УНИВЕРСИТЕТ ИТМО

НАУЧНО-ТЕХНИЧЕСКИЙ ВЕСТНИК ИНФОРМАЦИОННЫХ ТЕХНОЛОГИЙ, МЕХАНИКИ И ОПТИКИ
июль–август 2022 Том 22 № 4 http://ntv.ifmo.ru/
SCIENTIFIC AND TECHNICAL JOURNAL OF INFORMATION TECHNOLOGIES, MECHANICS AND OPTICS
Jule–August 2022 Vol. 22 No 4 http://ntv.ifmo.ru/en/
ISSN 2226-1494 (print) ISSN 2500-0373 (online)

НАУЧНО-ТЕХНИЧЕСКИЙ ВЕСТНИК УНИВЕРСИТЕТ ИТМО
ИНФОРМАЦИОННЫХ ТЕХНОЛОГИЙ, МЕХАНИКИ И ОПТИКИ

doi: 10.17586/2226-1494-2022-22-4-699-707
УДК 004.72

Разработка модели обнаружения сетевых аномалий трафика в беспроводных распределенных самоорганизующихся сетях

Леонид Вячеславович Легашев[1]✉, Любовь Сергеевна Гришина[2], Денис Игоревич Парфенов[3], Артур Юрьевич Жигалов[4]

[1,2,3,4] Оренбургский государственный университет, Оренбург, 460018, Российская Федерация

[1] silentgir@gmail.com✉, https://orcid.org/0000-0001-6351-404X
[2] zabrodina97@inbox.ru, https://orcid.org/0000-0003-2752-7198
[3] parfenovdi@mail.ru, https://orcid.org/0000-0002-1146-1270
[4] leroy137.artur@gmail.com, https://orcid.org/0000-0003-3208-1629

Аннотация

Предмет исследования. Мобильные самоорганизующиеся сети — одно из перспективных направлений технологии граничных вычислений. Такие сети применяются в различных областях деятельности, в частности при разработке интеллектуальных транспортных систем. Особенность мобильных самоорганизующихся сетей заключается в постоянно изменяющейся их динамической топологии. В результате таких изменений необходимо использовать реактивные протоколы маршрутизации при передаче пакетов между узлами. Данные сети уязвимы к кибератакам, поэтому возникает необходимость разработки мер по идентификации сетевых угроз и разработке правил реагирования на них на основе моделей машинного обучения. Цель работы — разработка динамической модели обнаружения сетевых аномалий трафика в беспроводных распределенных самоорганизующихся сетях. **Метод.** Применены методы и алгоритмы интеллектуального анализа данных и машинного обучения. Предлагаемый подход к мониторингу трафика в беспроводных распределенных самоорганизующихся сетях состоит в реализации двух этапов: первоначального анализа трафика для выявления аномальных событий и последующего глубокого изучения инцидентов кибербезопасности для классификации типа атакующего воздействия. В рамках подхода построены модели на основе ансамблевых методов машинного обучения. Выполнен сравнительный анализ и выбор наиболее эффективных алгоритмов машинного обучения и их оптимальных гиперпараметров. **Основные результаты.** Проведена формализация модели обнаружения аномалий трафика в беспроводных распределенных самоорганизующихся сетях, и выделены основные количественные метрики производительности сети. Представлен обобщенный алгоритм обнаружения аномалий трафика в мобильных самоорганизующихся сетях. Выполнено экспериментальное исследование симуляции сегмента сети с позиции снижения производительности в условиях реализации различных сценариев возникновения сетевых атак. Показано, что сетевая распределенная атака вида «отказ в обслуживании» и кооперативная атака вида «Blackhole» оказывают наибольшее негативное влияние на производительность сегмента мобильной самоорганизующейся сети. Результаты моделирования сети применены для построения модели машинного обучения выявления аномалий и классификации типов атак. Результаты сравнительного анализа алгоритмов машинного обучения показали, что метод LightGBM наиболее эффективен для выявления аномалий сетевого трафика, при использовании которого доля правильных ответов составила 91 %. Тип проводимой атаки определен с долей правильных ответов 90 %. **Практическая значимость.** Предложенный подход к обнаружению сетевых аномалий за счет применения обученных моделей анализа трафика позволяет своевременно идентифицировать рассмотренные типы атак. Будущее направление развития данного исследования — рассмотрение новых сценариев возникновения сетевых атак и дополнительное онлайн-обучение построенных моделей идентификации. Разработанное программное средство обнаружения сетевых аномалий трафика в распределенных мобильных самоорганизующихся сетях может найти применение для любых типов беспроводных самоорганизующихся сетей.

Ключевые слова

мобильные самоорганизующиеся сети, метрики производительности, система обнаружения вторжений

Благодарности
Исследование выполнено при финансовой поддержке гранта Президента Российской Федерации для государственной поддержки молодых российских ученых — кандидатов наук (МК-2959.2021.1.6).

Ссылка для цитирования: Легашев Л.В., Гришина Л.С., Парфенов Д.И., Жигалов А.Ю. Разработка модели обнаружения сетевых аномалий трафика в беспроводных распределенных самоорганизующихся сетях // Научно-технический вестник информационных технологий, механики и оптики. 2022. Т. 22, № 4. С. 699–707. doi: 10.17586/2226-1494-2022-22-4-699-707

Development of a model for detecting network traffic anomalies in distributed wireless ad hoc networks

Leonid V. Legashev[1]✉, Lubov S. Grishina[2], Denis I. Parfenov[3], Arthur Yu. Zhigalov[4]

[1,2,3,4] Orenburg State University, Orenburg, 460018, Russian Federation

[1] silentgir@gmail.com✉, https://orcid.org/0000-0001-6351-404X
[2] zabrodina97@inbox.ru, https://orcid.org/0000-0003-2752-7198
[3] parfenovdi@mail.ru, https://orcid.org/0000-0002-1146-1270
[4] leroy137.artur@gmail.com, https://orcid.org/0000-0003-3208-1629

Abstract
Mobile ad hoc networks are one of the promising directions of the edge computing technology and they are used in various applications, in particular, in the development of intelligent transport systems. A feature of mobile ad hoc networks lies in the constantly changing dynamic network topology, as a result of which it is necessary to use reactive routing protocols when transmitting packets between nodes. Mobile ad hoc networks are vulnerable to cyber-attacks, so there is a need to develop measures to identify network threats and develop rules for responding to them based on machine learning models. The subject of this study is the development of a dynamic model for detecting network traffic anomalies in wireless distributed ad hoc networks. Within the framework of this study, methods and algorithms of data mining and machine learning were applied. The proposed approach to traffic monitoring in wireless distributed ad hoc networks consists in the implementation of two stages: initial traffic analysis to identify anomalous events and subsequent in-depth study of cybersecurity incidents to classify the type of attack. Within the framework of this approach, the corresponding models are constructed based on ensemble methods of machine learning. A comparative analysis and selection of the most efficient machine learning algorithms and their optimal hyperparameters has been carried out. In this paper, a formalization of the traffic anomaly detection model in distributed wireless ad hoc networks is carried out, the main quantitative metrics of network performance are identified, a generalized algorithm for detecting traffic anomalies in mobile ad hoc networks is presented, and an experimental study of the network segment simulation is carried out from the point of view of performance degradation during the implementation of various network attack scenarios. Network distributed denial of service attacks and cooperative blackhole attacks have the greatest negative impact on the performance of the mobile ad hoc network segment. In addition, the network simulation results were used to build a machine learning model to detect anomalies and classify types of attacks. The results of a comparative analysis of machine learning algorithms showed that the use of the LightGBM method is the most effective for detecting network traffic anomalies with an accuracy of 91 %, and for determining directly the type of attack being carried out with an accuracy of 90 %. The proposed approach for network anomalies detection through the use of trained traffic analysis models makes it possible to identify the considered types of attacks in due time. The future development direction of this research is the consideration of new scenarios for the emergence of network attacks and online additional training of the constructed identification models. The developed software tool for detecting network traffic anomalies in distributed mobile ad hoc networks can be used for any type of wireless ad hoc networks.

Keywords
mobile ad hoc networks, performance metrics, intrusion detection system

Acknowledgements
The research was funded by the grant from President of the Russian Federation for state support of young Russian scientists (MK-2959.2021.1.6).

For citation: Legashev L.V., Grishina L.S., Parfenov D.I., Zhigalov A.Yu. Development of a model for detecting network traffic anomalies in distributed wireless ad hoc networks. *Scientific and Technical Journal of Information Technologies, Mechanics and Optics*, 2022, vol. 22, no. 4, pp. 699–707 (in Russian). doi: 10.17586/2226-1494-2022-22-4-699-707

Введение

Особенность мобильных самоорганизующихся сетей (Mobile Ad-hoc Networks, MANETs) заключается в отсутствии заранее определенной сетевой инфраструктуры при передаче информации между двумя беспроводными устройствами. Каждый узел в мобильной беспроводной сети может служить как роутером, так и хостом, и осуществляет пересылку пакетов по запросу. Для MANET характерна динамическая топология, повышенная мобильность сетевых узлов, а также многопереходная маршрутизация, когда связность двух элементов обеспечивается пересылкой данных через промежуточные элементы сети. Наиболее популярные протоколы сетевой маршрутизации в MANET — семейства реактивных и проактивных протоколов: AODV (Ad hoc On-Demand Distance Vector), DSDV (Destination-Sequenced Distance-Vector), OLSR (Optimized Link State

Routing), DSR (Dynamic Source Routing) и др. Как правило, узлы в MANET представляют собой мобильные устройства с небольшими объемами дисковой и оперативной памяти и процессорной мощностью, при этом такие сетевые устройства могут выполнять определенную вычислительную нагрузку. В частности, бинарная классификация сетевых угроз может производиться на конечных узлах MANET при наличии заранее обученного классификатора. Развитие архитектуры программно-конфигурируемых сетей (ПКС) и технологии граничных вычислений (edge computing) позволяют оптимальным образом увеличить эффективность функционирования MANETs, сделать их более гибкими с точки зрения обнаружения сетевых угроз и выработки правил реагирования на них. На рис. 1 представлена общая схема функционирования сегмента MANET с поддержкой ПКС-контроллера.

Особенность анализа функционирования MANETs — необходимость фиксирования взаимосвязей объектов сети и их характеристик не только в некоторый момент времени, но и в соответствующем пространственном положении. Объекты сети, кроме обычных координат долготы и широты, имеют высоту расположения (например, придорожные устройства, такие как светофор, и антенны на автомобилях могут располагаться на разных высотах). В связи с этим расстояние между беспроводными роутерами такого типа необходимо рассчитывать с учетом высоты расположения. Зоны покрытия сигналов могут не перекрываться, и обеспечение стабильной связи между объектами нельзя гарантировать.

Реализация ПКС-контроллера в качестве элемента MANET отделяет плоскость данных (Data plane) от плоскости контроля (Control plane), позволяя проводить эффективный мониторинг сетевых потоков трафика практически в режиме реального времени, собирая статистические данные потоков и осуществляя маршрутизацию пакетов по всей сети. Коммутаторы с поддержкой OpenFlow осуществляют поиск по таблицам коммутации и обновляют информацию, если правило пересылки пакета не найдено. При возникновении сетевой угрозы ПКС-контроллер формирует сообщение с политикой реагирования (как правило, происходит изоляция злонамеренного узла и удаление его из всех таблиц коммутации) и рассылает его коммутаторам OpenFlow. Базовые станции используются для покрытия групп мобильных устройств. На каждой базовой станции работает механизм обнаружения сер-

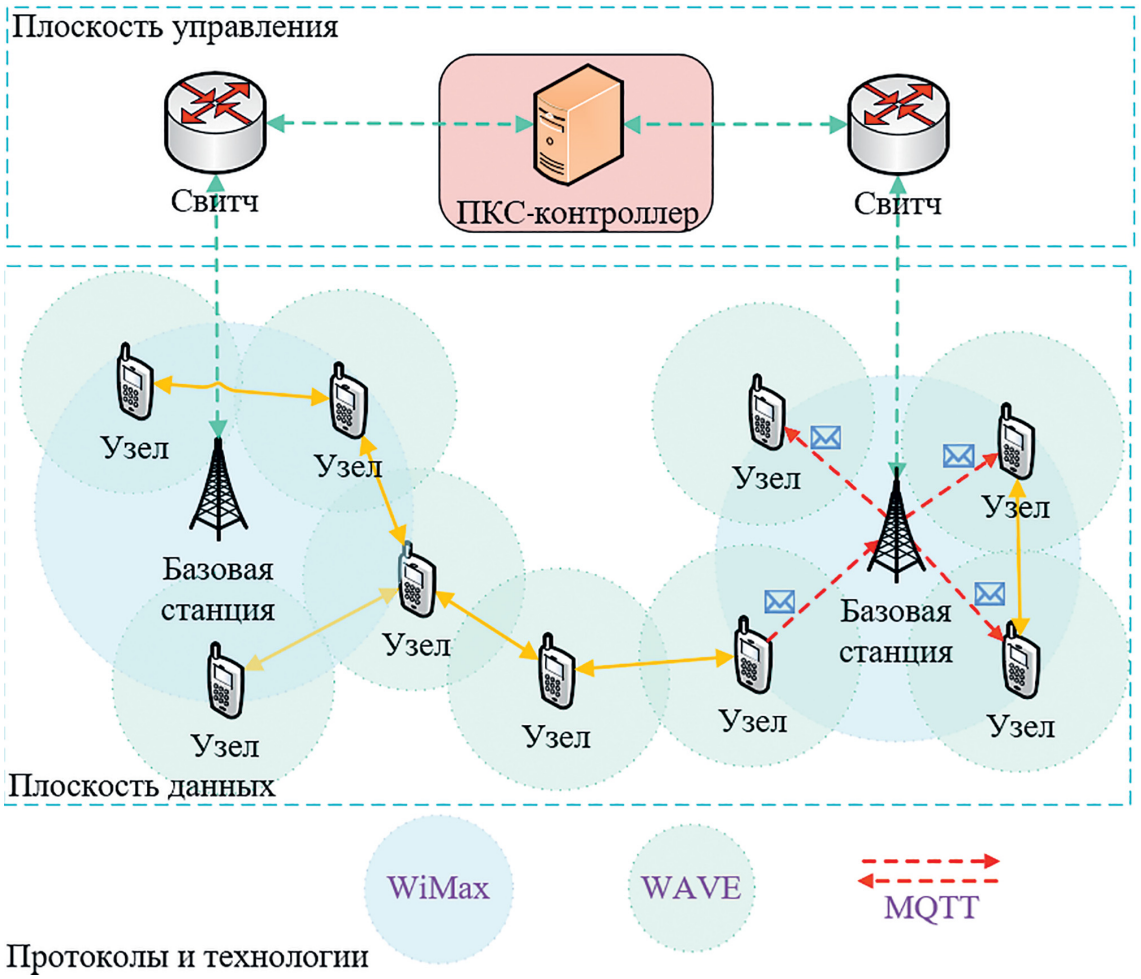

Рис. 1. Общая схема функционирования сегмента мобильной самоорганизующейся сети с поддержкой программно-конфигурируемых сетей

Fig. 1. General scheme of the mobile ad hoc network segment functioning with software-defined networking support

висов (service discovering) с целью регистрации мобильного узла и рассылки определенного тематического контента. Рассылка информации с датчиков конечных устройств может осуществляться с помощью протокола работы с телеметрией MQTT (Message Queuing Telemetry Transport) по модели подписки на контент. Конечный узел сети может осуществлять определенную рассылку (например, сервис информирования о погодных условиях, сервис информирования о дорожной ситуации и др.), предварительно зарегистрировавшись на базовой станции и указав способ доведения информации до остальных узлов сети.

Современное состояние исследований

Вопросы разработки архитектуры и моделей обеспечения безопасности MANETs рассмотрены во многих научных работах. В работе [1] описана архитектура безопасности MANET в виде пяти уровней: надежной инфраструктуры, безопасности связи и маршрутизации, сетевой безопасности и безопасности приложений. В [2] исследованы вопросы обеспечения безопасности протоколов маршрутизации интернета вещей в MANETs, с помощью описания классов используемых протоколов и расширения безопасности. В работе [3] представлена концептуальная облачная модель MANET для умных устройств на базе технологии 5G. В [4] разработана модель безопасности на основе метода шифрования Advanced Encryption Standard (AES) для генерации секретных ключей в кластерных MANETs. В работе [5] предложена модель байесовской игры с неполной информацией для анализа обычных и злонамеренных узлов в MANETs. В [6] описана энергоэффективная многомерная модель доверительного управления для достижения улучшенных параметров качества обслуживания в MANETs. В [7] представлены двухуровневая модель клиент-сервера для комплексной безопасности в MANETs, которая объединяет внутренние и внешние системы обнаружения вторжений в единое устройство.

Наиболее распространенными в MANETs являются атаки вида «отказ в обслуживании» DoS (Denial-of-Service) и DDoS (Distributed Denial-of-Service), а также Blackhole [8]. В случае реализации DoS- и DDoS-атак тот или иной узел сети временно выходит из строя, получая на обработку множество однотипных запросов, сгенерированных множеством злонамеренных узлов. При реализации Blackhole-атак, злонамеренный узел сбрасывает все входящие пакеты, затрудняя маршрутизацию сетевых потоков в MANETs.

Для повышения безопасности протокола маршрутизации AODV в MANET в работе [9] предложен подход изоляции вредоносных узлов на основе модели доверия. В [10] рассмотрено использование нечеткой логики для методики расчета доверия узлов сети, с целью обнаружения атак вида Blackhole, Grayhole и DDoS. В [11] описана вариация безопасного протокола маршрутизации AODV для защиты от кооперативной атаки вида Blackhole на базе хаотических отображений. Для обнаружения атак вида DDoS и Blackhole в работе [12] использован механизм аутентификации, основанный на упрощенном алгоритме шифрования и MAC-аутентификации, который доказал эффективность предложенного решения на базе сетевого симулятора NS-2. В [13] использован сетевой симулятор NS-3 для изучения влияния атаки вида Blackhole на параметры производительности MANET, такие как пропускная способность, сквозная задержка и коэффициент потери пакетов. В работе [14] использована оптимизация муравьиной колонии для предотвращения атаки вида Blackhole в MANET. В [15] проведены экспериментальные исследования обнаружения DDoS-атак, с помощью метода опорных векторов и оптимизации метода роя частиц. В [16] представлен метод на основе бэггинга классификаторов для выявления аномалий сетевого трафика.

В [17] разработана модель распространения информации в автомобильных самоорганизующихся сетях с использованием протокола передачи телеметрии MQTT. Работа [18] направлена на повышение безопасности MQTT-протокола на уровне приложений с целью противодействия DoS-атакам в беспроводных сетях. В [19] представлен механизм управления потоком на базе протокола MQTT, снижающий показатели метрик отбрасывания пакетов и сквозной задержки по сравнению со стандартной реализацией MQTT.

Таким образом, обзор актуальных научных исследований в области обеспечения безопасности сетей MANET показал, что в условиях отсутствия заранее определенной сетевой инфраструктуры при передаче информации между беспроводными устройствами методы интеллектуального анализа данных достаточно эффективно могут идентифицировать атаки. При этом на данный момент отсутствует общая формализованная структура MANET, а также обобщенный алгоритм обнаружения аномалий трафика. В рамках настоящей работы рассмотрены более подробно сформулированные проблемы обеспечения безопасности сети MANET.

Модель обнаружения аномалий трафика в сегменте мобильной самоорганизующейся сети

Представим сегмент MANET в момент времени t_j в виде случайного геометрического неориентированного графа $G^j = (V, E^j)$, $E^j \subseteq V \times V$, $|V| = n$, $|E^j| = m$ с фиксированным множеством узлов $V = (v_1, v_2, \ldots, v_{|V|})$ размера n и множеством дуг $E^j = (e_1, e_2, \ldots, e_{|E^j|})$ размера m. Граф G^j представляет собой пространственную сеть, построенную посредством случайного размещения n узлов в трехмерной плоскости A размера $s_1 \times s_2 \times s_3$, при этом два узла соединяются дугой e_k только в том случае, если их расстояние в момент времени t_j находится в заданных зонах покрытия. В связи с динамикой объектов MANET и изменением расстояния между ними, в каждый следующий момент времени t_{j+1} изменяется множество дуг E^{j+1} и, следовательно, сам неориентированный граф G^{j+1}. Множество дуг E^{j+1} сохраняет ребра множества E^j, если к моменту времени t_{j+1} связь между соответствующими объектами не потеряна, и добавляет новые ребра, которые характеризуют новые образовавшиеся связи за момент времени $(t_{j+1} - t_j)$. Таким образом, два $G^j = (V, E^j)$ и $G^i = (V, E^i)$ описывают одну и ту

же MANET с одними и теми же участниками движения (вершины графа полностью совпадают), но связь между ними через момент времени Δt будет характеризоваться различными дугами E^j, E^i (множества частично совпадают, если сохранилась связь между некоторыми объектами).

С учетом принципов функционирования MANETs, введем пространственно-временные характеристики для каждого узла динамического графа G^j.

Каждая вершина графа G^j представляет собой беспроводной роутер в виде кортежа значений

$$v_i^j = \{r_i, mob_i^j, spd_i^j, (x_i^j, y_i^j, z_i^j)\},\ i = \overline{1, |V|},$$

где r_i — зона покрытия i-го беспроводного роутера; mob_i^j — вид мобильности j-го узла в момент времени t_j; spd_i^j — скорость движения i-го узла в момент времени t_j; (x_i^j, y_i^j, z_i^j) — координаты местоположения i-го узла в момент времени t_j. По умолчанию все узлы графа G^j имеют линейную мобильность $mob_i^j = Linear$, однако если узел является стационарным, тогда его мобильность имеет вид $mob_i^j = Fixed$, а скорость $spd_i^j = 0$. Множество дуг E^j графа G^j представляет собой множество сетевых связей между узлами сети, размер которого динамически изменяется во времени в зависимости от текущей топологии MANET.

Определим расстояние между двумя беспроводными роутерами v_a^j и v_b^j в момент времени t_j как евклидово расстояние:

$$d(v_a^j, v_b^j) = \|v_a^j - v_b^j\|_2 = \sqrt{(x_a^j - x_b^j)^2 + (y_a^j - y_b^j)^2 + (z_a^j - z_b^j)^2}.$$

Дуга $e(v_a^j, v_b^j)$ строится только в том случае, когда $d(v_a^j, v_b^j) \le r_a + r_b$, что означает пересечение зон покрытия двух узлов.

При установлении соединения между двумя произвольными узлами в сети графа G осуществляется пересылка сетевых пакетов согласно выбранному протоколу маршрутизации. Множество всех потоков сетевого трафика в сегменте MANET обозначим в виде кортежа значений

$$Z = \{flowID, bR, fB, fA\},\ |Z| = fNUM,$$

где $flowID$ — уникальный идентификатор потока; bR — битрейт потока; fB и fA — множество базовых и приобретенных признаков потока. Введем понятие ПКС-контроллера в виде OpenFlow контроллера C и обозначим множество коммутаторов S_W, содержащих таблицы маршрутизации пакетов в сегменте MANET.

Модель обнаружения аномалий сетевого трафика

Построим модель машинного обучения на основе ансамблевых алгоритмов для первичного выявления аномалий внутри беспроводной распределенной самоорганизующейся сети, генерирующую потоки сетевого трафика в сегменте в формате множества Z. Задача состоит в распределении трафика и отсеивании «подозрительного». Для решения данной задачи построим модель бинарного классификатора сетевых угроз и обозначим ее в виде функции $h(Z)$: $Z \to \{0, 1\}$ которая присваивает каждому потоку трафика tz_i из множества всех сетевых потоков $Z = \{tz_1, tz_2, \ldots, tz_n\}$ метку 0 в случае отсутствия сетевой атаки и метку 1 в случае ее наличия. Обозначим через $bCLF$ выбранный для бинарной классификации наиболее эффективный метод машинного обучения.

Модель идентификации типа сетевой атаки

Следующий этап анализа «подозрительного» сетевого трафика — идентификация конкретного типа атаки для выработки последующей стратегии противодействия. Построим модель мультиклассового классификатора сетевых угроз и обозначим ее в виде функции $f(Z)$: $Z \to K$, которая присваивает каждому потоку трафика tz_i метку $k_j \in K$, $|K| > 2$, соответствующую нормальному трафику (benign traffic), либо конкретному виду сетевой атаки. Обозначим через $mCLF$ выбранный для мультиклассовой классификации метод машинного обучения. Результаты сравнения работы классификаторов представлены в разделе «Моделирование сценариев сетевых атак в рамках сегмента мобильной самоорганизующейся сети».

Оценим производительность сегмента MANET, а также эффективность и точность системы обнаружения аномалий, для этого введем в рассмотрение количественные метрики производительности.

1. Коэффициент доставки пакетов (Packet Delivery Ratio) — соотношение количества полученных пакетов к количеству отправленных, для исследуемых узлов сегмента сети.
2. Пропускная способность сети (Throughput) — соотношение размера успешно переданных по сети пакетов к общему времени симуляции сети $simT$.
3. Время передачи пакета от источника к получателю и обратно (round-trip-time) — разница времени получения ответа от получателя и времени отправки запроса от источника.
4. Сквозная задержка передачи пакетов в сети (End-to-end Delay) — разница между временем отправки пакета от источника и получения его получателем. В среднем End-to-end Delay составляет половину времени метрики round-trip-time.
5. Издержки (Overhead) — среднее количество пакетов, необходимых для доставки одного пакета данных. Рассчитаем в виде соотношения общего количества пакетов к количеству пакетов, полученных узлом-получателем. При этом общее количество пакетов включает в себя служебный (пакеты, передаваемые между роутерами) и пользовательский трафики (пакеты приложений).

Перечисленные метрики позволяют оценить эффективность симулируемых сетевых угроз в сегменте MANET с целью дальнейшего формирования набора данных для исследования методами машинного обучения.

Рассмотрим обобщенный алгоритм обнаружения аномалий трафика в MANETs.

Шаг 1	ПКС-контроллер *C* осуществляет мониторинг состояния сетевых потоков из множества *Z*, выбирая для анализа случайный сетевой поток каждые t_M минут.
Шаг 2	Для выбранного сетевого потока tz_i: **2.1** Проводится бинарная классификация $h(tz_i)$ с помощью классификатора *bCLF*. **2.2** Если $h(tz_i) = 1$: **2.2.1** Проводится мультиклассовая классификация $f(tz_i)$ с помощью классификатора *mCLF*. **2.2.2** Если обнаружена атака вида DDoS: **2.2.2.1** На ПКС-контроллере *C* формируется сообщение *flowPLC* для коммутатора S_i с политикой выборочного отбрасывания маркированных пакетов. **2.2.2.2** При получении сообщения на коммутаторе S_i происходит отбрасывание всех маркированных пакетов, соответствующих потоку tz_i. **2.2.3** Если обнаружена атака вида Blackhole: **2.2.3.1** На контроллере *cSDN* формируется сообщение *routingPLC* для коммутатора S_i с исключением злонамеренного узла, соответствующего потоку tz_i из всех таблиц маршрутизации сегмента сети. **2.3** Атака отсутствует, возобновление мониторинга (шаг 1 работы алгоритма).

Время мониторинга t_M подбирается экспериментально в рамках симулятора сегмента MANET при реализации различных сценариев осуществления сетевых атак. Операции классификации возможно выполнять на конечных узлах сегмента MANET при соблюдении вычислительных ресурсных ограничений. В этом случае узел самостоятельно проводит классификацию сетевых потоков данных и при обнаружении сетевой атаки информирует ПКС-контроллер *C* о возникшей угрозе. Далее происходит выработка правил реагирования на инциденты безопасности.

Моделирование сценариев сетевых атак в рамках сегмента мобильной самоорганизующейся сети

На базе симулятора OMNeT++ версии 5.6.2 и демонстрационных примеров фреймворка INET построен сегмент MANET, в рамках которого произведена отправка пакетов вида Ping, UDP (User Datagram Protocol) и TCP (Transmission Control Protocol) от узла-отправителя к узлу-получателю. Стандартный инструментарий OMNeT++ включает в себя возможность отслеживания количественных метрик производительности по результатам симуляции. На рис. 2 представлена схема сетевых потоков данных узла-отправителя по уровням

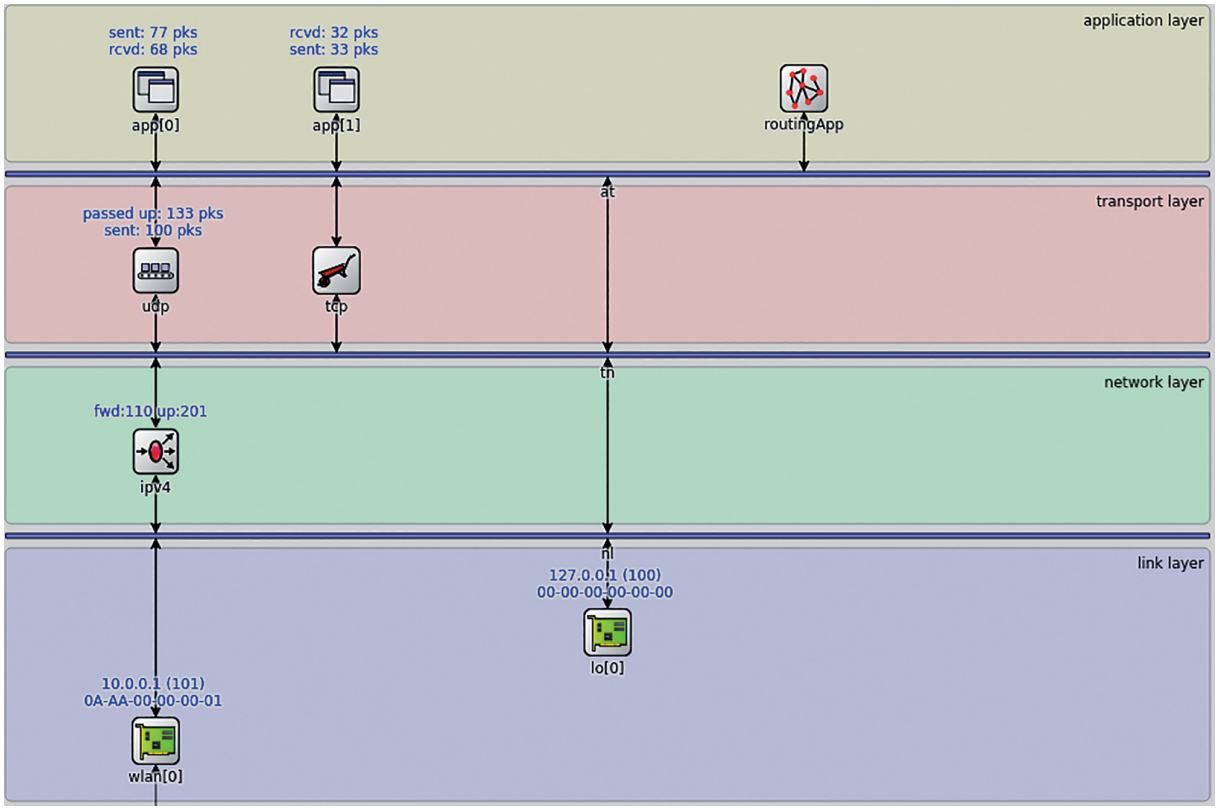

Рис. 2. Схема сетевых потоков данных для узла отправителя в OMNeT++

Fig. 2. Scheme of network data flows for the source node in OMNeT++

сетевой модели OSI в случайный момент выполнения симуляции.

Для оценки показателей качества функционирования сегмента MANET рассмотрим пять сценариев симуляций. Результаты рассмотренных симуляций приведены в таблице.

Сценарий 1. Симуляция сегмента сети без атак. Симуляция осуществляется в соответствии с общими настройками сегмента сети, при этом потенциально зловредные узлы также используются для маршрутизации.

Сценарий 2. Симуляция сегмента сети с Blackhole атакой. Симуляция осуществляется в соответствии с общими настройками сегмента сети, при этом на одном из узлов отключена опция forwarding, что приводит к удалению всех входящих на узел пакетов.

Сценарий 3. Симуляция сегмента сети с кооперативной Blackhole атакой. Симуляция осуществляется в соответствии с общими настройками сегмента сети, при этом на двух узлах отключена опция forwarding, что приводит к удалению всех входящих на узлы пакетов.

Сценарий 4. Симуляция сегмента сети с DoS-атакой. Симуляция осуществляется в соответствии с общими настройками сегмента сети, при этом один из узлов реализует UDP Flooding атаку, отправляя пакеты на источник с частотой 0,05 с, размер пакета распределен равномерно в интервале от 200 до 500 Б.

Сценарий 5. Симуляция сегмента сети с DDoS-атакой. Симуляция осуществляется в соответствии с общими настройками сегмента сети, при этом три узла реализуют UDP Flooding атаку, отправляя пакеты на источник и на адресат, с усредненной частотой 0,05 с, размер пакета распределен равномерно в интервале от 200 до 500 Б.

В соответствии с выполненными экспериментальными исследованиями, множество меток K мультиклассового классификатора $f(Z)$ зададим в виде: K = {«*Bening*», «*DoS*», «*DDoS*», «*Blackhole*», «*CooperativeBlackhole*»}. Отметим, что сетевые атаки вида cooperative blackhole attack и distributed denial-of-service attack оказывают наибольшее негативное влияние на производительность сегмента MANET, и система обнаружения вторжений в первую очередь должна быть сфокусирована на классификацию паттернов поведения сетевых угроз, характерных для этих типов атак.

Проведем исследование эффективности предложенного алгоритма классификации сетевого трафика в сегменте MANET. Для этого выполним одновременную симуляцию Сценариев 3 и 5 с кооперативной Blackhole атакой и атакой DDoS в исходном сегменте сети. В результате симуляции получим несбалансированный набор данных, состоящий из 52 столбцов-признаков и 5840 записей со следующим распределением: «Benign»: 4247; «DDoS»: 834; «Cooperative Blackhole»: 759. Балансировку данных произведем с помощью алгоритма SMOTE. Получим сбалансированный набор данных, состоящий из 11 375 записей со следующим распределением: «Benign»: 3849; «DDoS»: 3847; «Cooperative Blackhole»: 3679. В качестве метрики оценки классификации используем долю правильных ответов (accuracy) при сравнении трех современных классификаторов: XGBoost, LightGBM и AdaBoost. Подбор оптимальных гиперпараметров произведем с использованием функции GridSearchCV. Результаты бинарной классификации на сбалансированном наборе данных: XGBoost — 88 %, LightGBM — 91 %, AdaBoost — 83 %. Результаты многоклассовой классификации на сбалансированном наборе данных: XGBoost — 83 %, LightGBM — 90 %, AdaBoost — 64 %. Матрица ошибок классификатора LightGBM для многоклассовой классификации сетевого траффика представлена на рис. 3.

В результате можно сделать вывод о том, что классификатор LightGBM показывает наилучшие результаты для обнаружения аномалий сетевого трафика и идентификации конкретной сетевой атаки. При проведении дальнейших исследований обученный классификатор с подобранными гиперпараметрами будет выгружен в качестве модели обнаружения атак.

Таблица. Оценка показателей качества функционирования сегмента мобильной самоорганизующейся сети
Table. Evaluation of the functioning quality indicators of the MANET segment

Результаты симуляций	Сценарий				
	1	2	3	4	5
Отправлено/получено UDP-пакетов	729/259	798/625	718/36	734/425	708/225
Количество операций маршрутизации	31 447	32 058	19 859	65 223	206 879
Время в очереди, с	4,29	8,85	1,69	4,62	7,04
Полное время передачи пакета, с	1,15	0,84	0,62	0,98	1,2
Коэффициент доставки пакетов, %	36	78	5	58	32
Пропускная способность, Б/с	60,43	145,83	8,40	99,17	52,50
Сквозная задержка, с	0,58	0,42	0,31	0,49	0,60
Издержки маршрутизации, пакеты	121	51	551	153	919

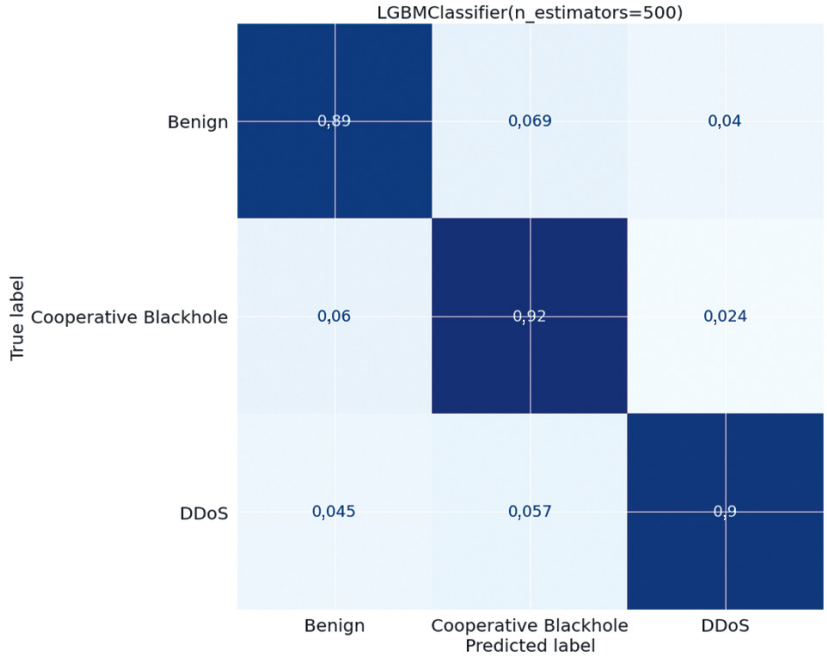

Рис. 3. Матрица ошибок классификатора LightGBM
Fig. 3. Confusion matrix of LightGBM Classifier

Заключение

Мобильные самоорганизующиеся сети имеют большой потенциал применения, особенно в сфере развития интеллектуальных транспортных систем. Разработанная модель обнаружения аномалий трафика легла в основу архитектуры распределенной интеллектуальной системы выявления угроз и обеспечения безопасности при передаче данных в беспроводных распределенных самоорганизующихся сетях. Обобщенный алгоритм обнаружения аномалий трафика будет использоваться при разработке метода распределенного обнаружения сетевых атак в рамках дальнейших исследований.

Литература

1. Li S.-C., Yang H.-L., Zhu Q.-S. Research on MANET security architecture design // Proc. of the 2010 International Conference on Signal Acquisition and Processing (ICSAP). 2010. P. 90–93. https://doi.org/10.1109/ICSAP.2010.19
2. Karlsson J., Dooley L.S., Pulkkis G. Secure routing for MANET connected Internet of Things systems // Proc. of the 6th IEEE International Conference on Future Internet of Things and Cloud (FiCloud). 2018. P. 114–119. https://doi.org/10.1109/FiCloud.2018.00024
3. Alam T. Device-to-Device communications in cloud, MANET and Internet of Things integrated architecture // Journal of Information Systems Engineering and Business Intelligence. 2020. V. 6. N 1. P. 18–26. https://doi.org/10.20473/jisebi.6.1.18-26
4. Nehra D., Dhindsa K.S., Bhushan B. A Security Model to Make Communication Secure in Cluster-Based MANETs // Advances in Intelligent Systems and Computing. 2020. V. 1079. P. 183–193. https://doi.org/10.1007/978-981-15-1097-7_16
5. Olanrewaju R.F., Khan B.U.I., Anwar F., Mir R.N., Yaacob M., Mehraj T. Bayesian signaling game based efficient security model for MANETs // Lecture Notes in Networks and Systems. 2020. V. 70. P. 1106–1122. https://doi.org/10.1007/978-3-030-12385-7_75
6. Shabut A.M., Kaiser M.Sh., Dahal K.P., Chen W. A multidimensional trust evaluation model for MANETs // Journal of Network and Computer Applications. 2018. V. 123. P. 32–41. https://doi.org/10.1016/j.jnca.2018.07.008
7. Salama H.M., El Mageed M.Z.A., Salama G.I.M., Badran K.M. CSMCSM: Client-Server Model for Comprehensive Security in MANETs // International Journal of Information Security and Privacy. 2021. V. 15. N 1. P. 44–64. https://doi.org/10.4018/IJISP.2021010103
8. Alani M.M. MANET security: A survey // Proc. of the 4th IEEE International Conference on Control System, Computing and

References

1. Li S.-C., Yang H.-L., Zhu Q.-S. Research on MANET security architecture design. *Proc. of the 2010 International Conference on Signal Acquisition and Processing (ICSAP)*, 2010, pp. 90–93. https://doi.org/10.1109/ICSAP.2010.19
2. Karlsson J., Dooley L.S., Pulkkis G. Secure routing for MANET connected Internet of Things systems. *Proc. of the 6th IEEE International Conference on Future Internet of Things and Cloud (FiCloud)*, 2018, pp. 114–119. https://doi.org/10.1109/FiCloud.2018.00024
3. Alam T. Device-to-Device communications in cloud, MANET and Internet of Things integrated architecture. *Journal of Information Systems Engineering and Business Intelligence*, 2020, vol. 6, no. 1, pp. 18–26. https://doi.org/10.20473/jisebi.6.1.18-26
4. Nehra D., Dhindsa K.S., Bhushan B. A Security Model to Make Communication Secure in Cluster-Based MANETs. *Advances in Intelligent Systems and Computing*, 2020, vol. 1079, pp. 183–193. https://doi.org/10.1007/978-981-15-1097-7_16
5. Olanrewaju R.F., Khan B.U.I., Anwar F., Mir R.N., Yaacob M., Mehraj T. Bayesian signaling game based efficient security model for MANETs. *Lecture Notes in Networks and Systems*, 2020, vol. 70, pp. 1106–1122. https://doi.org/10.1007/978-3-030-12385-7_75
6. Shabut A.M., Kaiser M.Sh., Dahal K.P., Chen W. A multidimensional trust evaluation model for MANETs. // *Journal of Network and Computer Applications*. 2018, vol. 123, pp. 32–41. https://doi.org/10.1016/j.jnca.2018.07.008
7. Salama H.M., El Mageed M.Z.A., Salama G.I.M., Badran K.M. CSMCSM: Client-Server Model for Comprehensive Security in MANETs. *International Journal of Information Security and Privacy*, 2021, vol. 15, no. 1, pp. 44–64. https://doi.org/10.4018/IJISP.2021010103

Engineering (ICCSCE). 2014. P. 559–564. https://doi.org/10.1109/ICCSCE.2014.7072781
9. Kamel M.B.M., Alameri I., Onaizah A.N. STAODV: a secure and trust based approach to mitigate blackhole attack on AODV based MANET // Proc. of the 2nd IEEE Advanced Information Technology, Electronic and Automation Control Conference (IAEAC). 2017. P. 1278–1282. https://doi.org/10.1109/IAEAC.2017.8054219
10. Khare A.K., Rana J.L., Jain R.C. Detection of wormhole, blackhole and DDOS attack in MANET using trust estimation under fuzzy logic methodology // International Journal of Computer Network and Information Security (IJCNIS). 2017. V. 9. N 7. P. 29–35. https://doi.org/10.5815/ijcnis.2017.07.04
11. El-Semary A.M., Diab H. BP-AODV: Blackhole protected AODV routing protocol for MANETs based on chaotic map // IEEE Access. 2019. V. 7. P. 95197–95211. https://doi.org/10.1109/ACCESS.2019.2928804
12. Khan S., Hashim F., Rasid M.F.A., Perumal T. Reducing the severity of black hole and DDoS attacks in MANETs by modifying AODV protocol using MAC authentication and symmetric encryption // Proc. of the 2nd International Conference on Telematics and Future Generation Networks (TAFGEN). 2018. P. 109–114. https://doi.org/10.1109/TAFGEN.2018.8580488
13. Li G., Yan Z., Fu Y. A study and simulation research of blackhole attack on mobile AdHoc network // Proc. of the 6th IEEE Conference on Communications and Network Security (CNS). 2018. P. 8433148. https://doi.org/10.1109/CNS.2018.8433148
14. Khan D.M., Aslam T., Akhtar N., Qadri S., Khan N.A., Rabbani I.M., Aslam M. Black hole attack prevention in mobile ad-hoc network (MANET) using ant colony optimization technique // Information Technology and Control. 2020. V. 49. N 3. P. 308–319. https://doi.org/10.5755/j01.itc.49.3.25265
15. Gautam D., Tokekar V. A novel Approach for Detecting DDoS Attack in MANET // Materials Today: Proceedings. 2020. V. 29. P. 674–677. https://doi.org/10.1016/j.matpr.2020.07.332
16. Рзаев Б.Т., Лебедев И.С. Применение бэггинга при поиске аномалий сетевого трафика // Научно-технический вестник информационных технологий, механики и оптики. 2021. Т. 21. № 2. С. 234–240. https://doi.org/10.17586/2226-1494-2021-21-2-234-240
17. Tomar R., Prateek M., Sastry H.G. A novel approach to multicast in VANET using MQTT // Ada User Journal. 2017. V. 38. N 4. P. 231–235.
18. Potrino G., De Rango F., Santamaria A.F. Modeling and evaluation of a new IoT security system for mitigating DoS attacks to the MQTT broker // Proc. of the IEEE Wireless Communications and Networking Conference (WCNC). 2019. P. 8885553. https://doi.org/10.1109/WCNC.2019.8885553
19. Sadeq A.S., Hassan R., Al-Rawi S.S., Jubair A.M., Aman A.H.M. A QoS approach for Internet of Things (IoT) environment using MQTT protocol // Proc. of the 2019 International Conference on Cybersecurity (ICoCSec). 2019. P. 59–63. https://doi.org/10.1109/ICoCSec47621.2019.8971097

8. Alani M.M. MANET security: A survey. *Proc. of the 4th IEEE International Conference on Control System, Computing and Engineering (ICCSCE)*, 2014, pp. 559–564. https://doi.org/10.1109/ICCSCE.2014.7072781
9. Kamel M.B.M., Alameri I., Onaizah A.N. STAODV: a secure and trust based approach to mitigate blackhole attack on AODV based MANET. *Proc. of the 2nd IEEE Advanced Information Technology, Electronic and Automation Control Conference (IAEAC)*, 2017, pp. 1278–1282. https://doi.org/10.1109/IAEAC.2017.8054219
10. Khare A.K., Rana J.L., Jain R.C. Detection of wormhole, blackhole and DDOS attack in MANET using trust estimation under fuzzy logic methodology. *International Journal of Computer Network and Information Security (IJCNIS)*, 2017, vol. 9, no. 7, pp. 29–35. https://doi.org/10.5815/ijcnis.2017.07.04
11. El-Semary A.M., Diab H. BP-AODV: Blackhole protected AODV routing protocol for MANETs based on chaotic map. *IEEE Access*, 2019, vol. 7, pp. 95197–95211. https://doi.org/10.1109/ACCESS.2019.2928804
12. Khan S., Hashim F., Rasid M.F.A., Perumal T. Reducing the severity of black hole and DDoS attacks in MANETs by modifying AODV protocol using MAC authentication and symmetric encryption. *Proc. of the 2nd International Conference on Telematics and Future Generation Networks (TAFGEN)*, 2018, pp. 109–114. https://doi.org/10.1109/TAFGEN.2018.8580488
13. Li G., Yan Z., Fu Y. A study and simulation research of blackhole attack on mobile AdHoc network. *Proc. of the 6th IEEE Conference on Communications and Network Security (CNS)*, 2018, pp. 8433148. https://doi.org/10.1109/CNS.2018.8433148
14. Khan D.M., Aslam T., Akhtar N., Qadri S., Khan N.A., Rabbani I.M., Aslam M. Black hole attack prevention in mobile ad-hoc network (MANET) using ant colony optimization technique. *Information Technology and Control*, 2020, vol. 49, no. 3, pp. 308–319. https://doi.org/10.5755/j01.itc.49.3.25265
15. Gautam D., Tokekar V. A novel Approach for Detecting DDoS Attack in MANET. *Materials Today: Proceedings*, 2020, vol. 29, pp. 674–677. https://doi.org/10.1016/j.matpr.2020.07.332
16. Rzayev B.T., Lebedev I.S. Applying bagging in finding network traffic anomalies. *Scientific and Technical Journal of Information Technologies, Mechanics and Optics*, 2021, vol. 21, no. 2, pp. 234–240. (in Russian). https://doi.org/10.17586/2226-1494-2021-21-2-234-240
17. Tomar R., Prateek M., Sastry H.G. A novel approach to multicast in VANET using MQTT. *Ada User Journal*, 2017, vol. 38, no. 4, pp. 231–235.
18. Potrino G., De Rango F., Santamaria A.F. Modeling and evaluation of a new IoT security system for mitigating DoS attacks to the MQTT broker. *Proc. of the IEEE Wireless Communications and Networking Conference (WCNC)*, 2019, pp. 8885553. https://doi.org/10.1109/WCNC.2019.8885553
19. Sadeq A.S., Hassan R., Al-Rawi S.S., Jubair A.M., Aman A.H.M. A QoS approach for Internet of Things (IoT) environment using MQTT protocol. *Proc. of the 2019 International Conference on Cybersecurity (ICoCSec)*, 2019, pp. 59–63. https://doi.org/10.1109/ICoCSec47621.2019.8971097

Авторы

Легашев Леонид Вячеславович — кандидат технических наук, ведущий научный сотрудник, Оренбургский государственный университет, Оренбург, 460018, Российская Федерация, SC 56134425700, https://orcid.org/0000-0001-6351-404X, silentgir@gmail.com

Гришина Любовь Сергеевна — преподаватель, Оренбургский государственный университет, Оренбург, 460018, Российская Федерация, SC 57205597695, https://orcid.org/0000-0003-2752-7198, zabrodina97@inbox.ru

Парфенов Денис Игоревич — кандидат технических наук, начальник отдела, Оренбургский государственный университет, Оренбург, 460018, Российская Федерация, SC 55809642700, https://orcid.org/0000-0002-1146-1270, parfenovdi@mail.ru

Жигалов Артур Юрьевич — ведущий программист, Оренбургский государственный университет, Оренбург, 460018, Российская Федерация, SC 57212882576, https://orcid.org/0000-0003-3208-1629, leroy137.artur@gmail.com

Autors

Leonid V. Legashev — PhD, Leading Researcher, Orenburg State University, Orenburg, 460018, Russian Federation, SC 56134425700, https://orcid.org/0000-0001-6351-404X, silentgir@gmail.com

Lubov S. Grishina — Lecturer, Orenburg State University, Orenburg, 460018, Russian Federation, SC 57205597695, https://orcid.org/0000-0003-2752-7198, zabrodina97@inbox.ru

Denis I. Parfenov — PhD, Head of Department, Orenburg State University, Orenburg, 460018, Russian Federation, SC 55809642700, https://orcid.org/0000-0002-1146-1270, parfenovdi@mail.ru

Arthur Yu. Zhigalov — Leading Software Developer, Orenburg State University, Orenburg, 460018, Russian Federation, SC 57212882576, https://orcid.org/0000-0003-3208-1629, leroy137.artur@gmail.com

Статья поступила в редакцию 15.09.2021
Одобрена после рецензирования 21.04.2022
Принята к печати 12.07.2022

Received 15.09.2021
Approved after reviewing 21.04.2022
Accepted 12.07.2022