическую) мер противодействия, поскольку строится на изучении произошедших событий.

В случае успешной кибератаки нарушителя она может быть расследована с получением максимально полных данных о ее характере и способе проведения, но существенный ущерб уже может быть необратим. В случае своевременного реагирования и предотвращения атаки ущерба удается избежать, однако получить более подробную информацию о нарушителе и его потенциале крайне сложно. Решением данной задачи может быть использование приемов и методов отвлечения нарушителя на ложные цели, то есть использование так называемых *Deception Technologies* (технологий «обманки»), направленных на введение в заблуждение нарушителя.

Назначение и перспективность применения технологий «обманки» в корпоративных сетях

Большинство современных центров защиты информации оснащены технологиями, фиксирующими инциденты безопасности [6–9]. Но современная ситуация с защитой периметра сети все чаще рассматривается специалистами как вопрос времени. Отмечается тенденция, при которой злоумышленники обнаруживаются спустя все более существенное время нахождения внутри сети. Однако недостаточно найти и удалить злоумышленника из сети, и на основе анализа его поведения выработать решения. Следует более полно изучить противника, чтобы понять его, а для этого нужно предоставить ему больше времени для совершения злонамеренных действий.

Поскольку его действия несут все в себе угрозу, необходимо принять меры, позволяющие специалистам по безопасности изучать злоумышленника в воспринимаемой им как естественной среде (оставаясь при этом незамеченными для него), то есть в имитированной среде, где невозможно нанесение реального ущерба [10–11]. При этом следует как можно дольше удерживать злоумышленника в имитированной среде для изучения его действий, что может достигаться использованием множества технологий «обманки», которые выглядят весьма естественно, но являются приманками, содержат скрытые механизмы оповещения и др. [12].

Распределение ловушек и приманок целесообразно осуществлять по всей сети и на конечных точках, которые представляются информационными активами организации. Как только злоумышленник подключается к «среде обмана», выдается предупреждение с высокой точностью, что дает организации возможность принять решение – либо быстро исключить его из сети, либо изучить его методы и поведение в контролируемой среде. Доказано, что использование технологий «обманки» резко сокращает время пребывания злоумышленника в среде до того, как он будет обнаружен средствами контроля безопасности [10].

Одним из эффективных направлений технологий «обманки» является использование Honeypot, так называемых «медовых» ловушек, которые привлекательно выглядят для киберпреступника, но в реальности чувствительных данных не содержат, а только имитируют их наличие и возможность доступа. Иными словами, «обманка» с помощью Honeypot – проактивная защита, которая делает атаку более трудной для выполнения, и в то же время делает возможным нанесение ответного удара по злоумышленнику. В процессе взаимодействия с Honeypot атакующий раскрывает свои приемы, средства и возможности; может быть идентифицирован в дальнейшем при анализе массивов данных об аналогичных инцидентах [11]. Успешность применения технологий Honeypot-«обманки» в значительной степени зависит от того, насколько реалистично активы сети выглядят при попытке доступа извне, а также от того, насколько эффективно реализованы механизмы наблюдения и анализа происходящих в них событий.

В последнее время ряд исследователей склонны использовать термин Honeypot для обозначения совокупности использующих данный подход технологий, как концептуальное направление для различных прикладных решений.

Концепция Honeypot: решения, эволюция, противодействие, требования

В настоящее время абсолютно универсального решения, которое использует концепцию Honeypot, не существует. Если рассматривать ее как имитационную модель реального вычислительного процесса, то к любому программно-аппаратному решению на базе этой концепции применимо ограничение Тьюринга. Последнее требует применения субоптимальных (рациональных) подходов к реализации Honeypot-решений в контексте более конкретной задачи. Так появились решения на базе Honeypot, которые разделяются по объектам, категориям и области применения в сети (таблица 1).

Таблица отражает типичные технологические Honeypot-решения, составлена на основе анализа их функциональных возможностей и результатов тестирования, описанных в литературе с учетом специфики задач, и соответственно, имитируемых объектов. Функциональные возможности Honeypot-продуктов могут расширяться, области применения пересекаться, в т. ч. вследствие специфики сетей.

ТАБЛИЦА 1. Обзор Honeypot-«обманок» по областям применения [13]

Технологические решения	Объект «обманки»	Категория	Хост	Сеть
Fake Honeypot	Honeypot	Server	✗	✓
Honeyentries	Table, data set	Database	✓	✗
MTD	Topo., net. interf., memory, arch.	Versatile	✓	✓
Honeyword	Password	Authentica-tion	✓	✗
Honeyaccount	User account	Authentica-tion	✓	✗
Honeyfile	(Cloud-)File	File system	✓	✓
Honeypatch	Vulnerability	Server	✓	✓
–	Memory	Server	✓	✗
–	Metadata	File	✓	✗
HoneyURL	URL	File	✗	✓
Honeymail	E-Mail adress	File	✗	✓
Honeypeople	Social network profile	File	✗	✗
Honeyport	Network port	Server	✗	✓
Decep. web server	Error codes, Robot.txt	Server	✗	✓
OS interf.	System call	Server	✓	✗

Изначально Honeypot развивались, чтобы соответствовать наиболее актуальным угрозам, которые прогнозировались с учетом данных об инцидентах безопасности, и ориентировались в большей степени на узкие прикладные задачи конкретных сетей. По мере усложнения сетей и вычислительных систем, увеличению числа возможных угроз, усложнились задачи и для Honeypot. Их разработка стала циклическим процессом, так как требовала постоянного совершенствования для все более эффективного привлечения злоумышленников, используемых ими инструментов и вредоносных программ.

Вредоносные программы, захваченные на Honeypot, анализируются ретроспективно с целью последующей переработки приманки. С этой точки зрения вклад Honeypot в безопасность считается реактивным, если имитация реального объекта проста и предполагает только регистрацию действий, т. е. выявление не очень квалифицированного нарушителя. Простые Honeypot имитируют поведение реальных систем, однако даже беглый взгляд, например, на процесс и результаты сканирования, позволяет более квалифицированному нарушителю увидеть, что цель имеет аномальное количество открытых портов со службой удаленного управления (рисунок 1).

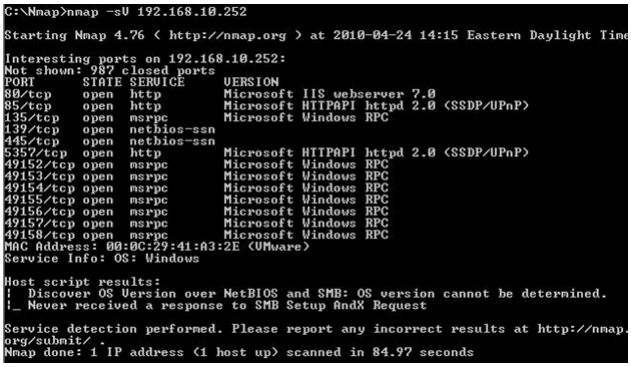


Рис. 1. Реакция Honeypot, имитирующая открытые порты MS Windows при сканировании с помощью nmap

Следующим этапом развития Honeypot стала более реальная имитация на основе паттернов реакции реальных систем. Но с началом использования в сетях Honeypot и развития решений на базе этой концепции, злоумышленниками стали разрабатываться и применяться инструментальные средства, основанные на различных методах детектирования (таблица 2, где mitigation – способ снижения эффективности метода детектирования).

ТАБЛИЦА 2. Обзор методов противодействия Honeypot [13]

Метод детектирования	Содержание, детали	Мишень	Mitigation
Временное поведение	Измерение RTT, чтобы выявить корреляции между IP-адресами	honeyed, virtual honeypots	Имитация времени поведения
Stack fingerprinting	Отправка поврежденных пакетов и анализ ответов	Имитация стеков связи	Реализация полного TCP / IP-стека
Функциональное зондирование	Использование предоставленных функций и проверка статуса	SMTP и DNS	Реализация полной функциональности
Поведение системных вызовов	Аномалии во временном поведении или локализации памяти	Система Linux	Имитация времени поведения, KASLR
Сетевой трафик	Анализ трафика сети RX и TX, например, количество байтов	Сетевая фильтрация данных, например, Sebek	Hinder network monitoring, VMI, Proxy
Обнаружение UML	Вывод dmesg, сетевое устройство, / proc /, структура памяти	UML-изоляция хоста	Инструменты манипуляции для показа информации
Обнаружение VMware	Аппаратное обеспечение, например, MAC-адрес, вход / выход бэкдор	Изоляция хоста на основе VMware	Настройка оборудования, патч I/O бэкдор
Обнаружение отладчика	Использование функции ptrace (), функции IsDebuggerPresent () или поиска в памяти для 0xCC	e.g. Cuckoo	–
Семантический разрыв	Управление структурой данных ядра	VMI	–
Кастомизация	Поиск строк по умолчанию	–	Настройка системы

В целом методы противодействия, основанные на концепции Honeypot-решениям, вырабатываются на базе выделения и анализа недостатков в моделировании сетевого объекта, выявления более примитивного в сравнении с реальными объектами поведения. Многие инструменты для создания Honeypot представляют собой ПО с открытым кодом, что облегчает их изучение злоумышленниками.

Honeypot-решения, как и технологии «обманки» в целом, в значительной степени основываются на человеческой психологии, поэтому единственным способом противостоять их обнаружению является развитие Honeypot по пути усложнения поведения, использования гибких масштабируемых конфигураций, которые могут быть построены на основе функционала и инструментов с открытым кодом.

Honeypot-решения в этом смысле должны быть в большей степени проактивны, максимально правдоподобно взаимодействуя с нарушителем, удерживая и провоцируя дополнительные действия, направляя по многовариантным ложным путям, предоставляя на пути проникновения в ложную систему задачи по преодолению сравнимых с реальной системой уровней сложности.

В числе характеристик таких решений целесообразно ввести параметр с условным названием *имитационная достоверность*, который должен оцениваться относительно 100-процентной вероятности того, что «медовые» ловушки не были определены как ложные активы и компоненты «обманки». Эффективность с учетом имитационной достоверности при этом можно рассматривать как результативность обнаружения атак, при которой они были обнаружены, но имитационный характер цели не был раскрыт злоумышленником.

Обзор результатов экспериментальных исследований применения технологии Honeypot-«обманок» на функционирующей инфраструктуре

В [14–26] подробно описан ряд «полевых» исследований технологий «обманки» с использованием Honeypot в университетских сетях. В этих статьях авторы провели анализ поведения как реальных, так и ирреальных (экспертов по безопасности) злоумышленников в уязвимой системе: они предоставили им атакуемую систему, в которой использовали ресурсы Honeypot, и следили за их поведением.

В первом раунде своего исследования Д. Франхольц и соавторы [14] предложили серверные Honeypot-приложения: ложные баннеры, фальшивый файл robots.txt, поддельные сообщения об ошибках, адаптивная задержка и honey-files. Было проверено 1 200 посещений злоумышленников. Во втором раунде авторы [15] проанализировали поведение злоумышленников, отслеживаемое в течение 222 дней с помощью шести Honeypots, развернутых на одном клиенте и пяти серверах веб-хостинга. Используемыми LIhoneypot отслеживались и контролировались более 12 млн. посещений. В Honeypot-объектах использовались протоколы honeytokenTP, honey-tokenTPS, FTP, POP3, SMTP, SSH и Telnet. Также имитировались протоколы Bacnet и Modbus для исследования угроз промышленным приложениям.

М. Лазаров и соавторы [16] преднамеренно поместили фиктивную конфиденциальную информацию в электронные таблицы Google, в т. ч. IP-адреса, призванные заманить злоумышленников. Было отслежено 174 клика, 44 посещения 39-ти уникальных IP-адресов.

Л. Лю и соавторы [17] следовали аналогичному подходу. Но в их эксперименте ключи SSH были выложены в свободный доступ на github, а Honeypot реализовывался на основе Cowrie. Контролировалось порядка 31 000 уникальных паролей и поведение пользователя после входа в систему в течение двух недель. Далее был выполнен анализ распределения наиболее часто использованных для осуществления атаки паролей из ежегодно публикуемыми SplashData списков наиболее употребительных паролей. Результат показал, что в 76 % атаки производились с IP-адресов, которые специально использовались для атаки и были квалифицированы как источники угроз сервисом IP Intelligence с вероятностью 1,0.

В [18] описан более сложный эксперимент: сформирована имитация сети организации, содержащая учетные записи пользователей, почтовые данные, документы, профили браузера и другие информационные ресурсы. В сеть были введены различные ловушки и приманки. Было организовано тестирование в форме квеста по принципу CTF (*от англ.* Capture the Flag – захват флага), в рамках которого специально привлеченным для этой цели экспертам по безопасности предлагалось осуществить проникновение в сеть и собрать некий актив из пяти расположенных в разных местах компонентов. Параллельно исследовалась реакция сети на автоматические атаки вредоносного ПО. В результате 100 % атак и людей, и машин были обнаружены как минимум одним из использованных средств, что доказало эффективность построенного Honeypot-решения, н вместе с тем и необходимость развития технологий симуляции в направлении усложнения поведения. Было отмечено, что, несмотря на не очень эффективные действия вначале, благодаря «knowledge gap» (разрыву между реальными знаниями атакующих и их самооценкой), этот разрыв по мере взаимодействия с объектами сети в ходе эксперимента существенно сокращался (что в частности демонстрировалось снижением числа используемых команд). А это позволяло прогнозировать относительно быструю выработку ими механизма выявления фиктивных активов при сохранении слож-

ности модели на первоначально предложенном уровне. Эксперимент также показал, что лучшие результаты были у атакующих, внимательно ознакомившихся с условиями задания (в которые намеренно были включены подсказки, что дополнительно акцентировало значимость наличия у атакующего предварительной информации для успешного проведения атаки).

Поведение атакующих после вторжения анализировалось в несколько ином аспекте и в более ранних работах. Целью эксперимента в [19] было определить характеристики подключений и классифицировать атаки, а также исследовать реакцию атакующих на предупреждающие баннеры. Для этого использовался набор данных Джонс [20], собранный с помощью HIhoneypot и содержащий 1 548 обращений от 478 атакующих. В эксперименте для развертывания Dionaea Honeypots использовались незадействованные IP-адреса сети университета Мэриленд; в ходе почти полугодового эксперимента 624 сеанса контролировались с помощью инструмента Honeypot Spy.

В аналогичном направлении (исследование реакции на баннеры) Д. Маймон и соавторы [21] выполнили два эксперимента, длительностью в 2 и 6 месяцев. В этих экспериментах использовались 86 и 502 компьютера соответственно. При подключении некоторые из них представляли предупреждающие баннеры. Рабочие станции также содержали различные уязвимые точки входа, созданные с использованием Sebek и OpenVZ в качестве шлюза, которые привлекли 1 058 и 3 768 вторжений соответственно.

Е. Хейрхак и соавторы [22] проанализировали учетные данные, использованные в ходе попыток логического подключения. 8 подключений Honeypot, которые были включены в SSH, представлены шести разным сетям университетского городка в течение семи недель. Было зафиксировано 98 180 соединений с 1 153 уникальных IP-адресов в 79 странах.

В [23, 24] Х. Цзян и соавторы применяли различные виды Honeypots, а именно: Dionaea, Mwcollector, Amun и Nepenthes, – которые использовались, для статистического анализа паттернов атак. Было выделено 5 периодов, в течение которых 166 атакующих проводили атаки на уязвимые сервисы: SMB, NetBIOS, honeytokenTP, MySQL и SSH.

С. Лорен и соавторы [25] проанализировали поведение злоумышленника на основе шаблонов нажатия клавиш. При этом были отслежены, как индикаторы для различных типов поведения, 24 различных действия злоумышленников.

Honeypot в количестве 3 единиц с различными конфигурациями, установленные на протяжении восьми месяцев в университетских сетях, были доступны через SSH и захватили 20 335 набранных команд в течение 1 171 сеанса атак.

Схожий подход был использован в [26]: 4 Linux honeypot были введены в университетскую сеть, доступную через SSH в течение 24 дней, с легко угадываемыми учетными данными. Действия злоумышленников контролировались с помощью syslog-ng (для захвата команд, быстрого доступа к системным вызовам) и Sebek (для сбора нажатий клавиш). Было собрано 269 262 попыток атак с 229 уникальных IP-адресов.

Следует отметить, что кроме различного рода Honeypot, использующих встроенные механизмы контроля, также часто применяются реальные системы с расширенными возможностями мониторинга, которые по определению относятся к HIhoneypot. Только две из описанных выше работ [15, 16] используют существенно различающиеся технологии «обманки», а наиболее сложный эксперимент, как представляется, описан в [18].

В обзоре [13] приводятся выполненные на основе опросов оценки вышерассмотренных (кроме [18]) и некоторых других экспериментов и использованных в них решений. Последние оценивались по таким признакам, как интерактивность, масштабируемость, юридические или этические соображения, тип, развертывание, преимущества и недостатки по сравнению с другими видами технологии защиты, качество и тип данных и полученные значения, тип ресурса технологии «обманки», технический способ развертывания и вид технологии «обманки», возможности обнаружения и предотвращения обнаружения и растяжимость. Оценка производилась по системе «да/нет» без более детальных характеристик. Будучи весьма условной, сравнительная оценка, тем не менее, отчетливо показала наряду с отсутствием идеального (или стремящегося к нему) решения, также и отсутствие решений, в которых бы сочетались интерактивность, масштабируемость и механизм предотвращения обнаружения.

Следует отметить, что все три характеристики взаимосвязаны и взаимопротиворечивы, и в некоторых рассмотренных решениях не могут сочетаться в силу имевшихся аппаратных ограничений. Как представляется, их сочетание может быть реализовано в Honeypot-решении на основе облачных вычислений. Масштабируемые устойчивые Honeypot-решения в облачной среде гипотетически могут также использоваться в качестве активной защиты для противодействия атакам, нацеленным на снижение производительности сети (DDoS-атаки), и могут быть реализованы с использованием подходов, изложенных в [27–29].

В контексте исследований технологий «обманки» и Honeypot-решений следует отметить также работы [30–34].

Предлагаемое решение

В интересах исследования и демонстрации возможностей Honeypot-решения для обеспечения безопасности, в корпоративных сетях был разработан специальный лабораторный стенд, созданный и протестированнный внутри системы Microsoft Azure. В качестве его основы был выбран Windows Server 2016 с развернутым веб-сервером Microsoft IIS. Устойчивость Honeypot исследовалась в условиях DDoS-атаки типа «TCP SYNFLOOD», для эмуляции которой развернут образ Kali linux для управления botnet-сетью (рисунок 2).

Веб-серверу с точки зрения вычислительных ресурсов выделено 1 ядро и 2 ГБ оперативной памяти. При генерации виртуальной машины (ВМ) в скрипте были прописаны условия автоматического создания реплик (instances) сервера и обработки трафика от него через подготовленный балансировщик. В рассматриваемой конфигурации ограничений по решаемым задачам и типам операционных систем нет.

Windows Server и IIS были выбраны из экономических и практических соображений, среди которых – простота эмуляции IIS web-сервера средствами honeyd. Windows server достаточно просто изобразить, поскольку он имеет значительное количество легко сканируемых портов, по которым можно определить, какие конкретно службы и сервисы запущены на публичном сервере. Однако слишком большое число портов может отпугнуть злоумышленника, так как крайне редко встречается в реальности.

Соответственно на honeyd реализована эмуляция базовых сервисов (сетевые сокеты 80/tcp, 443/tcp, 8080/tcp, 3389/tcp); также есть возможность получить базовые ответы. Обеим ВМ дана возможность соединяться с внешней средой с использованием «белых» (публичных) IP-адресов для возможности удаленного доступа к ВМ внутри стенда, а также для возможности реализации собственно DDoS-атаки, которая в исследовании реализована следующим образом. В качестве ботнет-сети выступают ВМ с установленной операционной системой Ubuntu и утилитой msfconsole, Command and Control (C&C); сервер Kali включает настроенный оркестратор Ansible. Из среды Kali через Ansible отдается команда о генерации TCP SYN-сообщений.

Для соответствующей подготовки ВМ был написан скрипт, в котором указана возможность масштабирования; сам же сервер создается один. При отработке системы реагирования на атаку предусмотрена возможность создать новые instances (реплики) с похожим набором параметров относительно шаблона ВМ. Сами реплики, как было указано ранее, являются Honeypot. При создании им выделяется меньше ресурсов: 1 ядро и 512 МБ оперативной памяти, но при этом настраивается сетевая карта с высокой производительностью (до 1 Гб/с). В скрипте на языке JSON указаны правила создания сетей и адаптеров ВМ, а также правила создания балансировщика нагрузки. В том числе в шаблоне указано ограничение на количество генерируемых ВМ, наличие публичных адресов и правила взаимодействия с балансировщиком. Также указаны правила прямого проброса интересующего трафика.

Балансировщик нагрузки реализован по принципу NAT-трансляций (*от англ.* Network Address Translation, преобразование сетевых адресов) в конкретный сетевой сокет реплики виртуальной машины с единым внешним IP-адресом (рисунок 3) и распределяет новые входящие потоки данных, которые поступают на внешний интерфейс для экземпляров внутреннего пула в соответствии с правилами и проверками работоспособности.

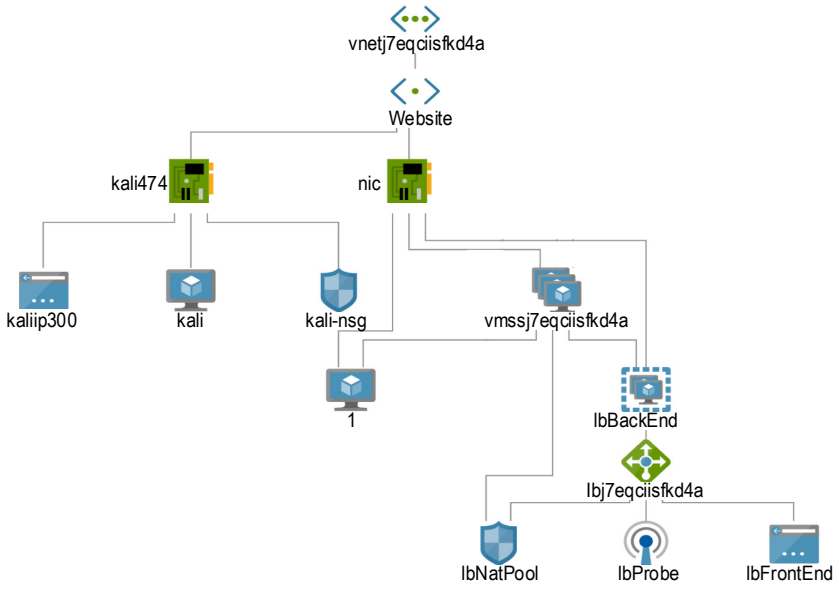


Рис. 2. Топология лабораторного стенда

Помимо этого, общедоступный балансировщик может предоставлять исходящие соединения для ВМ в виртуальной сети путем преобразования их частных IP-адресов в публичные. Все остальные сетевые сокеты при обработке входящего трафика он блокирует для того, чтобы не отпугнуть атакующего во время сканирования сетевой части веб-сервера.

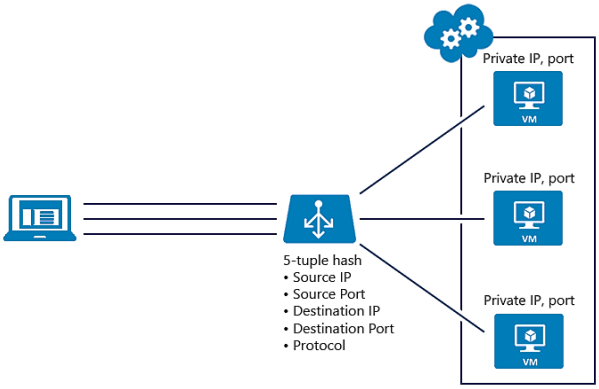


Рис. 3. Принцип балансировки нагрузки

По умолчанию балансировщик для сопоставления потоков с доступными серверами использует 5-элементный хэш, состоящий из IP-адреса источника, порта источника, IP-адреса назначения, порта назначения и номера протокола IP. Возможно создать сходство с конкретным исходным IP-адресом, выбрав двух- или трехэлементный хэш для данного правила. Все пакеты одного и того же потока пакетов поступают в один и тот же экземпляр за интерфейсом с балансировкой нагрузки. С помощью балансировщика можно создать входящее правило NAT для переноса трафика с определенного порта определенного IP-адреса внешнего интерфейса на определенный порт определенного внутреннего экземпляра внутри виртуальной сети. Это достигается тем же распределением на основе хэшей, что и для распределения нагрузки. Распространенными сценариями для этой возможности являются сеансы RDP (*от англ.* Remote Desktop Protocol, протокол удаленного рабочего стола) и SSH (*от англ.* Secure Shell, безопасная «оболочка») с отдельными экземплярами ВМ. Также можно сопоставить несколько внутренних конечных точек с различными портами на одном IP-адресе внешнего интерфейса.

Балансировщик нагрузки напрямую не взаимодействует с транспортным, пользовательским или прикладным уровнем, но может поддерживать любой сценарий TCP- или UDP-приложения. Он не прерывает и не инициирует потоки, взаимодействует с полезной нагрузкой потока, не предоставляет функции шлюза прикладного уровня, и протокольные «рукопожатия» всегда происходят непосредственно между клиентом и экземпляром ВМ. На каждую конечную точку отвечает только ВМ; ответ на запрос к внешнему интерфейсу является ответом, генерируемым серверной ВМ. При успешной проверке подключения к внешнему интерфейсу проверяется сквозное подключение по крайней мере к одной внутренней виртуальной машине. Публичный балансировщик отображает общедоступный IP-адрес и номер порта входящего трафика на частный IP-адрес и номер порта ВМ и, наоборот, для ответного трафика от ВМ. Применяя правила балансировки нагрузки, можно распределять определенные типы трафика между несколькими ВМ или службами.

При создании копии ВМ автоматически создаются новые правила; сами ВМ создаются прозрачно для администратора и эмулируют поведение на основе определенных параметров, выявленных системой по заданному паттерну, так же есть возможность генерировать автоматические сообщения администратору на почту или в SIEM-систему (*от англ.* Security Information and Event Management, системы управления событиями информационной безопасности).

Тестирование и анализ результатов

Как уже упоминалось, для исследования устойчивости решения была выбрана DDoS-атака, которая осуществлялась по открытому 80-му порту веб-сервера IIS. Отправной точкой послужил развернутый образ Kali linux, выступающий в качестве C&C-сервера, с которого была отдана команда на старт атаки, и некоторое количество хостов начали генерировать TCP-SYN. Хосты при генерации SYN-flood-а используют случайные порты источника и могут отправлять до 1 Гб/с трафика. Трафик попадает на балансировщик, которому предоставлена максимальная производительность сети (40 Гб/с). В скрипте прописано правило мониторинга загрузки процессора (CPU) и указаны пороговые значения, при которых происходит создание новых реплик ВМ и, соответственно, их удаление при спаде нагрузки.

После старта атаки происходит нарастание нагрузки на ВМ, который идет во время ожидания реакции системы на триггер для создания новой копии (рисунок 4). Осуществляется горизонтальное масштабирование сервиса, но сам сервис не увеличивает свою производительность – увеличивается только сетевая емкость за счет добавления «медовых» ловушек. И за счет увеличения производительности сети происходит снижение загрузки на основную реплику веб-сервера. В скрипте прописано правило: при наличии загрузки процессора более 90 % в течение 5 минут следует создать реплику Honeypot.

После создания одного нового инстанса происходит проверка правила и, если загрузка все еще больше 90 %, происходит создание еще одной реплики до тех пор, пока загрузка не упадет. Чтобы излишне не использовать вычислительные ресур-

сы, создано правило по удалению реплики при снижении средней загрузки по CPU.

На представленном графике (рисунок 5) видно, что при получении достаточно большого объема трафика возрастает нагрузка на CPU, вследствие чего происходит деградация конечного сервиса, которым могут пользоваться клиенты компании. Но после отработки реакции на триггер система начинает создавать новые реплики веб-сервера, и уже через 13 минут после атаки становится заметным линейный характер спада нагрузки на CPU сервера. Чем больше реплик генерируется в автоматическом режиме, тем меньше оказывается влияние на реальную инфраструктуру.

С точки зрения топологии (рисунок 6) рассматриваемой сети реплики веб-сервера находятся за балансировщиком трафика, и для пользователей конечного сервиса их количество незаметно. Но при этом имеется возможность снять нагрузку с ВМ и гарантировать определенный уровень сервиса на сайте компании.

Результат эксперимента показал возможность оказывать сервис клиентам в условиях активной защиты от атаки DDoS типа «TCP SYNFLOOD». Сегодня на рынке систем информационной безопасности существует несколько готовых решений, которые могут предложить не только горизонтальное масштабирование сервиса, но и вертикальное, позволяют не только в пределах облачной инфраструктуры разворачивать реплики ВМ. Имеются решения, которые не предоставляют автоматическое масштабирование среды, но дают возможность исследовать тип атаки и ее воздействие на сервис.

Предлагаемое решение может сочетать в себе масштабируемость, устойчивость и интерактивность, поскольку поведение Honeypot может формироваться на основе обновляемых паттернов, в него могут быть добавлены дополнительные механизмы мониторинга и др. Использование облачных ресурсов, аналогичных используемым реальной сетью в облачной среде, позволяет создавать масштабируемые Honeypot-решения с высокой имитационной достоверностью.

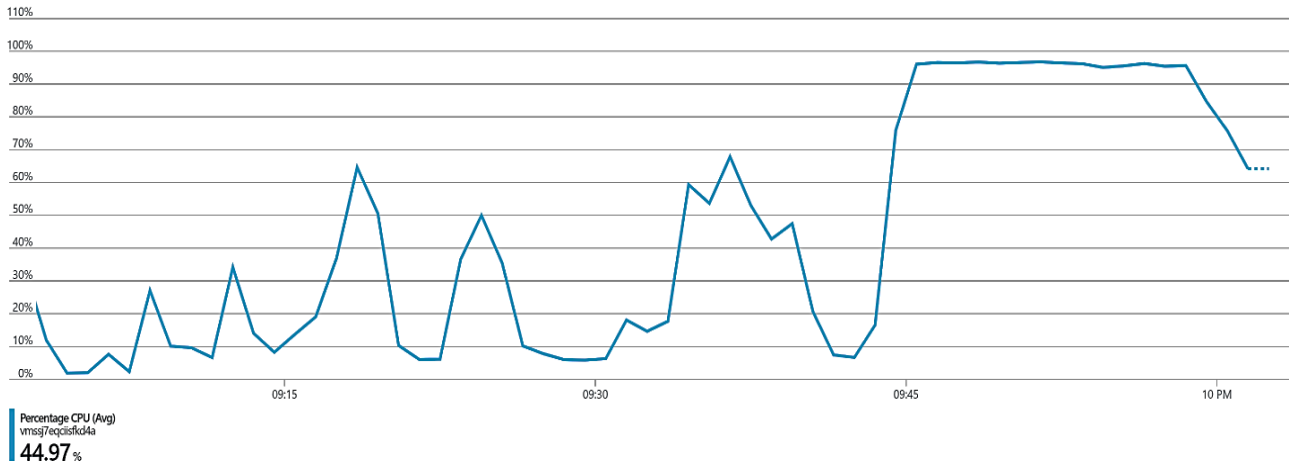


Рис. 4. График нагрузки CPU в начале атаки

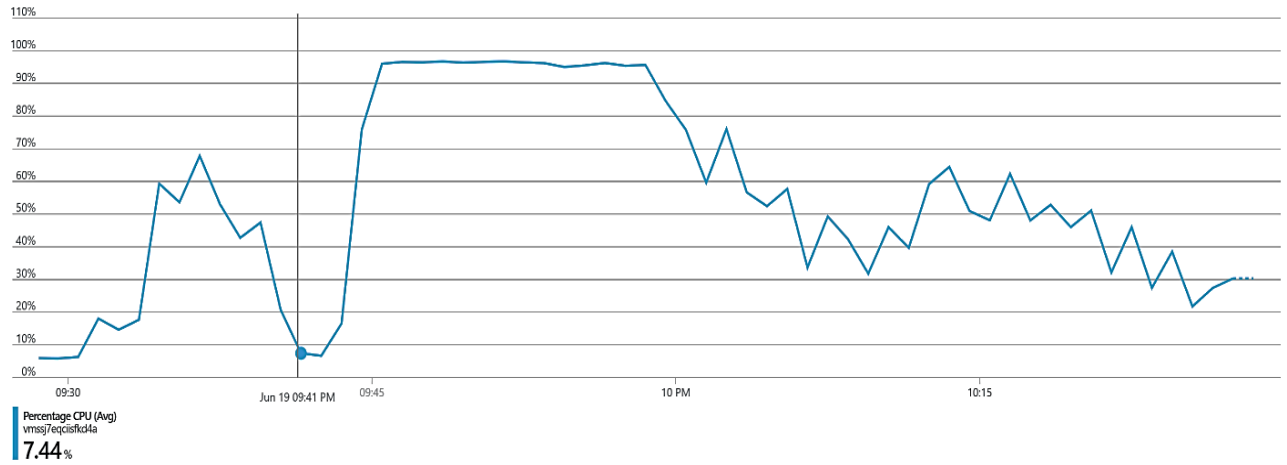


Рис. 5. Снижение нагрузки в зависимости от количества реплик

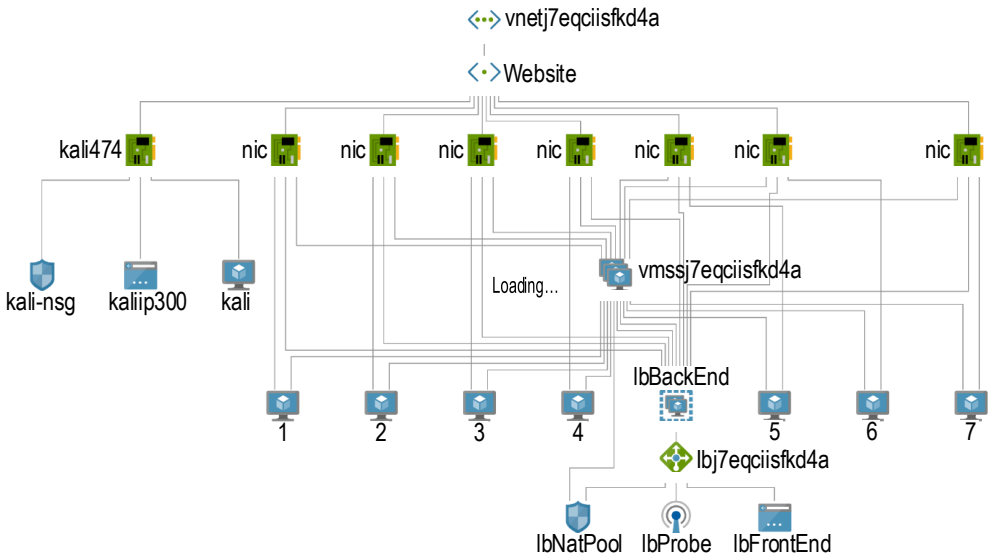


Рис. 6. Финальная топология

Заключение

В статье рассмотрен процесс создания масштабируемого Honeypot-решения, и исследована его работа с помощью стенда в среде Microsoft Azure. Использование технологии «обманки» потребовало разработки приложения, позволяющего применить механизмы копирования оконечного устройства и дублирование сервиса на его основе. Предложенный подход может быть расширен и масштабирован в качестве действующего решения в корпоративных сетях, построенных с использованием технологий облачных вычислений. В статье также отмечена необходимость разработки и применения системы показателей эффективности Honeypot-решений и комплексных решений с использованием технологий «обманки» на всех этапах создания для достижения высокой эффективности их практического использования.

Список используемых источников

1. 60 Must-Know Cybersecurity Statistics for 2019 // Varonis. URL: https://www.varonis.com/blog/cybersecurity-statistics (дата обращения 26.04.2019)

2. Буйневич М.В., Владыко А.Г., Доценко С.М., Симонина О.А. Организационно-техническое обеспечение устойчивости функционирования и безопасности сети связи общего пользования. СПб.: СПбГУТ, 2013. 192 с.

3. Буйневич М.В, Васильева И.Н, Воробьев Т.М, Гниденко И.Г, Егорова И.В, Еникеева Л.А и др. Защита информации в компьютерных системах. СПб.: Изд-во СПбГЭУ, 2017. 163 с.

4. Израилов К.Е. Анализ состояния в области безопасности программного обеспечения // II Международная научно-техническая и научно-методическая конференция «Актуальные проблемы инфотелекоммуникаций в науке и образовании» (Санкт-Петербург, Россия, 27–28 февраля 2013). СПб.: СПбГУТ, 2013. С. 874–877.

5. Израилов К.Е. Модель прогнозирования угроз телекоммуникационной системы на базе искусственной нейронной сети // Вестник ИНЖЭКОНа. Серия: Технические науки. 2012. № 8(59). С. 150–153.

6. Покусов В.В. Особенности взаимодействия служб обеспечения функционирования информационной системы // Информатизация и связь. 2018. № 5. С. 51–56.

7. Buinevich M., Fabrikantov P., Stolyarova E., Izrailov K., Vladyko A. Software Defined Internet of Things: Cyber Antifragility and Vulnerability Forecast // Proceedings of the 11th International Conference on Application of Information and Communication Technologies (AICT, Moscow, Russia, 20–22 September 2017). Piscataway, NJ: IEEE, 2017. PP. 293–297. DOI:10.1109/ICAICT.2017.8687021

8. Kotenko I., Kuleshov A., Ushakov I. Aggregation of elastic stack instruments for collecting, storing and processing of security information and events // Proceedings of the SmartWorld, Ubiquitous Intelligence & Computing, Advanced & Trusted Computed, Scalable Computing & Communications, Cloud & Big Data Computing, Internet of People and Smart City Innovation (SmartWorld/SCALCOM/UIC/ATC/CBDCom/IOP/SCI, San Francisco, USA, 4–8 August 2017). Piscataway, NJ: 2017. DOI:10.1109/UIC-ATC.2017.8397627

9. Котенко И.В., Левшун Д.С., Чечулин А.А., Ушаков И.А., Красов А.В. Комплексный подход к обеспечению безопасности киберфизических систем на основе микроконтроллеров // Вопросы кибербезопасности. 2018. № 3(27). С. 29–38. DOI:10.21681/2311-3456-2018-3-29-38

10. Котенко И.В., Ушаков И.А., Пелёвин Д.В., Овраменко А.Ю. Гибридная модель базы данных NoSQL для анализа сетевого трафика // Защита информации. Инсайд. 2019. № 1(85). С. 46–54.

11. Котенко И.В., Ушаков И.А. Использование технологий больших данных для мониторинга инцидентов информационной безопасности // Юбилейная XV Санкт-Петербургская Международная Конференция «Региональная Информатика (РИ-2016)» (Санкт-Петербург, Россия, 26–28 октября 2016). СПб.: СПОИСУ, 2016. С. 168–169.

12. Ушаков И.А., Котенко И.В., Крылов К.Ю. Анализ методик применения концепции больших данных для мониторинга безопасности компьютерных сетей // IX Санкт-Петербургская межрегиональная конференция «Информационная безопасность регионов России (ИБРР-2015)» (Санкт-Петербург, Россия, 28–30 октября 2015). СПб.: СПОИСУ, 2015. С. 75–76.

13. Fraunholz D., Anton S.D., Lipps C., Reti D., Krohmer D., Pohl F, et al. Demystifying Deception Technology: A Survey. 2018. DOI:10.13140/RG.2.2.30392.65288

14. Fraunholz D., Zimmermann M., Schotten H.D. Towards Deployment Strategies for Deception Systems // Advances in Science, Technology and Engineering Systems Journal. 2017. Vol. 2. Iss. 3. PP. 1272–1279.

15. Fraunholz D., Schotten H.D. Defending Web Servers with Feints, Distraction and Obfuscation // Proceedings of the International Conference on Computing, Networking and Communications (ICNC, Maui, USA, 5–8 March 2018). Piscataway, NJ: IEEE, 2018. DOI:10.1109/ICCNC.2018.8390365

16. Lazarov M., Onaolapo J., Stringhini G. Honey Sheets: What Happens to Leaked Google Spreadsheets? // Proceedings of the 9th Workshop on Cyber Security Experimentation and Test (CSET, Austin, USA, 8 August 2016). Berkeley: USENIX, 2016. URL: https://www.usenix.org/system/files/conference/cset16/cset16-paper-lazarov.pdf (дата обращения 17.09.2019)

17. Liu L., Mahar K., Virdi C., Zhou H. Hack Like no One is Watching: Using a Honeypot to Spy on Attackers. MIT Computer and Network Security Term Projects, 2016. URL: http://docplayer.net/21979034-Hack-like-no-one-is-watching-using-a-honeypot-to-spy-on-attackers.html (дата обращения 17.09.2019)

18. Applying Deception Mechanisms for Detecting Sophisticated Cyber Attacks // A Research Paper by TopSpin Security. October 2016. URL: https://www.cyentia.com/library-item/applying-deception-mechanisms-for-detecting-sophisticated-cyber-attacks (дата обращения 14.06.2019)

19. Robin B., Cukier M. An evaluation of connection characteristics for separating network attacks // International Journal of Security and Networks. 2009. Vol. 4. Iss. 1-2. PP. 110–24. DOI:10.1504/IJSN.2009.023430

20. Jones H.M. The Restrictive Deterrent Effect of Warning Messages on the Behavior of Computer System Trespassers. PhD Thesis. College Park: University of Maryland, 2014.

21. Maimon D., Alper M., Sobesto B., Cuckier M. Restrictive deterrent effects of a warning banner in an attacked computer system // Criminology. 2014. Vol. 52. Iss. 1. DOI:10.1111/1745-9125.12028

22. Kheirkhah E., Amin S.M.P., Sistani H.A., Acharya H.S. An experimental study of SSH attacks by using Honeypot Decoys // Indian Journal of Science and Technology. 2013. Vol. 6. Iss. 12. PP. 5567–5578.

23. Jiang X., Wang X., Xu D. Stealthy Malware Detection Through VMM-based "Out-of-the-box" Semantic View Reconstruction // Proceedings of the 14th ACM Conference on Computer and Communications Security (CCS, Alexandria, USA). New York: ACM Press, 2007. DOI:10.1145/1315245.1315262

24. Jiang X., Wang X. "Out-of-the-box" Monitoring of VM-Based High-Interaction Honeypots // Proceedings of the 10th International Symposium on Recent Advances in Intrusion Detection (RAID, Gold Goast, Australia, 5–7 September 2007). Lecture Notes in Computer Science. Berlin, Heidelberg: Springer, 2007. Vol. 4637. DOI:10.1007/978-3-540-74320-0_11

25. Laurén S., Rauti S., Leppänen V. An Interface Diversified Honeypot for Malware Analysis // Proceedings of the 10th European Conference on Software Architecture Workshops (ECSAW, Copenhagen, Denmark, 28 November – 02 December 2016). New York: ACM Press, 2016. DOI:10.1145/2993412.2993417

26. Al-Shaer E., Duan Q., Jafarian J. Random Host Mutation for Moving Target Defense // Proceedings of the 8th International Conference on Security and Privacy in Communication Networks (SecureComm, Padua, Italy, 3–5 September 2012). Lecture Notes of the Institute for Computer Sciences, Social Informatics and Telecommunications Engineering. Berlin: Springer, 2012. Vol. 106. DOI:10.1007/978-3-642-36883-7_19

27. Krasov A.V., Levin M.V., Shterenberg S.I., Isachenkov P.A. Traffic flow management model in software-defined networks with unequal load metric // H&ES Research. 2016. Vol. 8. Iss. 4. PP. 70–74.

28. Красов А.В., Левин М.В., Цветков А.Ю. Управление сетями передачи данных с изменяющейся нагрузкой // Всероссийская научная конференция по проблемам управления в технических системах. СПб.: Санкт-Петербургский государственный электротехнический университет, 2015. № 1. С. 141–146.

29. Красов А.В., Левин М.В., Штеренберг С.И., Исаченков П.А. Методология управления потоками трафика в программно-определяемой адаптивной сети // Вестник Санкт-Петербургского государственного университета технологии и дизайна. Серия 1: Естественные и технические науки. 2016. № 4. С. 3–8.

30. Whaley B. Toward a general theory of deception // Journal of Strategic Studies. 1982. Vol. 5. Iss. 1. PP. 178–192. DOI:10.1080/01402398208437106

31. Barros A. DLP and honeytokens. 2007. URL: http://blog.securitybalance.com/2007/08/dlp-and-honeytokens.html (дата обращения 17.09.2019)

32. Spitzner L. The Honeynet Project: Trapping the Hackers. URL: https://pdfs.semanticscholar.org/ec08/e8c4537db092da8c1fd239f2d9fe189d56d6.pdf (дата обращения 17.09.2019)

33. Sobesto B. Empirical Studies based on Honeypots for Characterizing Attackers Behaviour. PhD Thesis. College Park: University of Maryland, 2015.

34. Sentanoe S., Taubmann B., Reiser H.P. Virtual Machine Introspection Based SSH Honeypot // Proceedings of the 4th Workshop on Security in Highly Connected IT Systems (SHCIS, Neuchatel, Switzerland, 19–22 June 2017). New York: ACM Press, 2017. DOI:10.1145/3099012.3099016

* * *

SCALABLE HONEYPOT SOLUTION FOR CORPORATE NETWORKS SECURITY PROVISION

A. Krasov[1], R. Petriv[1*], D. Sakharov[1], N. Storozhuk[1], I. Ushakov[1]

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

Article info
The article was received 26 July 2019

For citation: Krasov A., Petriv R., Sakharov D., Storozhuk N., Ushakov I. Scalable Honeypot Solution for Corporate Networks Security Provision. *Proceedings of Telecommunication Universities*. 2019;5(3):86–97. (in Russ.) Available from: https://doi.org/10.31854/1813-324X-2019-5-3-86-97

Abstract: *Trends in modern security technologies with honeypot technologies use are analyzed to detect and explore intruders behavior for counteract measures development. Scalable solution proposed and tested within Microsoft Azure exploratory installation. DDoS attack stress test of the solution is performed.*

Keywords: *corporate networks, cloud computing, deception technologies, honeypot technologies, infocommunication networks security, cyberthreats, DDoS attack.*

References

1. Varonis. *60 Must-Know Cybersecurity Statistics for 2019*. Available from: https://www.varonis.com/blog/cybersecurity-statistics [Accessed 26th April 2019]

2. Buinevich M.V., Vladyko A.G., Dotsenko S.M., Simonina O.A. *Organizational and technical provision of functioning and security of public communications network*. St. Petersburg: The Bonch-Bruevich Saint-Petersburg State University of Telecommunications Publ.; 2013. 192 p. (in Russ.)

3. Buinevich M.V., Vasilyeva I.N., Vorobev T.M., Gnidenko I.G., Egorova I.V., Enikeeva L.A., et al. *Zashchita informatsii v kompiuternykh sistemakh* [Information Security in Computer Systems]. St. Petersburg: Saint-Petersburg State University of Economics Publ.; 2017. 163 p. (in Russ.)

4. Izrailov K. Analysis of the Security State of Software. *Proceedings of the IId International Conference on Infotelecommunications in Science and Education, 27–28 February 2013, St. Petersburg, Russia*. St. Petersburg: The Bonch-Bruevich Saint-Petersburg State University of Telecommunications Publ.; 2013. p.874–877. (in Russ.)

5. Izrailov K. Model of Forecasting the Telecommunication System Threats on the Basis of the Artificial Neural Network. *Vestnik INZHEKONa. Seriia: Tekhnicheskie nauki*. 2012;8(59):150–153. (in Russ.)

6. Pokusov V.V. Features of Interaction of Services for the Operation of the Information System. *Informatizatsiia i sviaz*. 2018;5:51–56. (in Russ.)

7. Buinevich M., Fabrikantov P., Stolyarova E., Izrailov K., Vladyko A. Software Defined Internet of Things: Cyber Antifragility and Vulnerability Forecast. *Proceedings of 11th International Conference on Application of Information and Communication Technologies, AICT, 20–22 September 2017, Moscow, Russia*. Piscataway, NJ: IEEE; 2017. p.293–297. Available from: https://doi.org/10.1109/ICAICT.2017.8687021

8. Kotenko I., Kuleshov A., Ushakov I. Aggregation of elastic stack instruments for collecting, storing and processing of security information and events. *Proceedings of the SmartWorld, Ubiquitous Intelligence & Computing, Advanced & Trusted Computed, Scalable Computing & Communications, Cloud & Big Data Computing, Internet of People and Smart City Innovation (SmartWorld/SCALCOM/UIC/ATC/CBDCom/IOP/SCI, 4–8 August 2017, San Francisco, USA*. Piscataway, NJ; 2017. Available from: https://doi.org/10.1109/UIC-ATC.2017.8397627

9. Kotenko I., Levshun D., Chechulin A., Ushakov I., Krasov A. Integrated Approach to Provide Security of Cyber-Physical Systems Based on Microcontrollers. *Voprosy kiberbezopasnosti*. 2018;3(27):29–38. (in Russ.) Available from: https://doi.org/10.21681/2311-3456-2018-3-29-38

10. Kotenko I.V., Ushakov I.A., Pelevin D.V., Ovramenko A. Yu. Hybrid NoSQL Database Model for Analysis of Network Traffic. *Zaŝita informacii. Inside*. 2019;1(85):46–54. (in Russ.)

11. Kotenko I.V., Ushakov I.A. Using big data technologies to monitor information security incidents. *Proceedings of the XV Anniversary St. Petersburg Internatonal Conference "Regional Informatics (RI-2016)", 26–28 October 2016, St. Petersburg, Russia.* St. Petersburg.: Sankt-Peterburgskoe obshchestvo informatiki vychislitelnoi tekhniki sistem sviazi i upravleniia; 2016. p.168–169. (in Russ.)

12. Ushakov I.A., Kotenko I.V., Крылов К. Yu. Analysis of methods of application of the big data concept for monitoring the security of computer networks. *Proceedings of the IX St. Petersburg Interregional Conference "Information Security of Russian Regions (ISRR-2015)", 28–30 October 2015, St. Petersburg, Russia.* St. Petersburg.: Sankt-Peterburgskoe obshchestvo informatiki vychislitelnoi tekhniki sistem sviazi i upravleniia; 2015. p.75–76. (in Russ.)

13. Fraunholz D., Anton S.D., Lipps C., Reti D., Krohmer D., Pohl F, et al. *Demystifying Deception Technology: A Survey*. 2018. Available from: https://doi.org/10.13140/RG.2.2.30392.65288

14. Fraunholz D., Zimmermann M., Schotten H.D. Towards Deployment Strategies for Deception Systems. *Advances in Science, Technology and Engineering Systems Journal*. 2017;2(3):1272–1279.

15. Fraunholz D., Schotten H.D. Defending Web Servers with Feints, Distraction and Obfuscation. *Proceedings of the International Conference on Computing, Networking and Communications, ICNC, 5–8 March 2018, Maui, USA*. Piscataway, NJ: IEEE; 2018. Available from: https://doi.org/10.1109/ICCNC.2018.8390365

16. Lazarov M., Onaolapo J., Stringhini G. Honey Sheets: What Happens to Leaked Google Spreadsheets? *Proceedings of the 9th Workshop on Cyber Security Experimentation and Test, CSET, 8 August 2016, Austin, USA*. Berkeley: USENIX; 2016. Available from: https://www.usenix.org/system/files/conference/cset16/cset16-paper-lazarov.pdf [Access 17th September 2019]

17. Liu L., Mahar K., Virdi C., Zhou H. *Hack Like no One is Watching: Using a Honeypot to Spy on Attackers*. MIT Computer and Network Security Term Projects. 2016. Available from: http://docplayer.net/21979034-Hack-like-no-one-is-watching-using-a-honeypot-to-spy-on-attackers.html [Access 17th September 2019]

18. *Applying Deception Mechanisms for Detecting Sophisticated Cyber Attacks. A Research Paper by TopSpin Security*. October 2016. Available from: https://www.cyentia.com/library-item/applying-deception-mechanisms-for-detecting-sophisticated-cyber-attacks [Access 14th June 2019]

19. Robin B., Cukier M. An evaluation of connection characteristics for separating network attacks. *International Journal of Security and Networks*. 2009;4(1-2):110–24. Available from: https://doi.org/10.1504/IJSN.2009.023430

20. Jones H.M. *The Restrictive Deterrent Effect of Warning Messages on the Behavior of Computer System Trespassers*. PhD Thesis. College Park: University of Maryland; 2014.

21. Maimon D., Alper M., Sobesto B., Cuckier M. Restrictive deterrent effects of a warning banner in an attacked computer system. *Criminology*. 2014;52(1). Available from: https://doi.org/10.1111/1745-9125.12028

22. Kheirkhah E., Amin S.M.P., Sistani H.A., Acharya H.S. An experimental study of SSH attacks by using Honeypot Decoys. *Indian Journal of Science and Technology*. 2013;6(12):5567–5578.

23. Jiang X., Wang X., Xu D. Stealthy Malware Detection Through VMM-based "Out-of-the-box" Semantic View Reconstruction. *Proceedings of the 14th ACM Conference on Computer and Communications Security, CCS, Alexandria, USA*. New York: ACM Press; 2007. Available from: https://doi.org/10.1145/1315245.1315262

24. Jiang X., Wang X. "Out-of-the-box" Monitoring of VM-Based High-Interaction Honeypots. *Proceedings of the 10th International Symposium on Recent Advances in Intrusion Detection, RAID, 5–7 September 2007, Gold Goast, Australia. Lecture Notes in Computer Science*. Berlin, Heidelberg: Springer; 2007. vol.4637. Available from: https://doi.org/10.1007/978-3-540-74320-0_11

25. Laurén S., Rauti S., Leppänen V. An Interface Diversified Honeypot for Malware Analysis. *Proceedings of the 10th European Conference on Software Architecture Workshops, ECSAW, 28 November – 02 December, 2016, Copenhagen, Denmark*. New York: ACM Press; 2016. Available from: https://doi.org/10.1145/2993412.2993417

26. Al-Shaer E., Duan Q., Jafarian J. Random Host Mutation for Moving Target Defense. *Proceedings of the 8th International Conference on Security and Privacy in Communication Networks, SecureComm, 3–5 September 2012, Padua, Italy. Lecture Notes of the Institute for Computer Sciences, Social Informatics and Telecommunications Engineering*. Berlin: Springer; 2012. vol.106. Available from: https://doi.org/10.1007/978-3-642-36883-7_19

27. Krasov A.V., Levin M.V., Shterenberg S.I., Isachenkov P.A. Traffic flow management model in software-defined networks with unequal load metric. *H&ES Research*. 2016;8(4):70–74.

28. Krasov A.V., Levin M.V., Tcvetkov A.I. Upravlenie setiami peredachi dannykh s izmeniaiushcheisia nagruzkoi [Management of Data Networks with Variable Load]. *Vserossiiskaia nauchnaia konferentsiia po problemam upravleniia v tekhnicheskikh sistemakh* [All-Russian Scientific Conference on Management Problems in Technical Systems]. St. Petersburg: Saint-Petersburg Electrotechnical University Publ.; 2015. iss.1. p.141–146. (in Russ.)

29. Krasov A.V., Levin M.V., Shterenberg S.I., Isachenkov P.A. Methodology Research on the Efficiency of the Traffic Flow Management Method Based on the Information About the Load of Software-Defined Networks with Unequal Route Metric. *Vestnik of St. Petersburg State University of Technology and Design. Series 1. Natural and technical science*. 2016;4:3–8. (in Russ.)

30. Whaley B. Toward a general theory of deception. *Journal of Strategic Studies*. 1982:5(1):178–192. DOI:10.1080/01402398208437106

31. Barros A. *DLP and honeytokens*. 2007. Available from: http://blog.securitybalance.com/2007/08/dlp-and-honeytokens.html [Access 17th September 2019]

32. Spitzner L. *The Honeynet Project: Trapping the Hackers*. URL: https://pdfs.semanticscholar.org/ec08/e8c4537db092da8c1fd239f2d9fe189d56d6.pdf [Access 17th September 2019]

33. Sobesto B. *Empirical Studies based on Honeypots for Characterizing Attackers Behaviour*. PhD Thesis. College Park: University of Maryland; 2015.

34. Sentanoe S., Taubmann B., Reiser H.P. Virtual Machine Introspection Based SSH Honeypot. *Proceedings of the 4th Workshop on Security in Highly Connected IT Systems, SHCIS, 19–22 June 2017, Neuchatel, Switzerland*. New York: ACM Press; 2017. Available from: https://doi.org/10.1145/3099012.3099016

МАТЕМАТИЧЕСКОЕ МОДЕЛИРОВАНИЕ И ЧИСЛЕННЫЕ МЕТОДЫ АНАЛИЗА НЕЙРОННЫХ СТРУКТУР

Л.М. Макаров[1], А.В. Поздняков[2, 3, 4], С.В. Протасеня[1*], Д.О. Иванов[2], В.С. Львов[2], С.Н. Львов[2]

[1]Санкт-Петербургский государственный университет телекоммуникаций им. проф. М.А. Бонч-Бруевича, Санкт-Петербург, 193232, Российская Федерация
[2]Санкт-Петербургский государственный педиатрический медицинский университет, Санкт-Петербург, 194100, Российская Федерация
[3]Северо-Западный государственный медицинский университет им. И.И. Мечникова, Санкт-Петербург, 191015, Российская Федерация
[4]Российский научный центр радиологии и хирургических технологий им. акад. А.М. Гранова, Санкт-Петербург, 197758, Российская Федерация
*Адрес для переписки: saitvodabur@yandex.ru

Информация о статье
УДК 519.61
Статья поступила в редакцию 26.06.2019

Ссылка для цитирования: Макаров Л.М., Поздняков А.В., Протасеня С.В., Иванов Д.О., Львов В.С., Львов С.Н. Математическое моделирование и численные методы анализа нейронных структур // Труды учебных заведений связи. 2019. Т. 5. № 3. С. 98–107. DOI:10.31854/1813-324X-2019-5-3-98-107

Аннотация: *В статье представлена математическая модель топологического описания нейронных структур головного мозга человека, описывающая процедуры численного анализа результатов магниторезонансной томографии. Созданная модель обеспечивает возможность построения облачной вычислительной среды, реализующей синтез количественных показателей различия анализируемых фрагментов нейронной ткани, которая создается средствами телекоммуникационного сервиса, способствующего вовлечению в процесс исследования большого количества специалистов в создание набора априорных суждений об эволюции регистрируемых процессов.*

Ключевые слова: *математическая модель, облачные вычисления, компьютерный анализ, нейронная структура.*

Организация и проведение научных исследований в современных условиях повсеместного использования компьютерных технологий основывается на большом материале междисциплинарных знаний. Потенциал знаний современной биофизики в значительной степени обновляется посредством большого количества научных исследований в области классической физики, биохимии, биологии и математики. Математические концепции, описывающие сложные биофизические процессы, формируются в терминах смежных научных дисциплин. Постоянно расширяющееся поле понятий актуализирует проблему создания аналитической среды, где широко представлены технологии интерактивного синтеза суждений, позволяющих формировать прогнозы развития событий в организме человека на основе результатов инструментального исследования.

Инструментальные исследования представляются как процесс создания комплексной аналитической среды, и осуществляются на основе вычислительных средств. Типичные решения в этой области формируются по двухуровневой схеме: создание математической модели вычислительного процесса, получение оценок исследуемого процесса и разработка модели сетевого доступа к конфигурационному вычислительному ресурсу. Второй уровень в современной терминологии соотносят с облачными вычислениями, реализуемыми для большого количества пользователей. «Публичное» облако позволяет средствами современных инфотелекоммуникаций обеспечить масштабные работы по анализу результатов перспективных медико-биологических исследований. В таком понимании телекоммуникационные средства и технологии представляются важнейшей составляющей в процессе познания особенностей развития нейронных структур.

Одним из перспективных методов научных исследований нейронных структур является магниторезонансная томография (МРТ). Разработка математических моделей интерпретации результатов

исследования посредством компьютерных технологий рассматривается в качестве первоочередной задачи, решение которой в будущем обеспечит построение системы облачных вычислений.

Создавая технические системы исследования живого организма, постоянно обновляется аксиоматический базис, способствующий формированию новых воззрений на эволюцию живой материи. Так, например, успехи в квантовой теории строения атома запустили обширный механизм исследований в области ядерного магнитного резонанса (ЯМР), которые с течением времени воспроизвели серию медицинских МРТ, значительно дополнив представления о нейронной сети, в частности структур головного мозга (СГМ) [1].

Расширяя эти представления, укажем, что компьютерный топологический анализ фреймов МРТ, создаваемых техническими средствами обработки сигналов ЯМР, представляется хорошо известной процедурой формирования профессиональных суждений о функциональном состоянии нейронной ткани СГМ. Значительное укрепление профессиональных суждений о состоянии СГМ является актуальной задачей, решение которой целесообразно вести в терминах и понятиях вычислительной компьютерной геометрии, где, оперируя понятиями точки, линии, многоугольника и поверхности, синтезируется искомое суждение о топологии нейронной структуры с набором количественных показателей.

Следует признать, что основные понятия и определения вычислительной геометрии составляют основу квантовой физики, широко оперирующей понятиями точечного объекта в нелинейном пространстве.

Проникновение сугубо теоретических квантовых постулатов в медицинскую практику создало основы развития квантовой биофизики. В этом эволюционном процессе витального развития биофизики отчетливо просматривается строгая линия взаимной связи материальных явлений, прослеживаемых от простейшей молекулы до сложной организации целостного организма. Размеры типичных молекулярных соединений, которые чрезвычайно широко распространены в структуре живых организмов, составляют 10^{-15} м. Атомарно-молекулярные конструкции биологической ткани разных видов обладают сложным строением и многообразием функциональных правил организации гомеостазиса.

Развивая общие представления о гомеостазисе, акцентируем внимание на энергетике отдельной клетки и клеточных кластеров. Эта тематическая линия исследований функционального состояния организма постоянно пополняется новыми представлениями, формируемыми на основе современных инструментальных исследований [2].

Отмечено, что в основе процессов изменения энергетического потенциала молекулы, по аналогии с атомарной конструкцией, находится процедура изменения электронной конфигурации, образующей периферическую часть молекулы. Изменение электронной конфигурации молекулы характеризуется переходным процессом – возбуждением, при котором изменяется кривая зависимости электронной энергии от расстояния между ядрами атомов [3]. При заданной электронной конфигурации атомы молекулы могут совершать колебательное движение относительно друг друга и вращаться относительно общего центра инерции. Полную энергию какого-либо стационарного состояния молекулы можно представить в виде аддитивного набора:

$$W = W_e + W_y + W_r, \qquad (1)$$

где W_e – энергия, обусловленная электронной конфигурацией; W_y – энергия колебательного движения; W_r – энергия вращательного движения.

Используя уравнения квантовой механики, установлено, что не только при изменении электронной конфигурации, но и при изменении энергии колебательного и вращательного движений энергия указанных видов движения характеризуется дискретными значениями [4].

Следуя этим представлениям, в системе, представленной из N частиц (атомов, молекул), количество частиц с энергией E_i определяется соотношением Л. Больцмана [5]:

$$n_i = A(\omega_i)\exp\left(-\left(\frac{E_i}{\kappa T}\right)\right), \qquad (2)$$

где ω_i – статистический вес (число возможных состояний частицы с энергией E_i); T – температура; постоянная A находится из условия, что сумма n_i по всем возможным значениям i равна заданному полному числу частиц N в системе (условие нормировки): $\sum_i n_i = N$; $A = 1/N$; $\kappa = 1{,}38 \cdot 10^{-23}$ Дж/К.

На начальном этапе развития статистических представлений о распределении энергии внутри системы оценка энергетического состояния рассматривалась исключительно для наблюдаемой материальной системы, обладающей множеством частиц. Эта оценка создавалась в рамках классической статистики, которая в последующем стала основой для формулировки постулатов квантовой статистики. Расширяя представления о физических основах процессов Природы, квантовая статистика привела к открытию распределений Бозе – Эйнштейна для частиц с целым спином и распределений Ферми – Дирака для частиц с полуцелым спином [6].

Теоретические положения квантовой физики, рассматривающие состояние сложной системы, представленной набором химических элементов, воспроизвели основные принципы создания технической системы, реализующей ЯМР. Наличие ин-

струментального средства исследования на основе ЯМР позволило использовать эффект резонансного радиочастотного поглощения электромагнитной энергии различными веществами с ненулевым магнитным моментом ядер, помещенных во внешнее постоянное магнитное поле. Типичными представителями таких веществ являются ядра химических элементов: ^{1}H, ^{2}H, ^{13}C, ^{14}N, ^{15}N.

Методология проведения исследований на основе ЯМР формируется на физических представлениях о том, что, создавая стационарное магнитное поле B_0 и дополняя этот физический фактор радиочастотным полем B_1, реализуется энергетическое воздействие на молекулярный кластер.

Типичный биологический объект можно охарактеризовать жидким кристаллом, представленным водной средой. Вода – это прежде всего водород и протонные кластеры, которые под действием внешнего электромагнитного поля разворачиваются по направлению силовых линий поля. Ориентация магнитных диполей по силовым линиям поля является вынужденной, а потому возникает явление прецессии, которая в квантовой физике определяется как Ларморова частота. При включении источника излучения радиоволн (РЧ1), магнитные моменты протонных образований начинают вращаться по часовой стрелке. Аналитическая система томографа фиксирует состояние магнитного резонанса.

Для веществ, у которых ядерный спин составляет полуцелое значение, а это в первую очередь водород, входящий в состав воды, наблюдается энергетическая смена состояний атомарной конструкции. В поле B_0 для атомарной молекулярной конструкции оказываются возможны только два состояния – невозбужденное (E_0) и возбужденное (E_1). Именно этот эффект порождает смену ориентации магнитного дипольного момента у ядер атома водорода (рисунок 1).

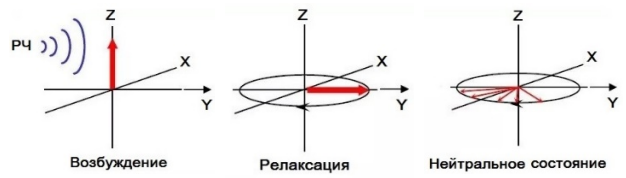


Рис. 1. Схема состояний магнитного диполя ядра водорода

В терминах теории Л. Больцмана в состоянии термодинамического (статистического) равновесия большое количество спинов (N) характеризуется небольшой энергией, условно равномерно распределенной по всему ансамблю атомов [5]. Напротив, при наложении на объект исследования внешнего поля уровень энергии возрастает. В нормальных условиях лаборатории при температуре 18–20 ˚С в магнитном поле 0,25 Тл разность концентраций спинов, направленных вдоль и против магнитного поля, незначительна – примерно один протон на миллион ядер.

Разность энергий ΔE между невозбужденным и возбужденным состоянием определяется так:

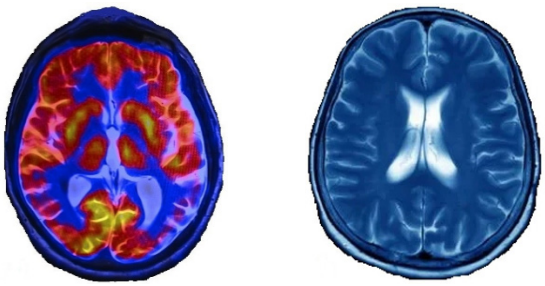
$$\Delta E = \hbar\omega_0, \qquad (3)$$

где $\hbar$ – постоянная Планка; ω_0 – частота электромагнитного излучения, необходимая для перехода системы из одного состояния в другое.

Синхронные колебания протонных кластеров с радиочастотой источника (РЧ1) фиксируются детекторами (РЧ2) томографа. Импульсное включение РЧ1, а затем фиксация детекторами РЧ2 радиочастотного отклика от водородного кластера характеризуется возрастающим уровнем прецессии, что соответствует физическим представлениям о повышении намагниченности водородных ядер кластера. Многократное повторение этой процедуры создает пространственный портрет распределения атомов водорода в исследуемом объекте.

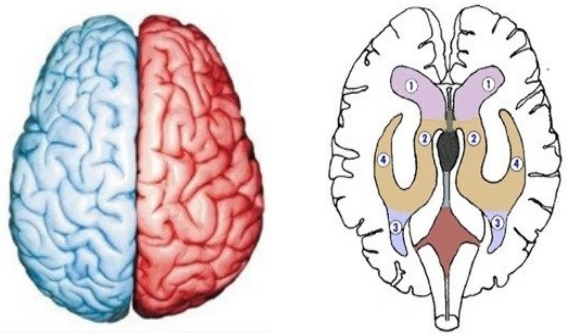
Уровень намагниченности водородного кластера пропорционален количеству протонов в единице объема ткани. Это позволяет вводить в рассмотрение обобщенный показатель кластера V, мм^3. Принимая во внимание, что количество протонов в биологической ткани велико, реализуется фиксация индуцированного радиоизлучения на катушке РЧ2, которое техническими средствами преобразуется в электрический сигнал, а средствами компьютерной графики в изображение – фрейм.

Одним из типичных объектов исследования средствами МРТ являются головной мозг. Детализируя структуру головного мозга, можно выделить функциональные нейронные образования (рисунок 2) и парные элементы желудочков (рога), где 1 – передний рог бокового желудочка; 2 – центральный отдел; 3 – задний рог бокового желудочка; 4 – боковой рог (рисунок 3). При выделении отдельных нейронных структур, обладающих известными анатомическими названиями, исследователь активно пользуется развитым интерфейсом компьютерной графики. Выбирая область интереса, исследователь указывает цветовой уровень, по которому интерфейс формирует периметр, а все дальнейшие процедуры исполняет аналитический блок компьютера. Метод ядерномагнитной томографии реализует возможность зафиксировать объемные показатели нейронных структур, выделенных исследователем в интерактивном режиме при работе с компьютерной программой формирования фрейма. На начальном этапе исследования создается полный фрейм СГМ (см. рисунок 2а). Затем оператор-исследователь самостоятельно устанавливает на фрейме область интереса, например, как указано на рисунке 2б, для которой программный вычислительный модуль компьютера проводит расчет объема нейронной структуры [2, 7].



а) б)

Рис. 2. Фрейм структур головного мозга: а) левая и правая гемисферы; б) левый и правый желудочки



а) б)

Рис. 3. Элементы структуры головного мозга: а) левая и правая гемисфера; б) желудочки

Понятие о финишном результате действий исследователя создается на основе представлений о единичном элементе графического изображения – вокселе. Это понятие формируется на определении поверхности [8] Гаусса, охватывающей установленную область пространства. Иначе говоря, оперируя понятием воксель, следует использовать методологию анализа изображений исключительно трехмерной графики. Для МРТ это представление полностью соответствует концепции подсчета протонов в единице объема биологической ткани.

Рассмотрим общий принцип формирования оценки пространственной структуры. В рамках принятых понятий поверхность *S* в окрестности точки *O* обладает критериями гладкости [8]. Полагаем, что через точку *O* проведена нормаль *n* к поверхности и касательная плоскость *P*. Проведем геометрические построения (рисунок 4).

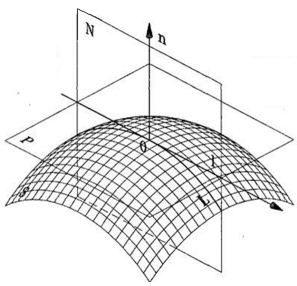


Рис. 4. Схема формирования пространственных координат

Проведем через нормаль *n* плоскость *N*, перпендикулярную к плоскости *P*, являющейся касательной к поверхности *S*. В таком построении плоскость *N* соприкасается с поверхностью *S* по кривой *L* и с касательной плоскостью по прямой *l*. Осуществим вращение плоскости *N* вокруг нормали *n*. В таком случае каждому положению плоскости *N* на поверхности *S* и на плоскости *P* будет соответствовать кривая *L* и прямая *l*. Многократное вращение создаст семейство кривых *L*. Данные кривые точно также, как и поверхность S, обладают определенными критериями гладкости, что характеризуется наличием не равных нулю радиусов кривизны *R* в точке *O*.

Сделанные построения позволяют констатировать, что при вращении плоскости *N* относительно нормали *n*, центры кривизны кривых *L* перемещаются и способны переходить с одной стороны плоскости *P* на другую. В этом случае происходит смена знака радиусов кривизны *L*, например, с плюса на минус. Это замечание чрезвычайно полезно при отслеживании динамики событий, воспроизводимых в виде трека на плоскости.

Развивая эти представления, можно сделать вывод о том, что полученные кривые в касательной плоскости *P* для любых гладких поверхностей порождают фигуры трех видов, в самом общем представлении соотносимых с эллипсом, гиперболой или парой параллельных прямых [6], которые называются индикатрисами (рисунок 5).

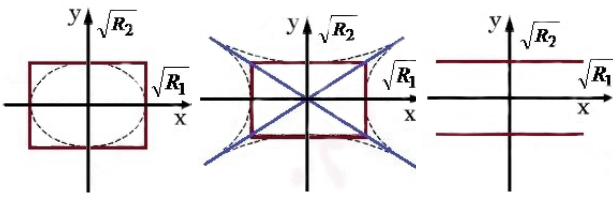


Рис. 5. Виды индикатрис поверхностей

Принимая во внимание, что рассматриваемые кривые описываются уравнениями второго порядка и имеют по две ортогональные оси симметрии, радиусы кривизны поверхностей по этим направлениям определяются как главные радиусы R_1 и R_2, иначе – параметры кривизны поверхности.

Для поверхностей в виде эллипса, где R_1 и R_2 имеют одинаковый знак, констатируем наличие положительной кривизны по Гауссу ($\Gamma > 0$). Для поверхностей в виде четырех ветвей гиперболы радиусы кривизны обладают разными знаками, что соответствует определению отрицательной кривизны по Гауссу ($\Gamma < 0$). Аналогичные суждения для поверхностей в виде двух параллельных прямых выявляют параметр $R = \infty$, а, следовательно, наличие нулевой кривизны $\Gamma = 0$.

Представленные суждения, хорошо известные в топологическом анализе поверхностей, позволяют их распространить на все множество гладких поверхностей, в том числе и таких, которые не обладают формальным описанием. Так, все множество гладких поверхностей, подвергающихся исследованию методом МРТ, могут адекватно замещаться одной из трех кривых (фигур) с положительной, отрицательной и нулевой гауссовой кривизной.

Акцентируя внимание на трех геометрических фигурах, отмечаем возможность выделения общего ключевого понятия, позиционируемого в образе окружности. Следуя теоретическим построениям Гаусса [6, 9], отмечаем безупречность логики выбора этого образа, а впоследствии и критерия кривизны поверхности. Окружность, как ключевой образ поверхности, можно трансформировать в пространственный образ – сферу [10]. Взаимосвязь геометрии многих пространственных фигур со сферой очевидна и представляет особый интерес в задачах моделирования. Вычислительная геометрия, оперируя понятиями одних топологических структур, определяет в модели подобие с другими структурами, используя базовый образ окружности – сферы.

Введем в рассмотрение додекаэдр как один из пяти возможных правильных многогранников, который состоит из двенадцати правильных пятиугольников, являющихся его гранями. Полагаем, что при определенных размерах граней додекаэдра, правильный пятиугольник на поверхности сферы обладает равными в 120° углами. Сформировав три пятиугольника, обнаружим хорошее, без зазоров, «замощение» поверхности. Продолжая эту процедуру, обнаружим, что такие двенадцать правильных пятиугольников полностью покрывают поверхность сферы [9, 10].

Исследование СГМ методом МРТ позволяет избирательно зафиксировать пространственный объем фрагментов, соотносимых с определенными анатомическими образованиями головного мозга. В рамках общности введенных понятий и определений, будем рассматривать СГМ как образ сферы, для которого внутреннее пространство отождествляется со структурой додекаэдра [11]. Введенные в рассмотрение понятия положены в основу модели вычисления оценки развертки событий намагниченности протонных кластеров на заданном интервале наблюдения. В качестве массива данных рассматривается набор фреймов СГМ, сформированный посредством магниторезонансного томографа, для двух групп: «норма» и «патология». Группа «патология» – это детский церебральный паралич (ДЦП).

Используя магниторезонансный томограф, компьютерный блок управления исследовательской процедурой, по установленной группе фреймов фиксируется набор показателей для детской возрастной группы от 3 месяцев до 1 года (таблица 1).

ТАБЛИЦА 1. Средние значения объема мозговых структур у детей с ДЦП (n = 20) и детей группы сравнения (n = 7) [11]

№ п/п	Анатомическая структура	Объем структуры, мм³		№ п/п	Анатомическая структура	Объем структуры, мм³	
		Группа «патология»	Группа «норма»			Группа «патология»	Группа «норма»
1.	Белое вещество, правая гемисфера	126901,15	164719,1	3.	Белое вещество, левая гемисфера	123735,748	162564,9
2.	Правый боковой желудочек	8009,2	4704,8	4.	Левый боковой желудочек	9434,5	3604,9

Примем в качестве основы средние значения объема СГМ (см. таблицу 1) и проведем вычисление показателей додекаэдра:

$$V = \frac{a^3}{4}\left(15 + 7\sqrt{5}\right) \approx 7{,}66a^3, \quad (4)$$

$$a = \sqrt[3]{\frac{V}{7{,}66}}, \quad (5)$$

$$S = 3a^2\sqrt{5(5 + 2\sqrt{5})} \approx 20{,}65a^2, \quad (6)$$

где V – объем додекаэдра; a – размер ребра; S – площадь поверхности.

Наличие исходных данных обследования позволяет сформировать пару показателей:

$$e = a;\ b = \frac{V}{S}. \quad (7)$$

Представленные показатели используем для создания модели развертки событий в выделенной анатомической структуре, характеризующейся намагниченностью протонных кластеров.

Принимая общую теоретическую линию формирования образа поверхности СГМ, проведем построение модели развертки событий по уравнению эллипса:

$$\begin{aligned} x(t) &= e\cos(t) \\ y(t) &= b\sin(t)' \end{aligned} \quad (8)$$

Отметим, что выбор функционала модели сделан в соответствии с общим тезисом Гаусса по топологии поверхности. Используя данные таблицы 1, вычислим значение ребра додекаэдра a, а затем проведем расчеты параметров e и b. По смыслу данные параметры характеризуют оси эллипса, задающие развертку событий, реализуемых в модели на интервале 2π. Проведем построение серии образов СГМ (рисунок 6), где оси абсцисс соответствует показатель деформации воксель (мм), а оси ординат – показатель деформации поверхности (мм). Формально, проведенные построения позволяют оценить «степень различия» нормальных нейронных структур от патологических структур. Такое сравнение проведем по выражению (9), где x_1 – текущее значение показателя деформации вокселя («норма»); y_1 – текущее значение показателя деформации поверхности («норма»); e_1 – текущее значение показателя деформации вокселя («патология»); h_1 – текущее значение показателя деформации поверхности («патология»).

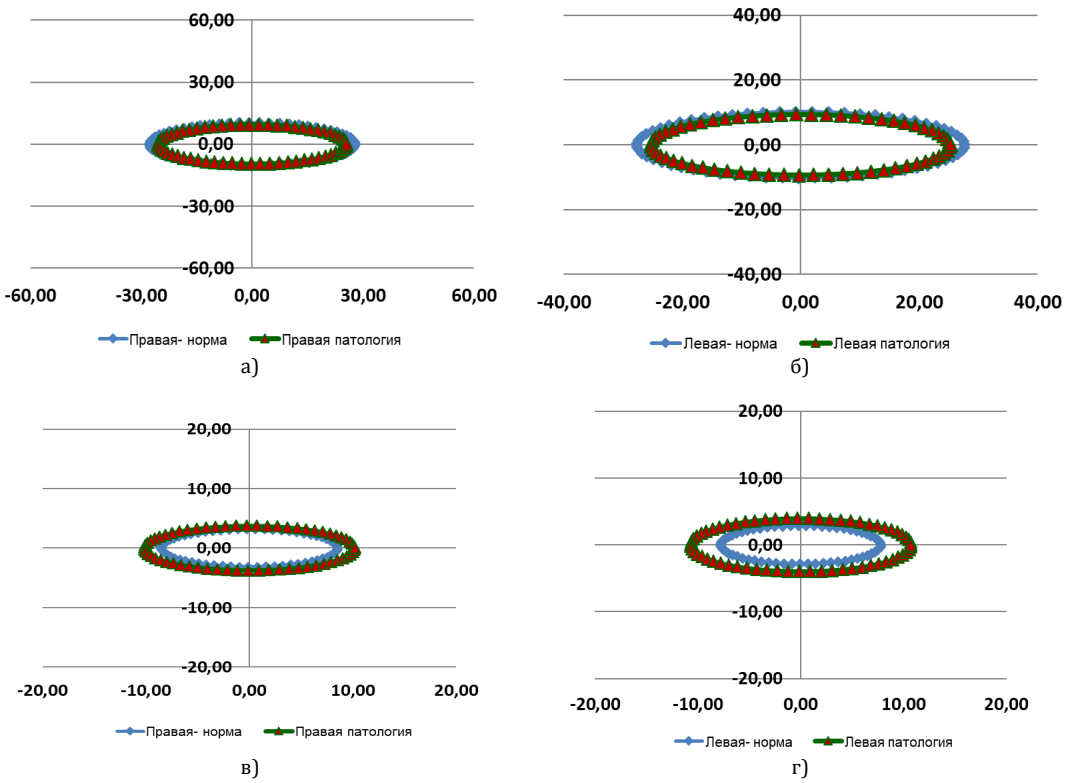


Рис. 6. Треки событий правой (а) и левой (б) гемисфер, правого (в) и левого (г) боковых желудочков в модели по функционалу эллипса

$$\Lambda = \sqrt{(x_1 - e_1)^2 + (y_1 - h_1)^2 + \ldots + (x_{1n} - e_{1n})^2 + (y_{1n} - h_{1n})^2}. \qquad (9)$$

Сформируем массивы для группы «норма»: $P(t) = [x_i, y_i)$, и для группы «патология»: $Q(t) = [e_i, h_i)$. Проведем сопоставление массивов, а результаты представим в таблице 2. Укажем область существования оценки $[0, \infty)$. Очевидно, что при полном совпадении образов исследуемых СГМ оценка различия составляет $\Delta = 0$.

ТАБЛИЦА 2. Расчетные значения различия нейронных СГМ

Трек событий		Оценка различия «Норма – Патология»
Гемисферы	правой	14,067
	левой	14,626
Желудочка	правого	10,019
	левого	17,865

Полученные оценки указывают на подобие – сопоставимость треков событий, инициализируемых в модели по функционалу эллипса. Относительно небольшие различия – отклонения патологических нейронных структур от «нормы» наблюдаются для гемисфер. Эти части головного мозга обладают большой массой и имеют много функциональных элементов. Для структур желудочкового комплекса отмечаем хорошо различимые и значимые различия. Здесь различие проявляется в несколько единиц.

Выявленные расчетные показатели отличия нейронных структур естественно связаны с топологией пространственной организации нейронной сети. Следуя этим представлениям, можно указать на то, что зрительные образы, воспроизведенные в модели по функционалу эллипса, создают приближенные понятия, которые требуется уточнить.

Принимая это во внимание, рассмотрим функционал модели на основе эпициклоиды, представленной выражением:

$$X(t) = (R + r)\cos(t) - r\cos\left(\frac{R + r}{r}t\right),$$
$$Y(t) = (R + r)\sin(t) - r\sin\left(\frac{R + r}{r}t\right), \qquad (10)$$

где t – вариативный циклический параметр развертки событий по намагниченности протонных кластеров, реализуемый на интервале $[0, 2\pi)$.

Используем данные таблицы 1 и проведем построения образов развертки событий. Введем обозначения:

$$R = a_{и_r} = \frac{V}{S}. \qquad (11)$$

По аналогии с выражениями (8, 9) создадим массив значений для группы «норма»: $P(t) = [x_i, y_i)$, и

для группы «патология»: $Q(t) = [e_i, h_i)$. В этом случае показатель R характеризует уровень деформации вокселя, а показатель r – уровень деформации поверхности кластера, обладающего установленным объемом.

Очевидно, созданные массивы обладают различиями, которые целесообразно представить в графическом виде. Этот прием хорошо известен в медицинской практике и является необходимым составляющим элементом построения финишного суждения. Однако, для множества практических задач диагностики этого недостаточно. Требуется указать численный показатель различия группы «норма» от группы «патология».

Вычисление показателя Ω проведем по аналогичному выражению (9). При этом полагаем, что $(x_i, y_j) \in P$; $(e_i, h_j) \in Q$.

Следуя установленным принципам получения итоговых оценок, проведем вычисление и построение образов событий, моделируемых по функционалу эпициклоиды. Очевидно, выбранный функционал модели содержит два переменных параметра X и Y, являющихся важным атрибутом понятия кривизны поверхности, которая позиционируется поверхностью СГМ. Проведем построение образов.

Первый образ СГМ (белое вещество, правая гемисфера) представлен на рисунке 7а. Отметим, что данная структура головного мозга представлена симметричными анатомическими фрагментами. Именно поэтому проводится сравнение сначала по правым фрагментам, а затем – по левым фрагментам головного мозга. Визуальный анализ пары образов указывает на более высокую интенсивность процессов модификации нейронной структуры в позиции «норма», чем в позиции «патология». Используя выражение (9), получим расчетное значение различия $\Omega_{\text{пр._гемисфера}} = 26{,}638$ по линии периметра образа. В терминах биофизики можно предложить суждение, указывающее на более интенсивное развитие нейронной структуры для «нормы», чем в случае «патологии».

Второй образ СГМ (белое вещество, левая гемисфера) представлен на рисунке 7б. Здесь уместны аналогичные пояснения, а расчетный показатель равен $\Omega_{\text{лв._гемисфера}} = 27{,}696$. Объединяя полученные пояснения, следует признать наличие подобия в образах «патология» правого и левого фрагмента гемисфер. Такое суждение справедливо, поскольку обнаруживаем незначительное различие в оценках:

$$\Omega_{\text{пр.гемисфера}} \approx \Omega_{\text{лв.гемисфера}}. \qquad (12)$$

Третий образ (правый боковой желудочек) представлен на рисунке 7в. Это также парный анатомический фрагмент СГМ. Осуществим сопоставление двух «нормальных» и двух «патологических» фрагментов, с использованием данных таблицы 1. Парное сопоставление фрагментов убедительно демонстрирует наличие существенных различий в структурах, которые представляется возможным оценить не только субъективно, по зрительному образу, но и количественно, по показателю $\Omega_{\text{пр._бокЖел.}} = 18{,}973$.

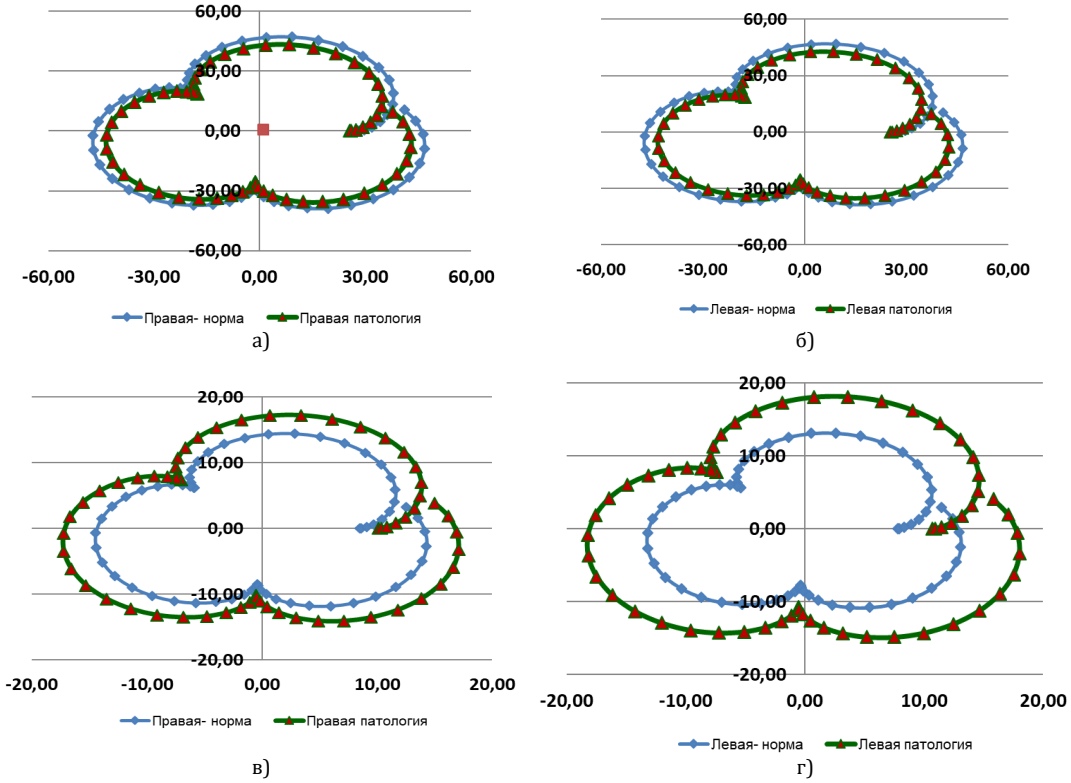


Рис. 7. Треки событий правой (а) и левой (б) гемисфер, правого (в) и левого (г) боковых желудочков в модели по функционалу эпициклоиды

Аналогичные построения и расчет для левого бокового желудочка указывают на несколько большее значение показателя $\Omega_{лв.\_бокЖел.} = 33{,}831$ (рисунок 7г). В данном случае отчетливо наблюдается преобладание патологических процессов. Это суждение создается на основе большей разницы в показателях:

$$\Omega_{пр.\_бокЖел.} \leq \Omega_{лв.\_бок.Жел.} \quad (13)$$

В методологии метода вычислений морфометрических оценок фрагментов головного мозга, в качестве базовых постулатов приняты физические принципы формирования фреймов МРТ, анализ которых осуществлен средствами вычислительной геометрии.

Аксиомы вычислительной геометрии традиционно оперируют понятиями сходства и подобия. Реализуя эти определения на топологических СГМ средствами компьютерного анализа, вычисляются количественные оценки функциональной развитости нейронных СГМ. Функциональная развитость нейронной структуры рассматривается с точки зрения подобия аналогичной структуры, обладающей статусом «нормы» или «патологии». В методологическом отношении такая трактовка результатов создается на хорошо известном базисе обширных натурных исследований, исполненных на разных материальных объектах в области классической физики – медицинской биофизики.

Внедрение в такие исследования компьютерных технологий, обладающих возможностью конструировать графические образы, способствует приобретению новых знаний об особенностях функционирования СГМ. Так, например, наличие возможности укрепить суждение о «норме» нейронного кластера избранного анатомического отдела можно на основании анализа данных модели. Действительно, рассматривая имеющиеся наборы данных клинических исследований (таблица 1), представляется возможным в модели воспроизвести обобщенный показатель μ исследуемой нейронной структуры. Апеллируя понятиями кривизны поверхности, по определению Гаусса, можно сказать, что вычисляемое значение μ характеризует динамику изменения кривизны поверхности. Чем большее значение μ будет получено в расчетах, тем выше «изрезанность поверхности вершинами и провалами». С учетом выражения (10) вычисление показателя μ проведем по выражению:

$$\mu = \sqrt{\sum_i (R_i - r_i)^2}. \quad (14)$$

В качестве иллюстративного примера рассмотрим «нормальную» структуру гемисферы и «нормальную» структуру правого бокового желудочка. Очевидно, что при условии одного и того же организма биохимические и биофизические свойства нейронных структур в указанных кластерах будут примерно одинаковыми, поскольку дипольные моменты водородных ядер мало отличаются. Принимая это во внимание, а также расчеты для структур в категории «патология», представим результат вычислений в таблице 3.

ТАБЛИЦА 3. Данные расчета показателя μ («норма» / «патология»)

Анатомическая структура		Показатель μ	Различие в парной структуре, %
Гемисфера	Правая	323,517 / 295,723	0,88 / 0,84
	Левая	320,662 / 293,251	
Боковой желудочек	Правый	98,451 / 117,628	8,49 / 5,51
	Левый	90,089 / 124,151	

Полученные результаты убедительны и, можно сказать, полностью соответствует позитивному тезису о схожести по биофизическому критерию элементарных нейронных СГМ. Другими словами, отклонение по симметричности в парных отделах головного мозга по показателю μ – естественное явление. Различия по массе и размерам поверхности выбранных для исследования анатомических фрагментов также хорошо известны и имеют строгое объяснение.

Но обнаруженное малое различие по показателю μ для гемисферы свидетельствует о высокой степени подобия топологий нейронных сетей. Наличие такого результата позволяет создать процедуру оценки состояния нейронной ткани не только по методике сравнительного анализа однотипных СГМ, принадлежащих разным организмам, но и на одном избранном организме. Фактически устанавливая приоритет некоторого нейронного кластера и соотнося полученные значения на фрейме с «нормой», представляется возможным обнаружить «фрагменты патологии», а также организовать мониторинг «участков патологии». Такая целевая постановка задачи исследования значительно повышает достоверность результатов.

В числе наиболее значимых нарушений нейронных СГМ находятся: энцефалопатия, ДЦП, инсульт, болезнь Паркинсона и болезнь Альцгеймера, распространенность последней ежегодно стремительно увеличивается. Это заболевание обладает нечеткой этиологией и характеризуется выраженным нарушением когнитивных функций, фактически на фоне абсолютно полно осознания окружающих событий. Для этого заболевания результаты исследования СГМ методом МРТ показывают выраженную атрофию коры больших полушарий (гемисфер) с расширением борозд и увеличением желудочков [1, 12].

Так, по результатам представленного анализа для правого и левого желудочков значение $\mu_{патология}$ меньше $\mu_{норма}$. Такое соотношение показателей возможно в случае «спрямления – выравнивания»

складчатой поверхности нейронной структуры, относимой к анатомическому образованию желудочков СГМ. Показатель «спрямления» поверхности, который соотносим с геометрией объема, действительно свидетельствует об увеличении размеров желудочков. В дополнении к этому следует указать, что представленные здесь атрибуты заболевания достаточно просто сочетаются с медицинской терминологией вывода суждений. Эта особенность представленной модели позволяет организовать диагностический процесс на основе МРТ-фреймов с высоким уровнем доверия.

Актуальность изучения функциональных проявлений деятельности нейронных СГМ продиктована наличием многочисленных нарушений, с относительно малой этиологией.

Следуя этим представлениям, которые актуализируют проблематику анализа результатов исследования фреймов ядерного магнитного томографа, средствами компьютерных технологий, в вышеизложенном материале рассмотрен традиционный метод выделения патологических участков СГМ, который развит и дополнен серией вычислительных процедур, позволяющих определять количественные оценки различия нейронных структур. Именно такой процесс обеспечивает возможность осуществления постоянного мониторинга практически любого нарушения СГМ с реальными показателями динамики смены состояний нейронного кластера. Такие показатели оказываются чрезвычайно полезными как в задачах этимологического характера, так и в формировании прогноза развития событий для установленного анатомического фрагмента нейронной СГМ.

Акцентируя внимание на компьютерных технологиях, следует указать на возможность организации телекоммуникационного медицинского сервиса. Действительно, широкое распространение ЯМР исследований СГМ в медицинской практике и сети Интернет позволяет оперативно проводить удаленный анализ фреймов, создавать электронные библиотеки, осуществлять системный мониторинг нарушений СГМ. Платформа облачных вычислений, должным образом представленная набором интерактивных процедур анализа фреймов, может рассматриваться как логическое продолжение проекта построения массового телекоммуникационного сервиса в области анализа результатов номографического исследования.

Полученные результаты исследования создают благоприятные предпосылки формирования диагностических заключений о состоянии СГМ на основе компьютерного анализа томограмм. Использование компьютерных технологий анализа данных открывает широкие возможности количественного описания развития СГМ как в норме, так и при различных видах патологии. Применение предложенных в статье информационных компьютерных технологий оценки нарушений СГМ способствует отбору наиболее перспективных терапевтических процедур, учитывающих индивидуальные особенности организма.

Список используемых источников

1. Румболдт З., Кастильо М., Хуанг Б., Росси А. КТ- и МРТ-визуализация головного мозга. Подход на основе изображений. М.: МЕДпресс-информ, 2016. 428 с.

2. Макаров Л.М., Поздняков А.В., Мелашенко Т.В., Александров Т.А., Тащилкин А.И. МРТ головного мозга в онтогенезе плода новорожденного – диагностическая основа модели диссипативных систем // International Scientific Review. 2017. № 4(35). С. 85–91.

3. Головинский П.А. Математические модели. Теоретическая физика и анализ сложных систем. От формализма классической механики до квантовой интерференции. М.: Либроком, Editorial URSS, 2016. 370 с.

4. Мартинсон Л., Смирнов Е. Квантовая физика. М.: Изд-во МГТУ им. Н.Э. Баумана, 2012. 526 с.

5. Ландау Л.Д., Лифшиц Е.М. Теоретическая физика в 10 томах. Том 3. Квантовая механика (нерелятивистская теория). М.: Физматлит, 2008.

6. Гаусс К.Ф. Труды по теории чисел. М.: Издательство «Книга по Требованию», 2012. 979 с.

7. Львов В.С., Поздняков А.В., Иванов Д.О., Тащилкин А.И., Макаров Л.М., Позднякова О.Ф. и др. О возможности МР-морфометрии и диффузионно-тензорной МРТ в диагностике двусторонних спастических форм детского церебрального паралича // Педиатр. 2019. Т. 10. № 1. С. 29–36. DOI:10.17816/PED10129-36

8. Борисович Ю.Г., Близняков Н.М., Израилевич Я.А., Фоменко Т.Н. Введение в топологию. М.: Ленард, 2015. 448 с.

9. Пуанкаре А. Избранные труды. Том 2. М.: Наука, 1972. 358 с.

10. Арсенов О. Григорий Перельман и гипотеза Пуанкаре. М.: Эксмо, 2010.

11. Макаров Л.М., Поздняков А.В. МРТ диагностика и компьютерный анализ // Proceedings of the LVIII international Scientific and practical conference “International scientific review of the problems and prospects of modern science and education” (Boston, USA, 22–23 May 2019). 2019. С. 98–105. DOI:10.24411/2542-0798-2019-15802

12. Труфанов Г.Е, Рамешвили Т.Е. Лучевая диагностика опухолей головного мозга. Атлас КТ- и МРТ-изображений. СПб.: ЭЛБИ-СПб, 2007. 326 с.

* * *

MATHEMATICAL MODELLING AND NUMERICAL METHODS OF THE ANALYSIS OF NEURAL STRUCTURES

L. Makarov[1], A. Pozdnyakov[2, 3, 4], S. Protasenya[1], D. Ivanov[2], V. Lvov[2], S. Lvov[2]

[1]The Bonch-Bruevich Saint-Petersburg State University of Telecommunications,
St. Petersburg, 193232, Russian Federation
[2]Saint-Petersburg State Pediatric Medical University,
St. Petersburg, 194100, Russian Federation
[3]North-Western State Medical University named after I.I. Mechnikov,
St. Petersburg, 191015, Russian Federation
[4]Russian Research Center for Radiology and Surgical Technologies,
St. Petersburg, 197758, Russian Federation

Article info
The article was received 26 June 2019

For citation: Makarov L., Pozdnyakov A., Protasenya S., Ivanov D., Lvov V., Lvov S. Mathematical Modeling and Numerical Methods of the Analysis of Neural Structures. *Proceedings of Telecommunication Universities*. 2019;5(3): 98–107. (in Russ.) Available from: https://doi.org/10.31854/1813-324X-2019-5-3-98-107

Abstract: *In this article we can observe a mathematical model of the topological description of neural structure of human brain, which describes the results of numerical analysis process of a magnetic resonance tomography. The created model provides a possibility to organize a cloud computing environment, which achieves the synthesis of quantitative indicators of distinctions in analyzed fragments of neural tissue, it is created by means of the telecommunication service which is promoting the involvement of a large number of experts in to a research process, to create a set of a priori judgments of evolution of the registered processes.*

Keywords: *mathematical model, cloud computing, computer analysis, neural structure.*

References

1. Rumboldt Z., Kastilo M., KHuang B., Rossi A. *KT- i MRT-vizualizatsiia golovnogo mozga. Podkhod na osnove izobrazhenii* [Brain Imaging with MRI and CT: An Image Pattern Approach]. Moscow: MEDpress-inform Publ.; 2016. 428 p. (in Russ.)
2. Makarov L.M., Pozdnyakov A.V., Melashenko T.V., Alexandrov T.A., Tashchilkin A.I. MRI of Brain in the Ontogenesis of the Newborn – the Diagnostic Basic of the Model of Dissipative Sustems. *International Scientific Review*. 2017;4(35):85–91. (in Russ.)
3. Golovinskii P.A. Matematicheskie modeli. *Teoreticheskaia fizika i analiz slozhnykh system. Ot formalizma klassicheskoi mekhaniki do kvantovoi interferentsii* [Mathematical Models. Theoretical Physics and Analysis of Complex systems. From the Formalism of Classical Mechanics to Quantum Interference]. Moscow: Librokom Publ., Editorial URSS Publ.; 2016. 370 p. (in Russ.)
4. Martinson L., Smirnov E. *Kvantovaia fizika* [Quantum Physics]. Moscow: Bauman Moscow State Technical University Publ.; 2012. 526 p. (in Russ.)
5. Landau L.D., Lifshits E.M. *Teoreticheskaia fizika v 10 tomakh. Tom 3. Kvantovaia mekhanika (nereliativistskaia teoriia)* [Theoretical Physics in 10 Volumes. Volume 3. Quantum Mechanics: Nonrelativistic Theory]. Moscow: Fizmatlit Publ.; 2008. (in Russ.)
6. Gauss K.F. *Trudy po teorii chisel* [Proceedings in Number Theory]. Moscow: Kniga po Trebovaniiu Publ.; 2012. 979 p. (in Russ.)
7. Lvov V.S., Pozdnyakov A.V., Ivanov D.O., Tashilkin A.I., Makarov L.M., Pozdnyakova O.F., et al. Capabilities of voxel based morphometry and diffusion tensor imaging in diagnostics of bilateral spastic forms of cerebral palsy. *Pediatrician*. 2019;10(1):29–36. (in Russ.) Available from: https://doi.org/10.17816/PED10129-36
8. Borisovich Iu.G., Blizniakov N.M., Izrailevich Ia.A., Fomenko T.N. *Vvedenie v topologiiu* [Topology Introduction]. Moscow: Lenard Publ.; 2015. 448 p. (in Russ.)
9. Puankare A. *Izbrannye Trudy. Tom 2* [Selected Works. Vol. 2]. Moscow: Nauka Publ.; 1972. 358 p. (in Russ.)
10. Arsenov O. *Grigorii Perelman i gipoteza Puankare* [Grigorii Perelman and the Poincare Conjecture]. Moscow: Eksmo Publ.; 2010. (in Russ.)
11. Makarov L.M., Pozdnyakov A.V. MRT Diagnostics and Computer Analysis. *Proceedings of the LVIII International Scientific and Practical Conference "International Scientific Review of the Problems and Prospects of Modern Science and Education", 22–23 May 2019, Boston, USA*. 2019. p.98–105. (in Russ.) Available from: https://doi.org/10.24411/2542-0798-2019-15802
12. Trufanov G.E., Rameshvili T.E. *Luchevaia diagnostika opukholei golovnogo mozga. Atlas KT- i MRT-izobrazhenii* [Radiation Diagnosis of Brain Tumors. Atlas of CT and MRI Images]. St. Petersburg: SPb ELBI-SPb; 2007. 326 p. (in Russ.)

СВЕДЕНИЯ ОБ АВТОРАХ

БРАНИЦКИЙ Александр Александрович кандидат технических наук, старший научный сотрудник Санкт-Петербургского института информатики и автоматизации Российской академии наук (СПИИРАН), alexander.branitskiy@gmail.com

БУРАНОВА Марина Анатольевна кандидат технических наук, доцент, доцент кафедры информационной безопасности Поволжского государственного университета телекоммуникаций и информатики, buranova-ma@psuti.ru

ВОРОНИН Сергей Владимирович кандидат технических наук, доцент, доцент кафедры Пожарной безопасности технологических процессов и производств Санкт-Петербургского университета ГПС МЧС России, wsw1@yandex.ru

ДВОРНИКОВ Сергей Викторович доктор технических наук, профессор, профессор кафедры радиосвязи Военной академии связи им. Маршала Советского Союза С.М. Буденного, practicdsv@yandex.ru

ДОРОШЕНКО Виктор Иванович доктор технических наук, профессор, профессор кафедры Радиосвязи на морском флоте Государственного университета морского и речного флота имени адмирала С.О. Макарова, doroshenko1937@yandex.ru

ЕГОРОВ Александр Тимофеевич начальник отдела систем радиосвязи АО «Кронштадт», Aleksander.Egorov@kronshtadt.ru

ИВАНОВ Дмитрий Олегович доктор медицинских наук, профессор, ректор Санкт-Петербургского государственного педиатрического медицинского университета, radiolodgy@mail.ru

КИРИЧЕК Руслан Валентинович доктор технических наук, доцент, доцент кафедры сетей связи и передачи данных Санкт-Петербургского государственного университета телекоммуникаций им. проф. М.А. Бонч-Бруевича, kirichek.sut@mail.ru

КОРЖИК Валерий Иванович доктор технических наук, профессор, профессор кафедры защищенных систем связи Санкт-Петербургского государственного университета телекоммуникаций им. проф. М.А. Бонч-Бруевича, val-korzhik@yandex.ru

КРАСОВ Андрей Владимирович кандидат технических наук, доцент, заведующий кафедрой защищенных систем связи Санкт-Петербургского государственного университета телекоммуникаций им. проф. М.А. Бонч-Бруевича, krasov@inbox.ru

КСЕНОФОНТОВ Юрий Геннадьевич кандидат технических наук, доцент кафедры Радиосвязи на морском флоте Государственного университета морского и речного флота имени адмирала С.О. Макарова, ksenofontov.ura@mail.ru

КУЛИК Вячеслав Андреевич ассистент кафедры сетей связи и передачи данных Санкт-Петербургского государственного университета телекоммуникаций им. проф. М.А. Бонч-Бруевича, vslav.kulik@gmail.com

КУЧЕРЯВЫЙ Андрей Евгеньевич доктор технических наук, профессор, профессор кафедры сетей связи и передачи данных Санкт-Петербургского государственного университета телекоммуникаций им. проф. М.А. Бонч-Бруевича, akouch@mail.ru

ЛАТЫПОВ Руслан Танисович аспирант кафедры информационной безопасности Поволжского государственного университета телекоммуникаций и информатики, msibs@psuti.ru

ЛОМАКИН Андрей Александрович кандидат технических наук, старший научный сотрудник, ведущий научный сотрудник АО «Кронштадт», Andrei.Lomakin2@kronshtadt.ru

ЛЬВОВ Виктор Сергеевич аспирант кафедры медицинской биофизики Санкт-Петербургского государственного педиатрического медицинского университета, viktorlvov@list.ru

ЛЬВОВ Сергей Николаевич кандидат медицинских наук, профессор, декан лечебного факультета Санкт-Петербургского государственного педиатрического медицинского университета, radiolodgy@mail.ru

МАКАРОВ Леонид Михайлович кандидат технических наук, профессор, профессор кафедры конструирования и производства радиоэлектронных средств Санкт-Петербургского государственного университета телекоммуникаций им. проф. М.А. Бонч-Бруевича, elfbio@gmail.com

МАХМУД Омар Абдулкарим аспирант кафедры сетей связи и передачи данных Санкт-Петербургского государственного университета телекоммуникаций им. проф. М.А. Бонч-Бруевича, mahmood_omar@list.ru

ПАНТЕНКОВ Дмитрий Геннадьевич кандидат технических наук, начальник отделения радиосвязного оборудования АО «Кронштадт», Dmitrii.Pantenkov@kronshtadt.ru

ПАРАМОНОВ Александр Иванович доктор технических наук, профессор кафедры сетей связи и передачи данных Санкт-Петербургского государственного университета телекоммуникаций им. проф. М.А. Бонч-Бруевича, alex-in-spb@yandex.ru

ПЕТРИВ Роман Богданович старший преподаватель кафедры защищенных систем связи Санкт-Петербургского государственного университета телекоммуникаций им. проф. М.А. Бонч-Бруевича, roman.petriv@mail.ru

ПОЗДНЯКОВ Александр Владимирович доктор медицинских наук, профессор, заведующий отделением лучевой диагностики, заведующий кафедрой медицинской биофизики, профессор кафедры лучевой диагностики и лучевой терапии Санкт-Петербургского государственного педиатрического медицинского университета, руководитель лаборатории нейровизуализации Российского научного центра радиологии и хирургических технологий им. акад. А.М. Гранова, pozdnyakovalex@yandex.ru

ПРОТАСЕНЯ Сергей Витальевич кандидат технических наук, доцент кафедры конструирования и производства радиоэлектронных средств Санкт-Петербургского государственного университета телекоммуникаций им. проф. М.А. Бонч-Бруевича, saitvodabur@yandex.ru

САЕНКО Игорь Борисович доктор технических наук, профессор, ведущий научный сотрудник Санкт-Петербургского института информатики и автоматизации Российской академии наук (СПИИРАН), ibsaen@comsec.spb.ru

САХАРОВ Дмитрий Владимирович кандидат технических наук, доцент кафедры защищенных систем связи Санкт-Петербургского государственного университета телекоммуникаций им. проф. М.А. Бонч-Бруевича, d.sakharov@rkn.gov.ru

СТОРОЖУК Николай Леонидович кандидат технических наук, доцент кафедры защищенных систем связи Санкт-Петербургского государственного университета телекоммуникаций им. проф. М.А. Бонч-Бруевича, snl@kometeh.ru

ТИАМИЙУ Осуолале Абдулрахамон PhD, старший преподаватель кафедры телекоммуникационной науки Университета Илорина (г. Илорин, Нигерия), ozutiams@yahoo.com

УШАКОВ Игорь Александрович старший преподаватель кафедры защищенных систем связи Санкт-Петербургского государственного университета телекоммуникаций им. проф. М.А. Бонч-Бруевича, ushakovia@gmail.com

ФЛАКСМАН Дмитрий Алексеевич аспирант кафедры защищенных систем связи Санкт-Петербургского государственного университета телекоммуникаций им. проф. М.А. Бонч-Бруевича, flxdima4951@gmail.com

РОССВЯЗЬ СПбГУТ)))

V Всероссийская научно-техническая конференция с международным участием
«Модернизация информационной инфраструктуры для сетей 5G/IMT 2020 и для других перспективных технологий в интересах цифровой трансформации регионов»

9 октября 2019

Цель конференции:

определение основных направлений модернизации информационной инфраструктуры для сетей связи 5G/IMT 2020 в условиях цифровой трансформации регионов.

На конференции планируется рассмотреть и обсудить следующие вопросы:

- состояние инфраструктуры беспроводных сетей связей и перспективы их развития в ходе цифровой трансформации регионов;
- концепция создания и развития сетей 5G/IMT 2020;
- концепция по построению узкополосных беспроводных сетей связи «Интернета вещей»;
- концепция и технические требования покрытия транспортной инфраструктуры сетями связи для систем передач данных;
- современные исследования и разработки в области сквозных технологий.

Место проведения конференции:

Санкт-Петербург, пр. Большевиков, д. 22/1.

Организационно-техническое обеспечение Конференции осуществляет СПбГУТ.

rosinfocom@spbgut.ru www.sut.ru/rosinfocom

ДЛЯ ЗАМЕТОК

Дизайн обложки – ООО «Комильфо»

План издания научной литературы 2019 г., п. 2

Подписано в печать	Усл.-печ. л.	Формат	Тираж	Заказ	Свободная цена
27.09.2019	14,0	$60\times84_{1/8}$	1000 экз.	№ 1030	

Отпечатано в СПбГУТ
193232, Санкт-Петербург, пр. Большевиков, 22/1

Учредитель и издатель:
Федеральное государственное бюджетное образовательное учреждение
высшего образования "Санкт-Петербургский государственный университет
телекоммуникаций им. проф. М.А. Бонч-Бруевича"
E-mail: tuzs@spbgut.ru Web: tuzs.sut.ru VK: vk.com/spbtuzs

ISSN: 1813-324X
Подписной индекс по каталогу "Издания органов НТИ" Агентства "Роспечать" – 59983