Russian Technological Journal.
2026;14(1):19–30

ISSN 2782-3210 (Print)
ISSN 2500-316X (Online)

УДК 004.056.53
https://doi.org/10.32362/2500-316X-2026-14-1-19-30
EDN TXHMHW

НАУЧНАЯ СТАТЬЯ

Выделение потока сообщений между двумя абонентами в многоагентных системах на основе анализа его контекстуальных характеристик

М.О. Таныгин,
И.О. Мишин [@],
Е.А. Кулешова,
А.В. Киселев

Юго-Западный государственный университет, Курск, 305040 Россия
[@] Автор для переписки, e-mail: mishin.ilya46@yandex.ru

• **Поступила:** 28.04.2025 • **Доработана:** 01.07.2025 • **Принята к опубликованию:** 17.11.2025

Резюме

Цели. В статье исследуется задача повышения точности выделения потока сообщений между двумя абонентами в многоагентных системах на основе анализа контекстуальных характеристик общего потока сообщений в канале связи. При проведении процедур определения источника и установления его подлинности могут возникать коллизии кодов аутентификации двух и более сообщений. Одним из способов разрешения подобных ситуаций является выделение потока сообщений между двумя абонентами на основе его статистических характеристик, отличающихся от характеристик общего потока сообщений в системе. Цель работы – разработка метода, позволяющего надежно идентифицировать целевой поток в случае возникновения коллизий кодов аутентификации.

Методы. Для анализа и выделения паттернов активности агентов в потоке сообщений использованы контекстуальные характеристики сообщений: частота отправки, размер, временные метки и исторические данные взаимодействий. Метод включает формирование статистических характеристик потока сообщений между двумя агентами многоагентной системы (коэффициенты асимметрии и эксцесса, параметры распределения количества сообщений между событиями целевого источника) и их классификацию с помощью логистической регрессии.

Результаты. В ходе проведенных экспериментов было установлено, что разработанный метод демонстрирует значения метрики Precision (полнота) в диапазоне 0.81–0.85 (от 81% до 85% сообщений, классифицированных как принадлежащие целевому источнику, действительно являются таковыми), что на 40–50% превышает показатели существующих методов, основанных на анализе межпакетных интервалов времени. ROC[1]-анализ подтвердил высокую эффективность модели и приемлемое качество классификации.

[1] Receiver operating characteristic – рабочая характеристика приемника.

Выводы. Результаты исследования показали, что использование контекстуальных характеристик и статистического анализа позволяет точно выделять целевые потоки при общем числе агентов в многоагентных системах от 70 до 110. Метод может применяться в каналах связи с низкой пропускной способностью, где необходимо минимизировать размер заголовочных частей передаваемых пакетов данных и вычислительные затраты на выполнение процедур аутентификации.

Ключевые слова: многоагентные системы, контекстуальные характеристики, бинарная классификация, логистическая регрессия, асимметрия, эксцесс, ROC-анализ

Для цитирования: Таныгин М.О., Мишин И.О., Кулешова Е.А., Киселев А.В. Выделение потока сообщений между двумя абонентами в многоагентных системах на основе анализа его контекстуальных характеристик. *Russian Technological Journal*. 2026;14(1):19–30. https://doi.org/10.32362/2500-316X-2026-14-1-19-30, https://www.elibrary.ru/TXHMHW

Прозрачность финансовой деятельности: Авторы не имеют финансовой заинтересованности в представленных материалах или методах.

Авторы заявляют об отсутствии конфликта интересов.

RESEARCH ARTICLE

Identification of the message flow between two subscribers in multi-agent systems based on the analysis of its contextual characteristics

Maxim O. Tanygin,
Ilya O. Mishin [@],
Elena A. Kuleshova,
Alexey V. Kiselev

Southwest State University, Kursk, 305040 Russia
[@] Corresponding author, e-mail: mishin.ilya46@yandex.ru

• **Submitted:** 28.04.2025 • **Revised:** 01.07.2025 • **Accepted:** 17.11.2025

Abstract

Objectives. The paper examines the problem of improving the accuracy of identifying the message flow between two subscribers in multi-agent systems. This is done by analyzing the contextual characteristics of the overall message flow in the communication channel. Situations may arise during the process of source identification and verification of authenticity in which authentication codes for two or more messages collide. One way to resolve such conflicts is to isolate the message flow between two subscribers by leveraging its unique statistical characteristics which differ from the characteristics of the general message flow within the system. The aim of the paper is to develop a method which reliably identifies the target message flow even in cases of authentication code collisions.

Methods. The contextual characteristics of messages are used, in order to analyze and highlight patterns of agent behavior in the message flow. These characteristics include frequency of sending, message size, timestamps, and historical interaction data. The method involves the formation of statistical characteristics of the message flow between two agents in a multi-agent system, such as skewness and kurtosis, as well as distribution parameters for the number of messages sent between events from the target source along with their classification by means of logistic regression.

Results. During experiments, the method developed has been found to demonstrate a Precision metric value in the range of 0.81–0.85. This is 40–50% higher than existing methods based on the analysis of inter-packet time intervals, indicating that 81–85% of the messages classified as belonging to the target source are actually such. ROC[2] analysis confirmed the high efficiency of the model and acceptable classification quality.
Conclusions. The results of the study show that the use of contextual characteristics and statistical analysis enables the accurate identification of target flows in multi-agent systems with a total number of agents ranging from 70 to 110. This method can be used in low-bandwidth communication channels where it is essential to minimize the size of the transmitted batch header and computational costs associated with authentication procedures.

Keywords: multi-agent systems, contextual characteristics, binary classification, logistic regression, skewness, kurtosis, ROC analysis

For citation: Tanygin M.O., Mishin I.O., Kuleshova E.A., Kiselev A.V. Identification of the message flow between two subscribers in multi-agent systems based on the analysis of its contextual characteristics. *Russian Technological Journal.* 2026;14(1):19–30. https://doi.org/10.32362/2500-316X-2026-14-1-19-30, https://www.elibrary.ru/TXHMHW

Financial disclosure: The authors have no financial or proprietary interest in any material or method mentioned.

The authors declare no conflicts of interest.

ВВЕДЕНИЕ

Многоагентные системы (МАС) представляют собой сложные распределенные вычислительные системы, состоящие из множества взаимодействующих агентов, каждый из которых обладает определенной степенью автономии и способностью к адаптации. Эти системы находят широкое применение в различных областях, включая робототехнику, управление ресурсами, интеллектуальные транспортные системы и электронную коммерцию. Эффективность функционирования МАС во многом зависит от надежности и безопасности взаимодействий между агентами, что делает вопрос аутентификации особенно актуальным [1].

Аутентификация в контексте МАС представляет собой процесс проверки подлинности источников данных (агентов сети), что критически важно для обеспечения целостности и конфиденциальности передаваемой информации. Необходимость разработки адаптивных и устойчивых к атакам механизмов аутентификации становится очевидной, особенно в свете растущих угроз кибербезопасности.

Существует множество методов аутентификации, применяемых в МАС, каждый из которых оказывает влияние на безопасность и производительность системы.

Криптография является одним из наиболее распространенных подходов к аутентификации в МАС. Использование симметричных и асимметричных криптографических алгоритмов позволяет обеспечить надежную защиту данных и идентификацию агентов [2]. Симметричные методы, такие как симметричный алгоритм блочного шифрования (advanced encryption standard, AES), обеспечивают высокую скорость обработки, однако требуют безопасного обмена ключами. Асимметричные методы, такие как шифрование Ривеста – Шамира – Адлемана (Rivest – Shamir – Adleman, RSA) и шифрование на основе эллиптических кривых (elliptic-curve cryptography), позволяют избежать проблемы распределения ключей, но могут быть менее эффективными в условиях ограниченных ресурсов [3].

Существуют различные протоколы аутентификации, разработанные специально для МАС. Например, протоколы на основе challenge-response (вызов-ответ) позволяют агентам подтверждать свою идентичность, не раскрывая при этом свои секретные ключи. Эти протоколы могут быть дополнены механизмами временных меток для защиты от атак повторного воспроизведения [4, 5].

Многофакторная аутентификация (МФА), также применяющаяся в МАС, представляет собой подход, при котором для подтверждения идентичности агента требуется проверка нескольких параметров. Использование МФА в МАС обеспечивает высокий уровень безопасности, однако ее применение приводит к усложнению процесса аутентификации и увеличению времени отклика системы. Стоит отметить, что уязвимости и проблемы производительности могут возникнуть из-за недостатков проектирования или реализации протоколов. В работе [6] поднимается проблема поиска уязвимостей в протоколах МФА с применением систематического анализа. Авторы сформировали набор критериев для оценки безопасности, который включает как существующие, так и новые параметры. Также рассмотрена возможность применения МФА в различных сферах и выявлены потенциальные уязвимости. В результате исследования были обнаружены критические уязвимости в десяти основных протоколах МФА и предложены стратегии их устранения.

[2] Receiver operating characteristic.

Также стоит отметить применение динамической аутентификации в MAC, что предполагает использование изменяющихся параметров для подтверждения идентичности агентов. Например, агенты могут использовать временные пароли или одноразовые коды, генерируемые на основе определенных алгоритмов. Этот подход позволяет минимизировать риски, связанные с компрометацией статических учетных данных. Например, в статье [7] автор рассматривает пароль как метод аутентификации. Стоит отметить, что данный способ по-прежнему используется в качестве единственного метода аутентификации во многих системах. Если для конкретного сценария предъявляются более высокие требования к безопасности, он используется в сочетании с некоторыми другими методами аутентификации и формирует двухфакторную или многофакторную аутентификацию. В работе указаны недостатки данного метода аутентификации и предложен альтернативный метод – одноразовый пароль на основе времени (time-based one-time password, TOTP), который генерирует различные коды доступа, действительные в течение заранее установленного временного периода. Использование динамически созданных паролей и применение системы аутентификации, основанной на сочетании одноразовых паролей и классических паролей, может использоваться как для аутентификации пользователей, так и для аутентификации P2P (peer-to-peer, от хоста к хосту).

В MAC, где агенты могут взаимодействовать друг с другом в условиях неопределенности, важным инструментом является аутентификация на основе репутации. При этом агенты могут оценивать надежность и добросовестность других агентов на основе их предыдущих взаимодействий. Этот метод позволяет не только аутентифицировать агентов, но и формировать доверительные отношения в системе. В работе [8] авторами предложен метод аутентификации сообщений с помощью технологии блокчейн, основанный на механизме оценки репутации. В контексте данной работы блокчейн используется для управления идентификационными данными и сертификатами, а управление отзывом сертификатов и аутентификация личности реализованы с помощью смарт-контрактов. Для оценки надежности сообщений авторы предложили механизм оценки репутации, который можно интегрировать в аутентификацию сообщений для эффективной проверки их надежности. Проведенный в работе анализ производительности показал, что предложенная схема более эффективна в сравнении с традиционным протоколом аутентификации на основе подписей. Сравнение проводилось по таким характеристикам, как затраты вычислительных мощностей, время задержки сообщений и частота потери данных. Полученные авторами результаты показывают, что предложенная схема обеспечивает приемлемый уровень безопасности при воздействии различных известных типов кибератак.

С развитием блокчейн-технологий возникает возможность применения децентрализованных методов аутентификации в MAC. Блокчейн обеспечивает прозрачность и неизменность записей, что позволяет агентам безопасно обмениваться конфиденциальной информацией. Этот подход может значительно повысить уровень безопасности и снизить риски, связанные с централизованным управлением. В работе [9] предложена адаптивная модель стратегии МФА для обеспечения надежной аутентификации в динамических сценариях на основе технологии блокчейн и разработана модель консенсуса на основе алгоритма Raft для выбора авторитетного ведущего узла, обеспечивающая необходимую скорость аутентификации. Проведенный в работе анализ показал, что предложенная схема эффективна при противодействии кибератакам, нацеленным на системы аутентификации.

На основе проведенного анализа можно сделать вывод о том, что выбор метода аутентификации в MAC зависит от конкретных требований к безопасности, производительности и масштабируемости. Комбинирование различных подходов может привести к созданию более устойчивых и безопасных систем, способных эффективно функционировать в условиях динамичной среды, подверженной атакам.

ОБЗОР МЕТОДОВ ЗАЩИТЫ ОТ КОЛЛИЗИЙ ПРИ АУТЕНТИФИКАЦИИ В MAC

Каждое сообщение в MAC может быть снабжено уникальным идентификатором, который позволяет однозначно идентифицировать его среди других сообщений и предотвратить дублирование сообщений. Одной из проблем, возникающих при проведении процедур определения источника и установления его подлинности в MAC, являются коллизии таких идентификаторов. В рамках настоящей работы под коллизией понимается совпадение проверочных последовательностей у двух и более различных сообщений [10]. Существует множество методов защиты от коллизий. Рассмотрим основные из них.

Использование уникальных идентификаторов сообщений в качестве проверочных последовательностей позволяет избежать коллизий в процессе их аутентификации. Такие проверочные последовательности могут быть сгенерированы на основе временных меток, случайных чисел или комбинации этих факторов [11].

Одним из основных способов защиты от коллизий является использование криптографических стойких

хеш-функций, которые обладают свойствами, предотвращающими возможность нахождения двух или более различных сообщений, дающих одинаковый хеш-выход [12]. Примерами таких хеш-функций являются SHA-256 и SHA-3 (secure hash algorithm – безопасный алгоритм хеширования) [13]. К этому же классу систем относится использование алгоритмов цифровой подписи в различных областях для определения взаимосвязи между алгоритмами и их сценариями [14]. Авторы провели сравнительный анализ наиболее часто используемых алгоритмов цифровой подписи, в т.ч. алгоритмов RSA, алгоритмов Лэмпорта, алгоритма цифровой подписи на эллиптических кривых (elliptic curve digital signature algorithm) и алгоритма цифровой подписи на основе кривой Эдвардса (Edwards-curve digital signature algorithm), с точки зрения их производительности. В работе [15] проведен анализ существующих методов шифрования и предложена многоуровневая стратегия шифрования, в которой используются возможности AES для эффективного шифрования данных, RSA – для безопасной защиты ключей с помощью криптографии с открытым ключом и ролевое шифрование – для детального контроля доступа. Многоуровневый подход значительно увеличивает вычислительную сложность при попытках несанкционированного доступа. Интеграция этих алгоритмов позволила снизить риск компрометации ключей на 50% и повысить целостность данных за счет проверки MAC.

В то же время, если рассматривать класс MAC, где взаимодействие происходит по каналам связи с низкой пропускной способностью, примером которых могут быть сенсорные сети, сети промышленного интернета, интернета вещей, то для них использование описанных выше алгоритмов не представляется возможным, т.к. при ограниченном размере заголовка передаваемого пакета данных вероятность коллизии будет уже определяться не столько свойствами криптографических функций, сколько размером самого идентификатора. Это обеспечивает защиту от подмены и коллизий, т.к. изменение сообщения приведет к несоответствию хешей [16]. В работе рассмотрена конфиденциальность содержимого сообщения, а цифровая подпись подтверждает его подлинность и целостность. Эти методы позволяют не только защитить сообщение от несанкционированного доступа, но и гарантировать, что оно было отправлено именно тем агентом, который указан в подписи.

Соответственно, повысить достоверность разделения потоков (определения источника, сформировавшего каждое сообщение в потоке) можно за счет использования контекстуальных характеристик сообщений (информация о времени отправки, местоположении агента, типе сообщения и его содержании) в процессе аутентификации. Включение контекстуальной информации в процесс аутентификации позволяет более точно оценивать риски и принимать соответствующие меры. Например, в работе [17] поднимается проблема взаимодействия в MAC, связанная с коммуникацией, координацией и динамическими средами. Авторы описывают ключевые стратегии улучшения взаимодействия в MAC, уделяя особое внимание протоколам коммуникации, структурам вознаграждения, алгоритмам обучения и механизмам доверия. Внедрение стандартизированных форматов сообщений и разработка контекстно-зависимых коммуникационных стратегий могут значительно повысить ясность и актуальность совместно используемой информации. В свою очередь, алгоритмы обучения с подкреплением или глубоким обучением позволяют агентам адаптироваться к динамичным средам и со временем учиться кооперативному поведению. Интеграция таких стратегий при взаимодействии в MAC позволяет повысить эффективность и надежность решений в сложных динамичных средах.

В условиях динамичной среды MAC также целесообразно использовать адаптивные механизмы аутентификации, позволяющие изменять параметры в зависимости от характеристик сообщений и контекста взаимодействия. Например, в случае подозрительных сообщений система может запросить дополнительную аутентификацию или проверку. В работе [18] предложено решение, где используется оценка рисков в сочетании с системой МФА на базе платформы, которую можно интегрировать в приложения, что позволяет передать процесс аутентификации на внешний ресурс, сохраняя при этом внутреннюю защиту системы.

Использование комбинаций различных методов позволяет повысить точность выделения потока, например, применение статистического анализа – для предварительной фильтрации данных [19] и последующее применение алгоритмов машинного обучения – для увеличения точности классификации [20].

МАТЕРИАЛЫ И МЕТОДЫ

Для решения задачи выделения из общего потока сообщений в канале связи потока сообщений между двумя абонентами предлагается метод, основанный на анализе контекстуальных характеристиках общего потока сообщений в канале связи.

Если рассматривать в качестве примера MAC упомянутую ранее сенсорную сеть, то для разделения потоков сообщений от множества сенсоров в шлюзе в качестве контекстуальных характеристик можно рассматривать следующие [21]:

- частота отправки сообщений – это количественная характеристика, определяющая интенсивность передачи данных от отдельного агента – сенсора. Она рассчитывается как отношение количества сообщений, отправленных сенсором, к заданному временному интервалу;
- размер сообщений – это характеристика, отражающая объем данных, передаваемых сенсором. Она включает средний и максимальный размеры сообщений, отправляемых источником. Поскольку размер сообщений часто совпадает у сенсоров одного типа, этот параметр может быть использован для идентификации и классификации устройств в сети;
- типы сообщений – это параметр, который классифицирует сообщения по их содержанию или назначению (например, запросы, ответы, уведомления). Поскольку сенсоры одного типа часто отправляют сообщения схожего назначения, этот параметр может быть использован для выделения потоков данных от конкретных источников и анализа их активности;
- время отправки – это временная характеристика, определяющая момент передачи сообщений с использованием временных меток. Данный параметр позволяет анализировать паттерны активности сенсоров, однако потери пакетов, вызванные помехами, могут исказить данные, что необходимо учитывать при интерпретации результатов;
- исторические данные – информация о предыдущих взаимодействиях источника, включая успешные и неуспешные попытки аутентификации.

Предлагается способ разрешения ситуаций, связанных с коллизией идентификаторов сообщений, основанный на определении источника по числу сообщений, прошедших по каналу связи между двумя сообщениями, для которых проверяется гипотеза о том, что они сформированы данным источником. В основе рассматриваемого подхода лежит предположение о том, что контекстуальные характеристики агентов остаются относительно неизменными в течение времени, что позволяет использовать исторические данные для анализа и выделения потоков сообщений. Предполагается, что агент-источник может формировать свои сообщения для рассматриваемого приемника в зависимости от действий других агентов, например, формировать сообщения через фиксированное или вычисляемое число сообщений, переданных другими агентами MAC. Это значит, что агент может активным образом влиять на неизменность контекстуальных характеристик своего потока сообщений. Преимуществами такого решения являются простота реализации (что актуально для устройств с низкой производительностью, работающих от автономных источников питания), возможность реализации такого подсчета независимо как на стороне отправителя, так и на стороне получателя (не требуется передача такой метаинформации в служебных сообщениях).

Для анализа статистических характеристик потока сообщений в приемнике при проведении аутентификации и разделении потоков данных существует ряд механизмов:

1. Применение методов статистического анализа, таких как кластеризация и регрессионный анализ, позволяет выявить закономерности в данных и выделить целевой поток. Кластеризация может быть использована для группировки сообщений по схожим характеристикам, что позволяет выделить группы сообщений, относящихся к одному абоненту [22].
2. Алгоритмы машинного обучения (деревья решений, нейронные сети и методы опорных векторов) могут быть обучены на исторических данных для классификации сообщений и выделения интересующего потока. В качестве обучающего набора данных можно использовать формализованные данные об абонентах, между которыми происходило взаимодействие [23].
3. Анализ временных рядов позволяет учитывать временные зависимости в данных и выявлять аномалии, которые могут указывать на начало или окончание потока сообщений. Авторегрессионные модели и модели скользящего среднего, могут быть использованы для прогнозирования будущих сообщений на основе исторических данных [24].

Поскольку используется только одна контекстуальная характеристика, то кластеризация плохо подходит для принятия решения, потому что в таком случае она может давать большое количество ошибок первого и второго рода при схожести характеристик у разных потоков. Данные, полученные в результате анализа временных рядов, будут сильно искажаться в зависимости от используемых протоколов связи. Собственно, это вынудило авторов отказаться от модели с непрерывным временем [19], перейдя фактически к дискретному времени – подсчету переданных в MAC сообщений. Соответственно, целесообразным подходом к анализу получаемых выборок является машинное обучение и логистическая регрессия как способ, позволяющий минимизировать вычисления при принятии решений (что актуально для высокоавтономных устройств-сенсоров в рассматриваемом классе MAC).

Рассмотрим модель формирования анализируемых выборок, состоящих из количества переданных в MAC сообщений между сообщениями потока данных от одного источника в один приемник (рис. 1).

Имеем некоторую последовательность сообщений $S_{i-1}, S_i, S_{i+1}, S_{i+l-1}, ..., S_{i+l}, S_{i+l+1}, S_{i+l+2}$, отправляемых целевым агентом сети, и множества сообщений от других агентов сети $\mathbf{D}_{i-1}, \mathbf{D}_i, \mathbf{D}_{i+1}, ..., \mathbf{D}_{i+k-1}, \mathbf{D}_{i+k}$, передаваемых соответственно. Между парами S_{i-1} и S_i, S_i и S_{i+1}, ..., S_{i+l-1} и S_{i+l} подсчитывается количество сообщений других агентов, которые были переданы в системе. Обозначим как $n_{i-1}, n_i, n_{i+1}, ..., n_{i+k-1}, n_{i+k}$ мощности соответствующих множеств, на основании которых формируется последовательность значений, отражающих количество сообщений между предыдущим, текущим и следующим сообщениями целевого агента.

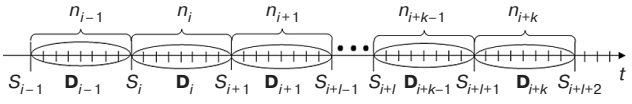

Рис. 1. Схема формирования выборки статистических характеристик потока сообщений в зависимости от времени поступления сообщений

Формирование сообщений через фиксированное или вычисляемое значение сообщений в МАС имеет существенный недостаток с точки зрения информационной безопасности, т.к. для стороннего наблюдателя сравнительно легко выделить такие потоки. Таким образом, структура МАС становится изучаемой для злоумышленника даже без анализа непосредственно содержимого передаваемых данных. Если же использовать в качестве размеров множеств $\mathbf{D}_{i-1}, \mathbf{D}_i, \mathbf{D}_{i+1}, ..., \mathbf{D}_{i+k-1}, \mathbf{D}_{i+k}$ случайные числа, при условии известности для приемника и отправителя закона распределения и параметров распределения как секретного идентификатора потока сообщений между ними, то для злоумышленника выделить сообщение анализируемого источника в общем потоке сообщений МАС становится трудноразрешимой задачей, требующей продолжительного времени наблюдения за системой.

Процесс формирования потока сообщений выглядит следующим образом. После отправки сообщения источником происходит ожидание отправки случайного числа сообщений другими агентами МАС. При этом само число, как было сказано выше, может быть постоянным или исчисляемым. В настоящей работе использован источник, который формировал свои сообщения через число сообщений, подчиненное распределению Пуассона. Случайность интервала позволяет маскировать сообщения каждого конкретного источника, скрывая структуру МАС и контекстуальные характеристики информационных потоков отдельных источников.

Рассмотрим ситуацию возникновения коллизии используемых в качестве проверочных последовательностей уникальных идентификаторов сообщений от одного конкретного агента (рис. 2). Имеем последовательность сообщений S_{i-1}, S_i, S_{i+1}, S_{i+l-1}, ..., S_{i+l}, S_{i+l+1}, S_{i+l+2}, сформированных целевым агентом с интервалами $n_{i-1}, n_i, n_{i+1}, ..., n_{i+k-1}, n_{i+k}$ – случайными числами, распределенными в рассматриваемом случае по закону Пуассона. В промежутке между сообщениями S_{i-1} и S_{i+1} получено сообщение S_{ab}, такое, что проверка его идентификатора позволяет определить его как сообщение целевого агента, сформированное между указанными двумя аутентичными сообщениями. Если исходить из предположения, что параметры формирования уникальных проверочных последовательностей неизвестны злоумышленнику, и совпадение таких последовательностей у S_{ab} и S_i произошло случайно, то случайным является номер такого сообщения в последовательности $n_{i-1} + n_i$ сообщений в МАС. Следовательно, n_{ab} равномерно распределено в интервале $n_{i-1} + n_i$.

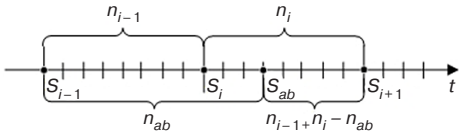

Рис. 2. Модель формирования интервалов в случае коллизии уникальных проверочных последовательностей двух различных сообщений

Перед приемником стоит задача на основе анализа двух пар значений (n_{i-1}, n_i) и $(n_{ab}, n_{i-1} + n_i - n_{ab})$ определения вероятности того, что пара 1 распределена по закону Пуассона, что соответствует формированию соответствующих сообщений целевым агентом, а пара 2, соответственно, нет, что позволяет проигнорировать сообщение S_i. При этом данные пары чисел могут быть дополнены некоторым количеством случайных чисел, распределенных по закону Пуассона (числом сообщений в МАС, переданным между несколькими сообщениями целевого источника, предшествующими или следующим после коллизии). Это соответствует рассмотрению не только последовательности из трех сообщений, где произошла коллизия, но и более объемной выборке сообщений данного агента. Но размер такой выборки априори не может быть большим, т.к. в противном случае решение о выборе одного из двух сообщений, вызвавших коллизию, происходило бы с существенной задержкой или требовало бы хранения большой истории сообщений, что снижало бы такие показатели агентов, как их автономность.

Как показано в работе [25], использование коэффициентов эксцесса и асимметрии позволяет идентифицировать тип распределения. Поскольку данные коэффициенты отражают различия в паттернах активности агентов, они могут применяться как признаки для классификации потоков сообщений.

Для анализа выборок небольшого размера использование коэффициентов эксцесса и асимметрии обосновано тем, что данные коэффициенты сильно зависят от крайних значений, что делает их ненадежными при малом размере выборки ($n < 50$), а стандартные ошибки коэффициентов растут при уменьшении n, что снижает мощность тестов на нормальность [26].

ЭКСПЕРИМЕНТАЛЬНЫЕ ИССЛЕДОВАНИЯ

В работе исследовалось разделение потоков сообщений в МАС при следующих параметрах формирования сообщения источником и анализа сообщений приемником:

- M_chain = 11 – число анализируемых сообщений целевого агента, среди которых для одного сообщения произошла коллизия идентификатора;
- K = 70–110 – параметр распределения Пуассона (известный приемнику), используемый источником для формирования интервалов между соседними сообщениями (применительно к МАС – отношение числа сообщений всех агентов МАС к числу сообщений, формируемых источником в единицу времени), также может трактоваться как число агентов в МАС в случае равенства интенсивностей формирования сообщений различными агентами.

Для оценки качества классификации с помощью метода выделения потоков сообщений, основанного на индивидуальных статистических характеристиках каждого абонента, использовалась бинарная классификация.

Каждый цикл моделирования тестового набора данных состоял из следующих этапов:

1. Создание пустых массивов для хранения данных о сообщениях и их характеристиках.
2. Цикл для генерации данных:
   а) генерация временных интервалов для последовательности сообщений с использованием распределения Пуассона (последовательность A_1: $n_1, ..., n_9, n_{10}$).
   б) генерация временных интервалов для последовательности сообщений с одним посторонним сообщением (последовательность A_2: $n_1, ..., n_{ab}, n_9 + n_{10} - n_{ab}$, где n_{ab} – равномерно распределенное число в интервале $n_9 + n_{10}$).
   в) вычисление асимметрии a и эксцесса e для двух наборов данных A_1 и A_2.
   г) присвоение меток из диапазона {0; 1} входным наборам данных: $f(e_1, a_1, e_2, a_2) = 1$, $f(e_2, a_2, e_1, a_1) = 0$.

Далее на сформированном наборе данных были синтезированы обучающие и тестовые наборы данных, которые использовались для обучения модели логистической регрессии. Проведена оценка качества классификации модели на тестовом наборе данных. На основе полученных значений ошибок первого и второго рода построена матрица классификации и проведен ROC[3]-анализ для оценки качества модели.

Для бинарной классификации использовалась логистическая регрессия. Вероятность того, что событие Y произойдет при заданных значениях X описывается следующим образом:

$$P(Y = 1 \mid X) = \frac{1}{1 + e^{-(\beta_0 + \beta_1 X_1 + \beta_2 X_2 + ... + \beta_n X_n)}}, \quad (1)$$

где $\beta_0, \beta_1, ..., \beta_n$ – коэффициенты модели.

Для оценки качества бинарной классификации использовались следующие метрики:

1. Специфичность (True Negative Rate), которая описывается формулой:

$$TNR = \frac{TN}{TN + FP}, \quad (2)$$

где TN (True Negatives) – количество истинно отрицательных результатов, FP (False Positives) – количество ложно положительных результатов.

2. Меткость (Accuracy) – метрика точности, которая показывает степень близости результатов измерений к принятому опорному значению, описывается формулой:

$$Accuracy = \frac{TP + TN}{TP + TN + FP + FN}, \quad (3)$$

где TP (True Positives) – количество истинно положительных результатов, FN (False Negatives) – количество ложно отрицательных результатов.

3. Точность (Precision), описывается формулой:

$$Precision = \frac{TP}{TP + FP}. \quad (4)$$

4. Полнота (Recall), описывается формулой:

$$Recall = \frac{TP}{TP + FN}. \quad (5)$$

5. $F1$-мера – гармоническое среднее между величинами Precision и Recall:

$$F1 = 2 \cdot \frac{Precision \times Recall}{Precision + Recall}. \quad (6)$$

Значение $F1$-меры варьируется от 0 до 1, где 1 указывает на идеальную точность и полноту, а 0 – на полное отсутствие правильных предсказаний.

[3] Receiver operating characteristic – рабочая характеристика приемника.

Для агрегирования таких метрик, как Precision, Recall и $F1$-меры, в многоклассовых задачах классификации использовались следующие способы:

1. Macro average (макроусреднение – среднее значение, которое связано с агрегированием или общими показателями) используется для оценки производительности модели по всем классам одинаково, независимо от их размера:

$$\text{Macro avg} = \frac{1}{N}\sum_{i=1}^{N} M_i, \quad (7)$$

где N – количество классов, M_i – значение метрики для класса i.

2. Weighted average (взвешенное среднее) – рассчитывает среднее значение метрики для каждого класса, но при этом учитывает количество экземпляров в каждом классе:

$$\text{Weight avg} = \frac{\sum_{i=1}^{N} M_i \omega_i}{\sum_{i=1}^{N} \omega_i}, \quad (8)$$

где ω_i – количество экземпляров (или вес) в классе i.

РЕЗУЛЬТАТЫ И ИХ ОБСУЖДЕНИЕ

В результате проведенных исследований установлено, что значения метрик (Precision, Recall, $F1$) для каждого из двух классов (0; 1) при K = 70–110, полученные при использовании метода выделения потоков сообщений на основе контекстуальных характеристик информационных потоков отдельных источников, находятся в диапазоне от 0.81 до 0.85. Значения метрик Precision означают, что от 81% до 85% сообщений, классифицированных как принадлежащие целевому источнику, действительно являются таковыми. Значение метрики Recall показывает, что от 81% до 85% всех сообщений целевого источника были идентифицированы корректно. Значение $F1$-меры указывает на сбалансированность модели, т.е. способность минимизировать как ложноположительные, так и ложноотрицательные ошибки.

Метрика Accuracy отражает общую долю верно классифицированных сообщений, это означает, что от 81% до 85% всех сообщений в системе (как целевых, так и посторонних) были корректно отнесены к своим классам. Совпадение значений Macro avg и Weighted avg указывает на отсутствие дисбаланса между классами, что является важным, т.к. в реальных условиях равномерное распределение целевых и посторонних сообщений упрощает анализ и повышает надежность метода.

Идентичные значения для классов 0 и 1 объясняются сбалансированностью данных и оптимизированным выбором признаков (статистических характеристики потока сообщений).

На рис. 3 изображена ROC-кривая для модели логистической регрессии при K = 90. Ось x отражает долю ложноположительных срабатываний (False Positive Rate), а ось y – долю истинно положительных срабатываний (True Positive Rate). Площадь под кривой AUC (Area Under Curve) составляет 0.83, что может свидетельствовать о высокой чувствительности модели и о ее способности к различению целевых и посторонних сообщений с приемлемым результатом.

Анализ результатов экспериментов показал, что модель демонстрирует стабильную работу даже при большой величине K – отношении общего числа сообщений в МАС в единицу времени к числу сообщений целевого агента за такой же временной интервал.

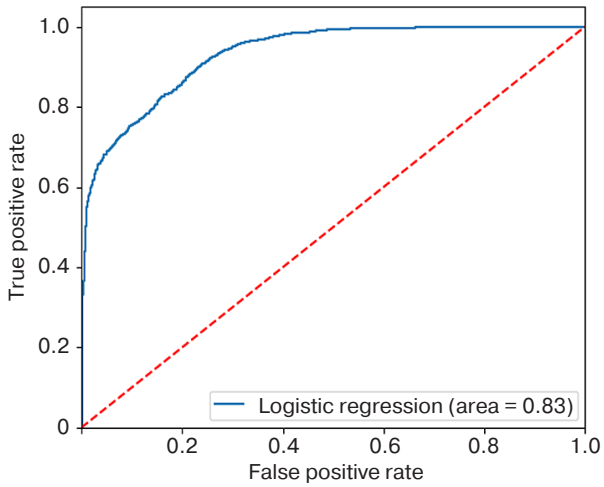

Рис. 3. ROC-кривая для модели логистической регрессии (Logistic Regression) при K = 90 (синяя сплошная линия), красная пунктирная линия – случайный классификатор (AUC = 0.5)

В рассматриваемой ранее работе [19] предложен метод определения источника сообщений на основе статистического анализа времени межпакетных интервалов. Также использован анализ коэффициентов эксцесса и асимметрии, но решающие правила сформулированы в виде линейных зависимостей между данными параметрами. В работе не учитывалось влияние помех на канал связи и время доставки, т.к. отказ от времени межпакетного интервала в нашем случае позволил обоснованно не учитывать такие помехи.

Использование же комплексного анализа статистических характеристик по сравнению с анализом алгебраического сравнения коэффициентов эксцесса и асимметрии позволил получить более высокие значения метрики Precision, чем в работе [19]. Так, при аналогичной заданной длине последовательности сообщений источника M_chain = 11 авторам [19] удалось достигнуть значения метрики Precision, равной 0.3–0.4.

Сравнив полученный в данном исследовании показатель с описанным выше методом, можно сделать вывод, что при аналогичных параметрах системы связи значение метрики Precision увеличилось на 0.4–0.5.

ВЫВОДЫ

Выполненная в настоящей работе проверка гипотезы о возможности использования коэффициентов эксцесса и асимметрии для идентификации типа распределения случайных величин показала ее применимость для выделения различий в паттернах активности агентов на основе их контекстуальных характеристик.

В результате имитационного моделирования работы подсистемы разделения потоков сообщений в случае коллизии уникальных идентификаторов сообщений получены приемлемые значения метрик качества бинарной классификации при использовании метода выделения потоков сообщений на основе характеристик информационных потоков отдельных источников.

Описанный подход, заключающийся в подсчете общего числа переданных всеми элементами MAC сообщений между сообщениями целевого агента, отличается простотой реализации (что актуально для устройств с низкой производительностью, работающих от автономных источников питания) и возможностью реализации такого подсчета независимо как на стороне отправителя, так и на стороне получателя. При этом достигаемая точность классификации равна 0.81–0.85.

Результаты исследования показали, что использование контекстуальных характеристик и статистического анализа позволяет точно выделять целевые потоки при общем числе агентов в MAC от 70 до 110. Метод может применяться в каналах связи с низкой пропускной способностью, где необходимо минимизировать размер заголовочных частей передаваемых пакетов данных и вычислительные затраты на выполнение процедур аутентификации. Перспективным направлением является интеграция адаптивных механизмов для работы в условиях динамически изменяемой загруженности каналов связи, когда эффективное число агентов в MAC может варьироваться в широких диапазонах.

Вклад авторов

М.О. Таныгин – разработка концепции, разработка методологии, утверждение окончательного варианта.

И.О. Мишин – проведение исследования, написание черновика, подготовка и редактирование текста.

Е.А. Кулешова – проведение исследования, проведение анализа данных, подготовка и редактирование текста.

А.В. Киселев – проведение исследования, проведение анализа данных.

Authors' contributions

M.O. Tanygin – concept development, methodology development, approval of the final version.

I.O. Mishin – conducting research, writing the draft, preparing and editing the text.

E.A. Kuleshova – conducting research, analyzing data, preparing and editing the text.

A.V. Kiselev – conducting research, analyzing data.

СПИСОК ЛИТЕРАТУРЫ

1. Öztürk G., Saran N., Doğanaksoy A. Modified Attribute-Based Authentication for Multi-Agent Systems. *Int. J. Inform. Security Sci.* 2023;12(3):1–13. https://doi.org/10.55859/ijiss.1294580
2. Кулешова Е.А., Марухленко А.Л., Добрица В.П., Таныгин М.О., Плугаторев А.В. Вариант алгоритма генерации псевдослучайных двоичных последовательностей, основанный на свойствах линейных клеточных автоматов. *Прикаспийский журнал: управление и высокие технологии.* 2021;54(2):62–70. https://doi.org/10.21672/2074-1707.2021.53.1.062-070
3. Таныгин М.О., Кулешова Е.А., Митрофанов А.В., Гладилина Е.Ю. Повышение скорости обнаружения ошибок при формировании цепочек блоков данных на основе анализа числа совпадений хешей. *Прикаспийский журнал: управление и высокие технологии.* 2022;1(57):85–93. https://doi.org/10.54398/2074-1707_2022_1_85
4. Yuan J., Yang J., Zhou S., Wang C. Efficient Group Authentication with Multiple Authentications on Resource-Limited Devices. *J. Supercomput.* 2025;81:929. https://doi.org/10.1007/s11227-025-07404-6
5. Gopirajan P.V., Mani K. Secure Multi-Authentication using BlockchainTechnology in Cloud based Internet of Things. *Telematique*. 2022;21(1):6640–6650.
6. Wee A.K., Chekole E.G., Zhou J. Excavating Vulnerabilities Lurking in Multi-Factor Authentication Protocols: A Systematic Security Analysis. *arXiv Cornell University*. 2024;2407(20459):1–24. https://doi.org/10.48550/arXiv.2407.20459
7. Chenchev I. Framework for Multi-factor Authentication with Dynamically Generated Passwords. In: Arai K. (Ed.). *Advances in Information and Communication. FICC 2023. Lecture Notes in Networks and Systems*. Springer; 2023. V. 652. P. 563–576. https://doi.org/10.1007/978-3-031-28073-3_39
8. Li H., Han D. Blockchain-assisted secure message authentication with reputation management for VANETs. *J. Supercomput.* 2023;79(17):19903–19933. https://doi.org/10.1007/s11227-023-05394-x
9. Xu Y., Jian X., Li T., Zou S., Li B. Blockchain-Based Authentication Scheme with an Adaptive Multi-Factor Authentication Strategy. *Mobile Inform. Syst.* 2023;2023:4764135. https://doi.org/10.1155/2023/4764135
10. Liu J., Mu Q., Che R., et al. Multi-participant quantum anonymous communication based on high-dimensional entangled states. *Physica Scripta*. 2024;99(9):095109. https://doi.org/10.1088/1402-4896/ad69d9
11. Кулешова Е.А., Таныгин М.О. Исследование характеристик современных генераторов псевдослучайных последовательностей. *Телекоммуникации*. 2023;7:28–39. https://doi.org/10.31044/1684-2588-2023-0-7-28-39

12. Таныгин М.О. Восстановление порядка следования информационных пакетов на основе анализа хеш-последовательностей. *Известия Юго-Западного государственного университета*. 2020;24(1):175–188.
13. Alamgir N., Negati S., Bright C. SHA-256 Collision Attack with Programmatic SAT. *arXiv Cornell University.* 2024;2406.20072. https://doi.org/10.48550/arXiv.2406.20072
14. Fang Y. A research on different digital signature schemes. *Appl. Comput. Eng.* 2023;16(1):27–35. http://doi.org/10.54254/2755-2721/16/20230855
15. Phatangare S., Jadhav S., Kawane S., Holkar P., Gaikwad P. Multi-Level Encryption System using AES and RSA Algorithms. *Int. J. Res. Appl. Sci. Eng. Technol.* 2024;15(5):4043–4051. https://doi.org/10.22214/IJRASET.2024.62420
16. Tanygin M.O., Alshaeaa H.Y., Kuleshova E.A. A method of the transmitted blocks information integrity control. *Radio Electronics, Computer Science, Control.* 2020;1:181–189.
17. Tao M., Li Q., Yu J. Multi-Objective Dynamic Path Planning with Multi-Agent Deep Reinforcement Learning. *J. Marin. Sci. Eng.* 2025;13(1):20. https://doi.org/10.3390/jmse13010020
18. Morais D., Zuquete A., Mendes A. Adaptive, Multi-Factor Authentication as a Service for Web Applications. In: *2023 7th Cyber Security in Networking Conference* (*CSNet*). 2023. P. 74–80. http://doi.org/10.1109/CSNet59123.2023.10339695
19. Плугатарев А.В. Модель определения источника сообщений на основе статистического анализа метаданных в открытом канале связи. *Прикаспийский журнал: управление и высокие технологии.* 2022;4(60):30–37.
20. Dharrao D., Gaikwad P., Gawai S.V., Bongale A.M., Patel K., Singh A. Classifying SMS as spam or ham: Leveraging NLP and machine learning techniques. *Int. J. Saf. Secur. Eng.* 2024;14(1):289–296. https://doi.org/10.18280/ijsse.140128
21. Placzek B. A Multi-Agent Prediction Method for Data Sampling and Transmission Reduction in Internet of Things Sensor Networks. *Sensors*. 2023;23(20):8478. https://doi.org/10.3390/s23208478
22. Vedmiediev D., Shapoval N. Text Message Clustering. *Electronics and Control Systems.* 2023;4(78):16–20.
23. Katwal S., Sharma N., Kumar K. A Deep Learning Approach for Throughput Enhanced Clustering and Spectrally Efficient Resource Allocation in Ultra-Dense Networks. *IEEE Trans. Netw. Service Manag*. 2025;22(1):582–591. https://doi.org/10.1109/TNSM.2024.3470235
24. Huang X., Zhou S. QMNet: Importance-Aware Message Exchange for Decentralized Multi-Agent Reinforcement Learning. *IEEE Trans. Mobile Comput*. 2023;23(5):4739–4751. https://doi.org/10.1109/TMC.2023.3296726
25. Головешкин В.А., Жукова Г.Н., Ульянов М.В., Фомичев М.И. Использование квантильных коэффициентов асимметрии и эксцесса для оценки сложности решения задачи коммивояжера. *Int. J. Open Inform. Technol.* 2016;4(12):7–12. https://elibrary.ru/xetabh
26. Таныгин М.О., Добрица В.П., Митрофанов А.В., Ахмат Х.И. Математическая интерпретация результатов когнитивного анализа метаданных сетевых пакетов. *Известия Юго-Западного государственного университета.* 2023;27(3):66–78.

REFERENCES

1. Öztürk G., Saran N., Doğanaksoy A. Modified Attribute-Based Authentication for Multi-Agent Systems. *Int. J. Inform. Security Sci.* 2023;12(3):1–13. https://doi.org/10.55859/ijiss.1294580
2. Kuleshova E.A., Maruhlenko A.L., Dobritsa V.P., Tanygin M.O., Plugatorev A.V. A variant of the algorithm for generating pseudorandom binary sequences based on the properties of linear cellular automata. *Prikaspiiskii zhurnal: upravlenie i vysokie tekhnologii = Caspian Journal: Control and High Technologies.* 2021;54(2):62–70 (in Russ.). https://doi.org/10.21672/2074-1707.2021.53.1.062-070
3. Tanygin M.O., Kuleshova E.A., Mitrofanov A.V., Gladilina E.U. Increasing the speed of error detection when forming data block chains based on the analysis of the number of hash matches. *Prikaspiiskii zhurnal: upravlenie i vysokie tekhnologii = Caspian Journal: Control and High Technologies.* 2022;1(57):85–93 (in Russ.). https://doi.org/10.54398/2074-1707_2022_1_85
4. Yuan J., Yang J., Zhou S., Wang C. Efficient Group Authentication with Multiple Authentications on Resource-Limited Devices. *J. Supercomput.* 2025;81:929. https://doi.org/10.1007/s11227-025-07404-6
5. Gopirajan P.V., Mani K. Secure Multi-Authentication using BlockchainTechnology in Cloud based Internet of Things. *Telematique*. 2022;21(1):6640–6650.
6. Wee A.K., Chekole E.G., Zhou J. Excavating Vulnerabilities Lurking in Multi-Factor Authentication Protocols: A Systematic Security Analysis. *arXiv Cornell University*. 2024;2407(20459):1–24. https://doi.org/10.48550/arXiv.2407.20459
7. Chenchev I. Framework for Multi-factor Authentication with Dynamically Generated Passwords. In: Arai K. (Ed.). *Advances in Information and Communication. FICC 2023. Lecture Notes in Networks and Systems*. Springer; 2023. V. 652. P. 563–576. https://doi.org/10.1007/978-3-031-28073-3_39
8. Li H., Han D. Blockchain-assisted secure message authentication with reputation management for VANETs. *J. Supercomput.* 2023;79(17):19903–19933. https://doi.org/10.1007/s11227-023-05394-x
9. Xu Y., Jian X., Li T., Zou S., Li B. Blockchain-Based Authentication Scheme with an Adaptive Multi-Factor Authentication Strategy. *Mobile Inform. Syst.* 2023;2023:4764135. https://doi.org/10.1155/2023/4764135
10. Liu J., Mu Q., Che R., et al. Multi-participant quantum anonymous communication based on high-dimensional entangled states. *Physica Scripta*. 2024;99(9):095109. https://doi.org/10.1088/1402-4896/ad69d9
11. Kuleshova E.A., Tanygin M.O. Study of characteristics of modern generators of pseudorandom sequences. *Telekommunikatsii = Telecommunications*. 2023;7:28–39 (in Russ.). https://doi.org/10.31044/1684-2588-2023-0-7-28-39
12. Tanygin M.O. Restoring the order of information packets based on hash sequence analysis. *Izvestiya Yugo-Zapadnogo gosudarstvennogo universiteta = Proceedings of the Southwest State University*. 2020;24(1):175–188 (in Russ.).

13. Alamgir N., Negati S., Bright C. SHA-256 Collision Attack with Programmatic SAT. *arXiv Cornell University.* 2024;2406.20072. https://doi.org/10.48550/arXiv.2406.20072
14. Fang Y. A research on different digital signature schemes. *Appl. Comput. Eng.* 2023;16(1):27–35. http://doi.org/10.54254/2755-2721/16/20230855
15. Phatangare S., Jadhav S., Kawane S., Holkar P., Gaikwad P. Multi-Level Encryption System using AES and RSA Algorithms. *Int. J. Res. Appl. Sci. Eng. Technol.* 2024;15(5):4043–4051. https://doi.org/10.22214/IJRASET.2024.62420
16. Tanygin M.O., Alshaeaa H.Y., Kuleshova E.A. A method of the transmitted blocks information integrity control. *Radio Electronics, Computer Science, Control.* 2020;1:181–189.
17. Tao M., Li Q., Yu J. Multi-Objective Dynamic Path Planning with Multi-Agent Deep Reinforcement Learning. *J. Marin. Sci. Eng.* 2025;13(1):20. https://doi.org/10.3390/jmse13010020
18. Morais D., Zuquete A., Mendes A. Adaptive, Multi-Factor Authentication as a Service for Web Applications. In: *2023 7th Cyber Security in Networking Conference* (*CSNet*). 2023. P. 74–80. http://doi.org/10.1109/CSNet59123.2023.10339695
19. Plugatarev A.V. Model for determining the message source by statistical analysis of metadata in an open communication channel. *Prikaspiiskii zhurnal: upravlenie i vysokie tekhnologii = Caspian Journal: Control and High Technologies.* 2022;4(60):30–37 (in Russ.).
20. Dharrao D., Gaikwad P., Gawai S.V., Bongale A.M., Patel K., Singh A. Classifying SMS as spam or ham: Leveraging NLP and machine learning techniques. *Int. J. Saf. Secur. Eng.* 2024;14(1):289–296. https://doi.org/10.18280/ijsse.140128
21. Placzek B. A Multi-Agent Prediction Method for Data Sampling and Transmission Reduction in Internet of Things Sensor Networks. *Sensors*. 2023;23(20):8478. https://doi.org/10.3390/s23208478
22. Vedmiediev D., Shapoval N. Text Message Clustering. *Electronics and Control Systems.* 2023;4(78):16–20.
23. Katwal S., Sharma N., Kumar K. A Deep Learning Approach for Throughput Enhanced Clustering and Spectrally Efficient Resource Allocation in Ultra-Dense Networks. *IEEE Trans. Netw. Service Manag*. 2025;22(1):582–591. https://doi.org/10.1109/TNSM.2024.3470235
24. Huang X., Zhou S. QMNet: Importance-Aware Message Exchange for Decentralized Multi-Agent Reinforcement Learning. *IEEE Trans. Mobile Comput*. 2023;23(5):4739–4751. https://doi.org/10.1109/TMC.2023.3296726
25. Goloveshkin V.A., Zhukova G.N., Ulyanov M.V., Fomichev M.I. The estimation of the complexity of solving a particular travelling salesman problem by quantile-based measures for skewness and kurtosis. *Int. J. Open Inform. Technol.* 2016;4(12):7–12 (in Russ.). https://elibrary.ru/xetabh
26. Tanygin M.O., Dobritsa V.P., Mitrofanov A.V., Ahmat Kh.I. Mathematical interpretation of the results of cognitive analysis of network packets metadata. *Izvestiya Yugo-Zapadnogo gosudarstvennogo universiteta = Proceedings of the Southwest State University*. 2023;27(3):66–78 (in Russ.).

Об авторах

Таныгин Максим Олегович, д.т.н., доцент, декан факультета фундаментальной и прикладной информатики, ФГБОУ ВО «Юго-Западный государственный университет» (305040, Россия, Курск, ул. 50 лет Октября, д. 94). E-mail: tanygin@yandex.ru. Scopus Author ID 19640649200, ResearcherID N-7689-2016, SPIN-код РИНЦ 2639-4800, https://orcid.org/0000-0002-4099-1414

Мишин Илья Олегович, аспирант, кафедра информационной безопасности, ФГБОУ ВО «Юго-Западный государственный университет» (305040, Россия, Курск, ул. 50 лет Октября, д. 94). E-mail: mishin.ilya46@yandex.ru. ResearcherID MXJ-7912-2025, SPIN-код РИНЦ 6911-3642, https://orcid.org/0009-0006-8883-1731

Кулешова Елена Александровна, к.т.н., доцент, кафедра информационной безопасности, ФГБОУ ВО «Юго-Западный государственный университет» (305040, Россия, Курск, ул. 50 лет Октября, д. 94). E-mail: lena.kuleshova.94@mail.ru. Scopus Author ID 57216349335, ResearcherID AAI-9214-2021, SPIN-код РИНЦ 9607-8582, https://orcid.org/0000-0002-8270-564X

Киселев Алексей Викторович, к.т.н., доцент, кафедра вычислительной техники, ФГБОУ ВО «Юго-Западный государственный университет» (305040, Россия, Курск, ул. 50 лет Октября, д. 94). E-mail: kiselevalexey1990@gmail.com. Scopus Author ID 57337411000, ResearcherID S-9914-2018, SPIN-код РИНЦ 2016-7550, https://orcid.org/0000-0001-7228-0281

About the Authors

Maxim O. Tanygin, Dr. Sci. (Eng.), Associate Professor, Dean of the Faculty of Fundamental and Applied Informatics, Southwest State University (94, 50 Let Oktyabrya ul., Kursk, 305040 Russia). E-mail: tanygin@yandex.ru. Scopus Author ID 19640649200, ResearcherID N-7689-2016, RSCI SPIN-code 2639-4800, https://orcid.org/0000-0002-4099-1414

Ilya O. Mishin, Postgraduate Student, Department of Information Security, Southwest State University (94, 50 Let Oktyabrya ul., Kursk, 305040 Russia). E-mail: mishin.ilya46@yandex.ru. ResearcherID MXJ-7912-2025, RSCI SPIN-code 6911-3642, https://orcid.org/0009-0006-8883-1731

Elena A. Kuleshova, Cand. Sci. (Eng.), Associate Professor, Department of Information Security, Southwest State University (94, 50 Let Oktyabrya ul., Kursk, 305040 Russia). E-mail: lena.kuleshova.94@mail.ru. Scopus Author ID 57216349335, ResearcherID AAI-9214-2021, RSCI SPIN-code 9607-8582, https://orcid.org/0000-0002-8270-564X

Alexey V. Kiselev, Cand. Sci. (Eng.), Associate Professor, Computer Engineering Department, Southwest State University (94, 50 Let Oktyabrya ul., Kursk, 305040 Russia). E-mail: kiselevalexey1990@gmail.com. Scopus Author ID 57337411000, ResearcherID S-9914-2018, RSCI SPIN-code 2016-7550, https://orcid.org/0000-0001-7228-0281