Оригинальная статья / Original article

https://doi.org/10.21869/2223-1536-2025-15-1-8-20

УДК 004.052

Оптимизация параметров классификатора при обработке статистических характеристик метаданных сетевых пакетов

М. О. Таныгин[1], В. П. Добрица[1], А. В. Митрофанов[1] ✉, Хауа Ибрахим Ахмат[1]

[1] Юго-Западный государственный университет
ул. 50 лет Октября, д. 94, г. Курск 305040, Российская Федерация

✉ e-mail: mitro3000@rambler.ru

Резюме

Цель исследования. *В статье рассматривается возможность повышения вероятности корректной аутентификации удалённого источника сообщений на основе анализа метаданных формируемых им сетевых пакетов. Целью данного исследования является разработка метода классификации аутентичных сетевых пакетов на основе анализа статистических характеристик времени поступления пакетов и оптимизация параметров классификатора для достижения максимальной точности определения аутентичных последовательностей пакетов.*

Методы. *В исследовании применены методы анализа высокопорядковых моментов межпакетных интервалов, а также логистическая регрессия для классификации пакетов. Использованы параметры эксцесса и асимметрии, вычисляемые на основе выборок временных интервалов, образованных приходом пакетов. Разработан классификатор, основанный на минимизации расстояния от пар значений (коэффициентов асимметрии и эксцесса) до параболы, соответствующей распределению Пуассона.*

Результаты. *Были сформированы выборки мощностью 10^4 с рассчитанными парами коэффициентов эксцесса и асимметрии. Полученные результаты показывают, что для максимально возможной точности классификации (82-84%) оптимальные параметры параболы составляют: a ≈ 1,0, c = 8–9. ROC-кривые анализировались для различных наборов параметров, что подтвердило линейность зависимости доли верноположительных результатов от доли ложноположительных.*

Заключение. *Результаты исследования подтвердили возможность повышения надежности аутентификации сетевых пакетов путем использования высокопорядковых моментов данных о временных интервалах, что демонстрирует эффективность предложенного метода. Основные выводы включают необходимость тщательной настройки параметров классификатора для оптимизации процесса аутентификации. Поскольку предложенный метод проявляет высокую чувствительность к изменениям в распределениях, это открывает новые направления для дальнейшего исследования в области защиты беспроводных сетей.*

Ключевые слова: *обработка данных; аутентификация; коэффициент эксцесса; коэффициент асимметрии; имитационное моделирование; сетевые пакеты; межпакетные интервалы.*

Конфликт интересов: *Автор декларирует отсутствие явных и потенциальных конфликтов интересов, связанных с публикацией настоящей статьи.*

Для цитирования: Оптимизация параметров классификатора при обработке статистических характеристик метаданных сетевых пакетов / М. О. Таныгин, В. П. Добрица, А. В. Митрофанов, Хауа Ибрахим Ахмат // Известия Юго-Западного государственного университета. Серия: Управление, вычислительная техника, информатика. Медицинское приборостроение. 2025. Т. 15, № 1. С. 8–20. https://doi.org/10.21869/ 2223-1536-2025-15-1-8-20

Поступила в редакцию 11.01.2025 *Подписана в печать 10.02.2025* *Опубликована 31.03.2025*

Optimization of classifier parameters when processing statistical characteristics of network packet metadata

Maxim O. Tanygin[1], Vyacheslav P. Dobritsa[1], Aleksey V. Mitrofanov[1] ✉, Khaua Ibrahim Ahmat[1]

[1] Southwest State University
50 Let Oktyabrya Str. 94, Kursk 305040, Russian Federation

✉ e-mail: mitro3000@rambler.ru

Abstract

Purpose of research. *The article considers the possibility of increasing the probability of correct authentication of a remote message source based on the analysis of metadata of the network packets it generates. The purpose of this purpose is to develop a method for classifying authentic network packets based on the analysis of statistical characteristics of the packet arrival time and to optimize the classifier parameters to achieve maximum accuracy in determining authentic packet sequences.*

Methods. *The study applies methods of analyzing high-order moments of interpacket intervals, as well as logistic regression for classifying packets. The parameters of excess and asymmetry calculated based on samples of time intervals formed by the arrival of packets are used. A classifier based on minimizing the distance from pairs of values (asymmetry and excess coefficients) to a parabola corresponding to the Poisson distribution is developed.*

Results. *Samples with a power of 10^4 with calculated pairs of excess and asymmetry coefficients were formed. The obtained results show that for the maximum possible classification accuracy (82-84%), the optimal parabola parameters are: $a \approx 1.0$, $c = 8–9$. ROC curves were analyzed for different sets of parameters, which confirmed the linearity of the dependence of the proportion of true positive results on the proportion of false positives.*

Conclusion. *The results of the study confirmed the possibility of increasing the reliability of network packet authentication by using high-order moments of time interval data, which demonstrates the effectiveness of the proposed method. The main conclusions include the need for careful tuning of the classifier parameters to optimize the authentication process. Since the proposed method exhibits high sensitivity to changes in distributions, this opens up new directions for further research in the field of wireless network security.*

Keywords: *data processing; authentication; kurtosis coefficient; skewness coefficient; simulation modeling; network packets; interpacket intervals.*

Conflict of interest: *The Authors declares the absence of obvious and potential conflicts of interest related to the publication of this article.*

For citation: Tanygin M.O., Dobritsa V.P., Mitrofanov A.V., Khaua Ibrahim Ahmat. Optimization of classifier parameters when processing statistical characteristics of network packet metadata. *Izvestiya Yugo-Zapadnogo gosudarstvennogo*

universiteta. Serija: Upravlenie, vychislitel'naja tekhnika, informatika. Meditsinskoe priborostroenie = Proceedings of the Southwest State University. Series: Control, Computer Engineering, Information Science. Medical Instruments Engineering. 2025;15(1):8–20. (In Russ.) https://doi.org/10.21869/2223-1536-2025-15-1-8-20

Received 11.01.2025 *Accepted 10.02.2025* *Published 31.03.2025*

Введение

Классическим способом аутентификации источников сетевых пакетов является внедрение кодов аутентификации сообщений или имитовставок в заголовки пакетов. Отправитель создает пакет данных и на основе его содержания генерирует имитовставку. Приемник, в свою очередь, анализирует полученный пакет и соответствующую имитовставку, определяя, является ли отправитель носителем идентификатора сеанса.

В целом вероятность преодоления имитозащиты или ошибок первого рода в процессе аутентификации зависит от разрядности кода аутентификации [1]. Однако, когда возникает необходимость уменьшения объема передаваемых данных [2], ограниченные размеры имитовставки [3] могут не позволить достичь необходимой вероятности ошибки [4]. Это приводит к необходимости применения алгоритмов аутентификации [5], построенных на принципах сцепления блоков [6], которые при одинаковом размере имитовставки обеспечивают меньшую вероятность ошибок [7], но требуют больше вычислительных ресурсов [8]. Для различных систем связи и протоколов важной становится задача уменьшения размера заголовков из-за ограничений на размеры передаваемых пакетов данных [9]. Другим подходом к повышению достоверности аутентификации является использование метаинформации[1]. Это информация, которую приемник может получить из факта получения пакета или нескольких пакетов, включая размеры дополнительной информации [10], передаваемой по альтернативным каналам, статистические характеристики сигнала в канале связи, время получения пакетов и пространственное расположение источников данных [11].

Наиболее перспективным представляется анализ времени прихода пакетов, так как каждый протокол передачи имеет свои распределения между пакетными интервалами. Это в сочетании с методами контроля аутентичности позволяет разработать критерии для выделения аутентичных пакетов, даже если анализ кодов аутентификации сообщений не позволяет этого [12]. При этом следует исследовать не только сами значения межпакетных интервалов, а также моменты этих значений как более информативные параметры [13].

В предложенном методе анализа высокопорядковых моментов для небольших выборок межпакетных интервалов

[1] Пат. 2233045 C2 Российская Федерация, МПК H04J 13/00, H04B 1/707, H04L 1/00. Способ и устройство высокоскоростной передачи пакетных данных / Падовани Р., Синдхушаяна Н. Т., Витли Ч. Е. [и др.]. № 2000114194/09; заявл. 03.11.1998; опубл. 20.07.04.

времени [10] применялся подход, подробно описанный в работе [14], в которой коэффициенты асимметрии и эксцесса для каждой выборки размещались на координатной плоскости, и анализировались зависимости между этими параметрами. Для моделирования передачи данных в сетях LoRaWAN использовалась модифицированная модель, которая учитывала применение кодирования с сцеплением блоков для аутентификации. В результате последовательности сообщений от источника к приемнику дают возможность использовать дополнительную метаинформацию для повышения надежности аутентификации – временные интервалы между получением сообщений. Для выборок, построенных на таких временных интервалах, вычислялись коэффициенты асимметрии и эксцесса. В ходе анализа различий распределений малых выборок, представляющих межпакетные интервалы при поступлении пакетов, наиболее информативными оказались моменты высоких порядков, которые, в отличие от низкопорядковых, более чувствительны к незначительным отклонениям в распределениях выборок. При возникновении ошибок аутентификации значения времени поступления пакета, вызвавшего конфликт среди кодов аутентификации сообщений, меняют два временных интервала в выборке, соответствующей последовательности аутентичных сообщений. Это создает отличия в картах коэффициентов асимметрии и эксцесса для выборок, образованных интервалами между приходом аутентичных пакетов и для последовательностей, включающих пакеты от сторон их источников.

В настоящей работе мы рассматриваем подход, основанный на анализе статистических характеристик времени поступления сетевых пакетов в приёмник. Как показали исследования, использование моментов высоких порядков позволяет выявлять отличия в законах распределения выборок размером 10–20 элементов. Отличия в законах распределения возникают, когда в последовательности сетевых пакетов происходит коллизия кодов аутентификации и формируются две последовательности межпакетных интервалов [15], отличающиеся двумя элементами: межпакетными интервалам до и после сетевого пакета, в котором возникла коллизия [16].

Используемое решение, основанное на анализе коэффициентов эксцесса и асимметрии двух выборок, сводит задачу разделения двух множеств точек (рис. 1): множество значений коэффициентов эксцесса и асимметрии для межпакетных интервалов в последовательности аутентичных сетевых пакетов (синие точки) и аналогичное множество для последовательностей, содержащих в произвольной позиции один посторонний пакет (красные плюсы). Причём на входе классификатора будет две пары параметров, и классификатор должен выдать «1», если первая пара относится к аутентичной последовательности, и «0» – в противном случае [17].

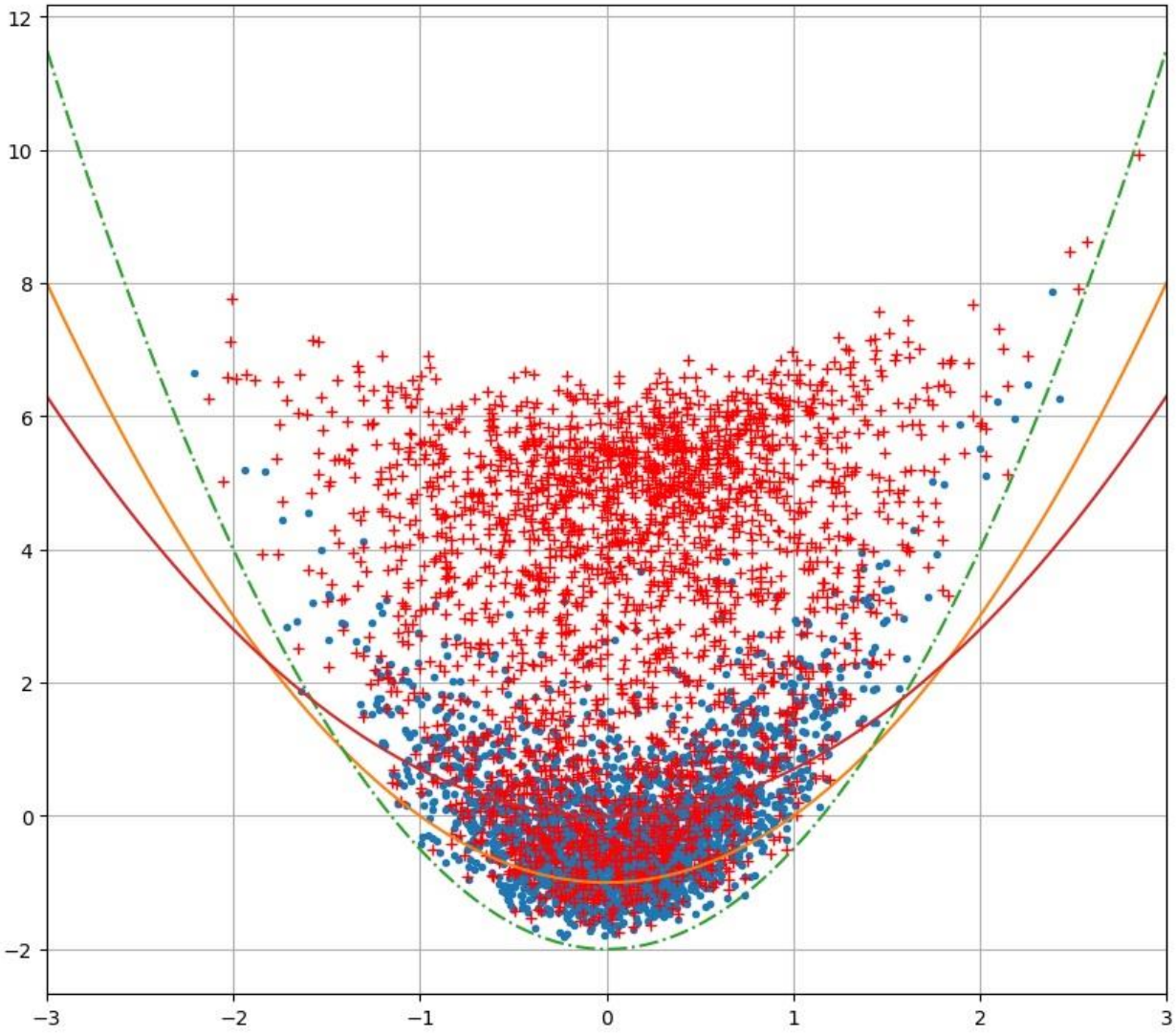

Рис. 1. Карты коэффициентов эксцесса и асимметрии для множества выборок, образованных интервалами между временем поступления пакетов данных: красные плюсы – значения коэффициентов для выборок, содержащих посторонние пакеты; синие точки – значения коэффициентов для выборок, состоящих полностью из аутентичных пакетов

Fig. 1. Maps of the kurtosis and asymmetry coefficients for a set of samples formed by intervals between the arrival times of data packets: red pluses are the coefficient values for samples containing extraneous packets; blue dots are the coefficient values for samples consisting entirely of authentic packets

Известные методы машинного обучения, такие как метод k ближайших соседей, метод сегментации и др. [18], для данных множеств не подходят, так как два множества в общем случае обладают достаточно значительным пересечением на карте коэффициентов эксцесса и асимметрии [19].

В работе [20] исследовался классификатор, в основе которого лежит расстояние до параболы. Парабола в качестве кривой выбрана неслучайно, а потому, что для распределения Пуассона, которое наиболее точно описывает распределение межпакетных временных интервалов, зависимость между коэффи-

циентом эксцесса и коэффициентом асимметрии квадратичная. В исследовании использовалось уравнение параболы $E = A^2$, тогда как даже поверхностный анализ размещения точек на карте позволяет сказать, что форма параболы может оказать существенное влияние на качество классификатора, в основе которого лежит расстояние от точек на карте до указанной кривой (рис. 1). Целью настоящего исследования является определение параметров (уравнения) кривой, используемой при классификации пары значений коэффициентов, при которых достигается максимальная точность классификации и достоверности определения аутентичных пакетов данных.

Материалы и методы

В качестве исходных данных классификатор получает четыре параметра: две пары значений (A_1, E_1) и (A_2, E_2). Как параметры обработки данных мы используем коэффициенты a и c уравнения параболы $E = a \cdot A^2 - c$. Симметричная относительно оси ординат картина значений коэффициентов эксцесса и асимметрии (рис. 1) позволяет использовать симметричную относительно оси ординат параболу с нулевым коэффициентом при множителе A. На основе полученных в [21] формул для расстояния от параболы формируем две метрики для каждой пары значений:

$$D_i = \left(Q - A_i\right)^2 + \left(a^2Q^2 - E_i + c\right)^2,$$

$$Q = \left(\frac{1}{4a^2} A_i + \left(\left(\frac{1 - 2a^2\left(-c - E_i\right)}{2a^4} \right)^3 + \frac{1}{4}\left(A_i\right)^2 \right)^{\frac{1}{2}} \right)^{\frac{1}{3}} + \tag{1}$$

$$+ \left(\frac{1}{4a^2} A_i - \left(\left(\frac{1 - 2a^2\left(-c - E_i\right)}{2a^4} \right)^3 + \frac{1}{4}\left(A_i\right)^2 \right)^{\frac{1}{2}} \right)^{\frac{1}{3}}, i = 1, 2.$$

Результаты и их обсуждение

На основе описанных в [21] моделей были сформированы выборки мощностью 10^4 последовательностей каждого типа, для которых рассчитаны 10^4 пар значений (A_1, E_1) и (A_2, E_2). Далее для каждой пары значений a и c рассчитаны 10^4 значений D_1 и D_2. Тогда задача классификации состоит в получении функции f, такой, что $f(D_1, D_2) = 1$, $f(D_2, D_1) = 0$. Для построения данной функции использовали логистическую регрессию. Характеристикой классификатора, которая может быть использована для настройки классификатора для решения частных задач, является ROC-кривая.

На рисунке 2 представлены данные характеристики для нескольких наборов параметров a и c.

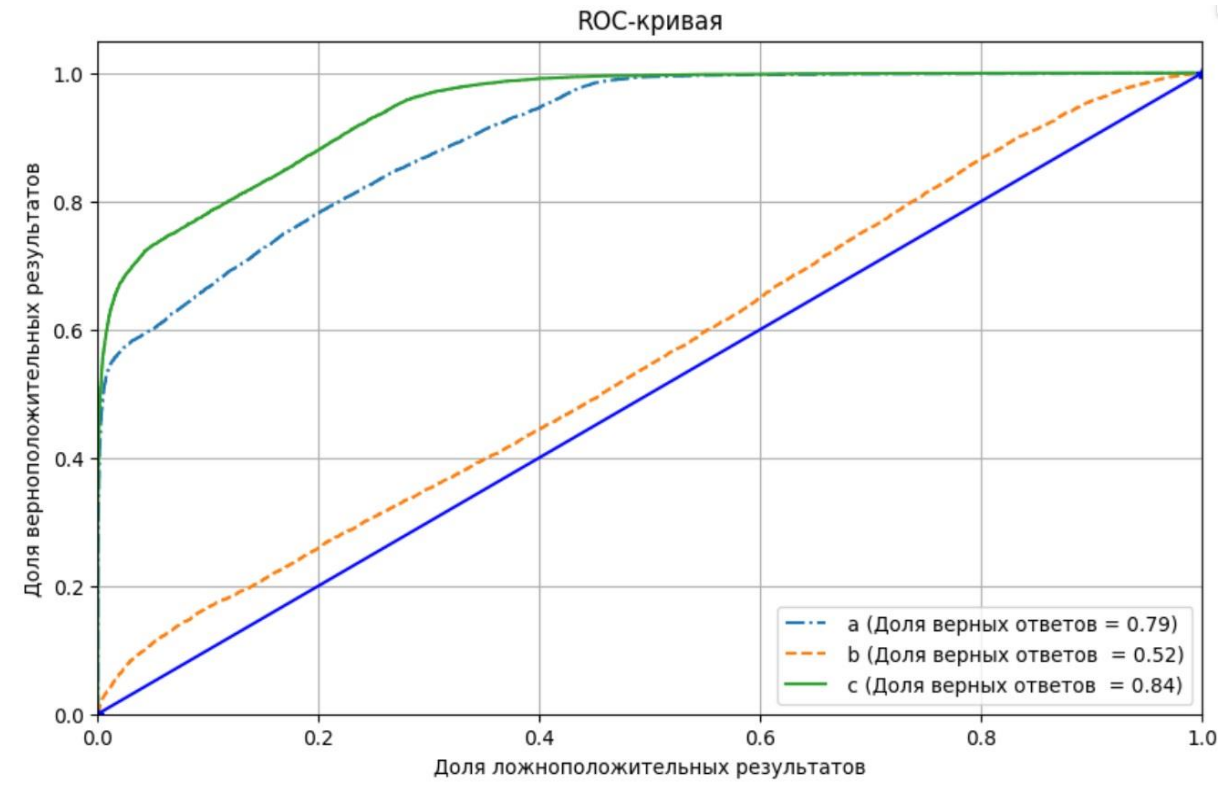

Рис. 2. ROC-кривая для метода классификации сетевых пакетов на основе расстояния от параболы при различных параметрах уравнения параболы: a – *a* = 1,2, *c*= –3; b – *a* = 0,7, *c* = 0; c – *a* = 1, *c* = –6.

Fig. 2. ROC curve for the distance-from-parabola network packet classification method with different parameters of the parabola equation: a – *a* = 1,2, *c* = –3; b – *a* = 0,7, *c* = 0; c – *a* = 1, *c* = –6

Форма ROC-кривой позволяет её достаточно легко аппроксимировать прямой, так как зависимость доли верноположительных результатов от доли ложноположительных результатов практически линейна. Площадь под ROC-кривой, интерпретируемая как процент верных ответов, находится в прямой зависимости от доли верноположительных результатов при фиксированном значении ложноположительных результатов

Поэтому на втором этапе исследования мы определяли зависимость данного показателя классификатора от параметров *a* и *c* обработки значений коэффициентов эксцесса и асимметрии (рис. 3).

Параметр a варьировался в диапазоне от 0,5 до 1,2, параметр *c* – в диапазон от –2 до 10. Градиентная диаграмма на рисунке 3 полученных результатов позволяет сделать вывод о том, что целесообразные значения параметров *a* и *c*, при которых точность рассматриваемого метода определения последовательности от целевого источника максимальна, равны: $a \approx 1{,}0$, $c = 8$–9. При этом точность классификации (достоверность аутентификации) находится в диапазоне 82–84%.

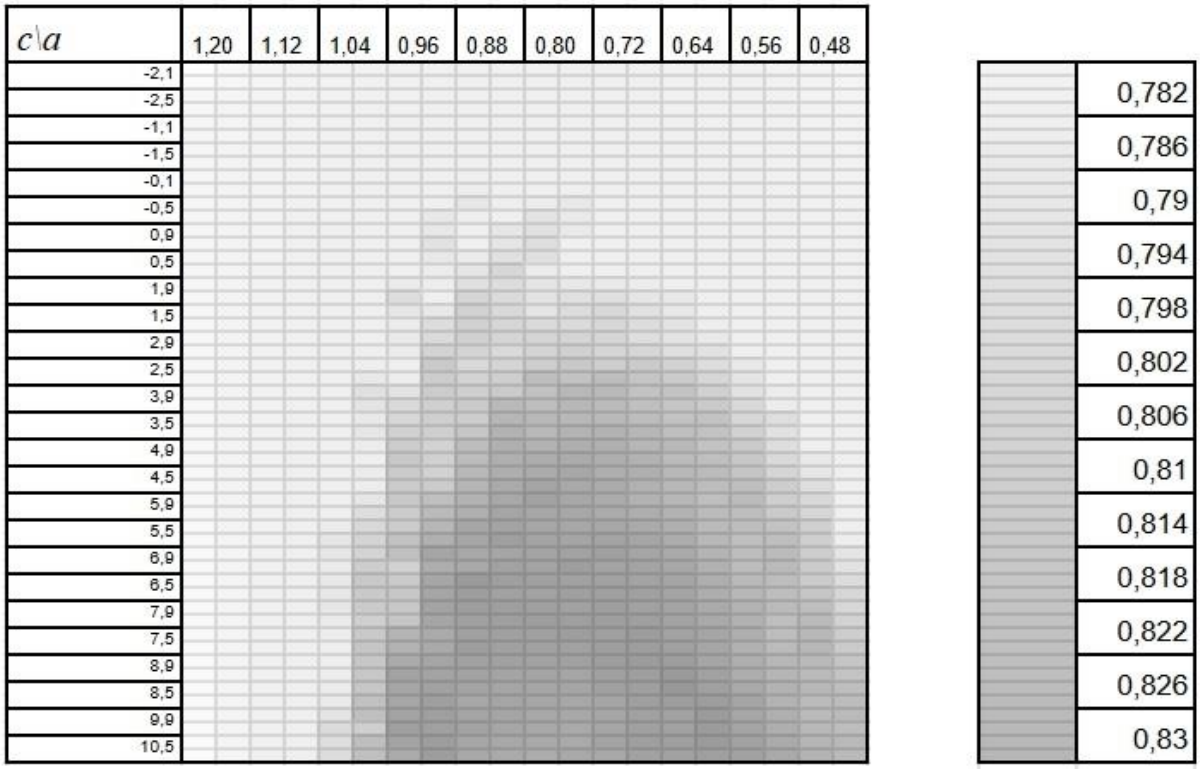

Рис. 3. Диаграмма зависимости доли верных ответов в зависимости от параметров обработки сообщений *a*, *c*.

Fig. 3. Diagram of the dependence of the proportion of correct answers on the parameters of message processing *a*, *c*.

Объяснением такого значения параметра *c*, которое соответствует параболе, достаточно сильно смещённой вниз по оси ординат относительно основного облака значений коэффициентов эксцесса и асимметрии, может быть объяснено тем, что пары значений пар значений (A_1, E_1) и (A_2, E_2) при значений $-1 < A_1 < 1$, $-2 < E_1 < 2$ расположены очень близко друг к другу. При значении $c = 0$ это создаст ошибку классификации, так как минимум расстояния будет рассчитываться до ветвей параболы, находящихся в диапазоне точка $|A_1| > 0{,}5$, и даже незначительное изменение коэффициента асимметрии может компенсировать значительное изменение коэффициента эксцесса. В случае же $c = 9$ минимум расстояния будет рассчитываться до окрестности нижней точки параболы, и влиять на значение данного минимума будет коэффициент эксцесса. Данное наблюдение порождает гипотезу о возможности построения классификатора, основанного на минимуме расстояния не до параболы (как кривой, характерной для распределения Пуассона), а до некоторой точки на карте коэффициентов эксцесса и асимметрии. Это позволило бы отказаться от вычисления корней кубического уравнения и значительно упростить вычислительный процесс нахождения минимума расстояния. Но проверка данной гипотезы выходит за рамки настоящей работы и является перспективным направлением исследования

возможности аутентификации в беспроводных сетях связи по значениям межпакетного интервала времени

Выводы

В данном исследовании был предложен новый метод классификации сетевых пакетов, основанной на анализе статистических характеристик времени их поступления. Улучшение надежности аутентификации в беспроводных сетях достигается за счет использования высокопорядковых моментов, которые позволяют выявлять различия в распределениях межпакетных интервалов. Эффективность предложенного подхода продемонстрирована на примере применения логистической регрессии и классификатора, опирающегося на минимизацию расстояния до кривой. Оптимальные параметры, полученные в ходе экспериментов, обеспечивают точность классификации в диапазоне 82–84%.

Результаты показывают, что интеграция временной информации и характеристик асимметрии и эксцесса значительно повышает возможность корректной идентификации аутентичных пакетов даже в условиях коллизий кодов аутентификации. Это открывает новые перспективы для применения в области сетевой безопасности и аутентификации в рамках современных протоколов связи.

Исследование подтверждает, что метаинформация, извлекаемая из временных интервалов между пакетами, может служить ценным дополнением к традиционным методам аутентификации, создавая более гибкие и надежные системы защиты. Данный подход может быть адаптирован для различных типов беспроводных сетей, что делает его перспективным направлением для дальнейших исследований и внедрений в практику.

Список литературы

1. Biswajit P. An Overview of LoRaWAN // WSEAS Transactions on communications. 2021. N 19. P. 231–239. https://doi.org/10.37394/23204.2020.19

2. Myung L. IEEE 802.15.5 WPAN mesh standard-low rate part: Meshing the wireless sensor networks // IEEE Journal on Selected Areas in Communications. 2010. N 28(7). P. 973–983. https://doi.org/10.1109/JSAC.2010.100902

3. Таныгин М. О., Гончаров А. С. Исследование характеристик сетей LoRaWAN // Телекоммуникации. 2023. № 3. С. 32–39. https://doi.org/10.31044/1684-2588-2023-0-3-32-39

4. A tutorial on IEEE 802.11ax high efficiency WLANs / E. Khorov, A. Kiryanov, A. Lyakhov, G. Bianchi // IEEE Communications Surveys and Tutorials. 2019. Vol. 21, N 1. P. 197–216. https://doi.org/10.1109/COMST.2018.2871099

5. Ferguson N., Schneier B., Kohno T. Block Cipher Modes // Cryptography Engineering: Design Principles and Practical Applications. Indianapolis: Wiley Publishing Inc., 2015. P. 63–76. https://doi.org/10.1002/9781118722367.ch4

6. Binoy K. R. Cybersecurity: Fast Encryption Cipher Block Chaining Mode (FCBC Mode) for Time Series Data // Journal of Mathematical & Computer Applications. 2024. Vol. 3(2). P. 1–3. https://doi.org/10.47363/JMCA/2024(3)E128

7. Lixiang L. An efficient secure data transmission and node authentication scheme for wireless sensing networks // Journal of Systems Architecture. 2022. N 133(4). P. 102760. https://doi.org/0.1016/j.sysarc.2022.102760

8. Bo Liang, Wenling Wu, Liting Zhang. BCBC: A More Efficient MAC Algorithm // Information Security Practice and Experience: 7th International Conference. Guangzhou, China. 2011. Berlin: Springer, 2011. https://doi.org/10.1007/978-3-642-21031-0_18

9. Никешин А. В., Шнитман В. З. Обзор расширяемого протокола аутентификации и его методов // Труды Института системного программирования РАН. 2018. Т. 30, вып. 2. С. 113–148. https://doi.org/10.15514/ISPRAS-2018-30(2)-7

10. 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). С. 30–37. https://doi.org/10.54398/20741707_2022_4_30

11. Таныгин М. О. Восстановление порядка следования информационных пакетов на основе анализа хеш-последовательностей // Известия Юго-Западного государственного университета. 2020. Т. 24, № 1. С. 175–188. https://doi.org/10.21869/2223-1560-2020-24-1-175-188

12. Plugatarev A. V., Tanygin M. O. Model for Determining the Message Source by Analyzing Their Arrival Time // 2022 International Russian Automation Conference (RusAutoCon). Sochi, 2022. P. 388–392. https://doi.org/10.1109/RusAutoCon54946.2022.9896326

13. Таныгин М. О., Митрофанов А. В., Плугатарев А. В. Использование статистических характеристик потоков сообщений для повышения достоверности аутентификации их источника // Телекоммуникации. 2023. № 2. С. 2–8. https://doi.org/10.31044/1684-2588-2023-0-2-2-8

14. Жукова Г. Н. Карта коэффициентов асимметрии и эксцесса в преподавании теории вероятностей и математической статистики // Научно-методический электронный журнал Концепт. 2015. № 8. С. 56–60.

15. Орлов А. И. Система моделей и методов проверки однородности двух независимых выборок // Политематический сетевой электронный научный журнал Кубанского государственного аграрного университета. 2020. № 157. С. 145–169. https://doi.org/10.21515/1990-4665-157-012

16. Орлов А. И. О методах проверки однородности двух независимых выборок // Заводская лаборатория. Диагностика материалов. 2020. Т. 86, № 3. С. 67–76. https://doi.org/10.26896/1028-6861-2020-86-3-67-76

17. Жукова Г. Н. Идентификация распределения по коэффициентам асимметрии и эксцесса // Автоматизация. Современные технологии. 2016. № 5. С. 26–33.

18. Керимов К. Ф., Азизова З. И. Анализ трафика сети с применением алгоритмов машинного обучения в автоматизированной информационной системе быстрого реагирования на инциденты информационной безопасности и фильтрации трафика сети // Электронный научный журнал «Потомки Аль-Фаргани» Ферганского филиала ТАТУ имени Мухаммада Аль-Хоразми. 2024. Т. 1, № 2. С. 281–285.

19. Костин Д. В., Шелухин О. И. Сравнительный анализ алгоритмов машинного обучения для проведения классификации сетевого зашифрованного трафика // T-Comm – Телекоммуникации и транспорт. 2016. Т. 10, № 9. С. 43–52.

20. Математическая интерпретация результатов когнитивного анализа метаданных сетевых пакетов / М. О. Таныгин, В. П. Добрица, А. В. Митрофанов, Х. И. Ахмат // Известия Юго-Западного государственного университета. 2023. Т. 27, № 3. С. 66–78. https://doi.org/10.21869/2223-1560-2023-27-3-66-78

References

1. Biswajit P. An Overview of LoRaWAN. *WSEAS Transactions on Communications*. 2021;(19):231–239. https://doi.org/10.37394/23204.2020.19

2. Myung L. IEEE 802.15.5 WPAN mesh standard-low rate part: Meshing the wireless sensor networks. *IEEE Journal on Selected Areas in Communications*. 2010;(28):973–983. https://doi.org/10.1109/JSAC.2010.100902

3. Tanygin M.O., Goncharov A.S. Investigation of the characteristics of LoRaWAN networks. *Telekommunikatsii = Telecommunications*. 2023;(3):32–39. (In Russ.) https://doi.org/10.31044/1684-2588-2023-0-3-32-39

4. Khorov E., Kiryanov A., Lyakhov A., Bianchi G. A tutorial on IEEE 802.11ax high efficiency WLANs. *IEEE Communications Surveys and Tutorials*. 2019;21(1):197–216. https://doi.org/10.1109/COMST.2018.2871099

5. Ferguson N., Schneier B., Kohno T. Block Cipher Modes. Cryptography Engineering: Design Principles and Practical Applications. Indianapolis: Wiley Publishing Inc.; 2015. P. 63–76. https://doi.org/10.1002/9781118722367.ch4

6. Binoy K.R. Cybersecurity: Fast Encryption Cipher Block Chaining Mode (FCBC Mode) for Time Series Data. *Journal of Mathematical & Computer Applications*. 2024;3:1–3. https://doi.org/10.47363/JMCA/2024(3)E128

7. Lixiang L. An efficient secure data transmission and node authentication scheme for wireless sensing networks. *Journal of Systems Architecture*. 2022;(133):102760. https://doi.org/ 0.1016/j.sysarc.2022.102760

8. Bo Liang, Wenling Wu, Liting Zhang. BCBC: A More Efficient MAC Algorithm. In: *Information Security Practice and Experience: 7th International Conference*. *2011. Guangzhou, China*. Berlin: Springer; 2011. https://doi.org/10.1007/978-3-642-21031-0_18

9. Nikeshin A.V., Shnitman V.Z. Review of the extensible authentication protocol and its methods. *Trudy Instituta sistemnogo programmirovaniya RAN = Proceedings of the Institute of System Programming of the Russian Academy of Sciences*. 2018;30(2):113–148. (In Russ.) https://doi.org/10.15514/ISPRAS-2018-30(2)-7

10. Plugatarev A.V. A model for determining the source of messages based on statistical analysis of metadata in an open communication channel. *Prikaspiiskii zhurnal: upravlenie i vysokie tekhnologii = Caspian Journal: Management and High Technologies*. 2022;4:30–37. (In Russ.) https://doi.org/10.54398/20741707_2022_4_30

11. Tanygin M.O. Restoring the order of information packets based on the analysis of hash sequences. *Izvestiya Yugo-Zapadnogo gosudarstvennogo universiteta = Proceedings of the Southwest State University*. 2020;24(1):175–188. (In Russ.) https://doi.org/10.21869/2223-1560-2020-24-1-175-188

12. Plugatarev A.V., Tanygin M.O. Model for Determining the Message Source by Analyzing Their Arrival Time. In: *2022 International Russian Automation Conference* (*RusAutoCon*). Sochi; 2022. P. 388–392. https://doi.org/10.1109/RusAutoCon54946.2022.9896326

13. Tanygin M.O., Mitrofanov A.V., Plugatarev A.V. Using statistical characteristics of message flows to increase the reliability of their source authentication. *Telekommunikatsii = Telecommunications*. 2023;(2):2–8. (In Russ.) https://doi.org/10.31044/1684-2588-2023-0-2-2-8

14. Zhukova G.N. Map of coefficients of asymmetry and excess in teaching probability theory and mathematical statistics. *Nauchno-metodicheskii elektronnyi zhurnal Kontsept = Scientific and Methodological Electronic Journal Concept*. 2015;(8):56–60. (In Russ.)

15. Orlov A.I. A system of models and methods for checking the uniformity of two independent samples. *Politematicheskii setevoi elektronnyi nauchnyi zhurnal Kubanskogo gosudarstvennogo agrarnogo universiteta = Polythematic Online Electronic Scientific Journal of the Kuban State Agrarian University*. 2020;(157):145–169. (In Russ.) https://doi.org/10.21515/1990-4665-157-012

16. Orlov A.I. On methods of checking the uniformity of two independent samples // Factory laboratory. *Diagnostika materialov = Diagnostics of Materials*. 2020;86(3):67–76. (In Russ.) https://doi.org/10.26896/1028-6861-2020-86-3-67-76

17. Zhukova G.N. Identification of distribution by coefficients of skewness and kurtosis. *Avtomatizatsiya. Sovremennye tekhnologii = Automation. Modern Technologies*. 2016;(5):26–33. (In Russ.)

18. Kerimov K.F., Azizova Z.I. Network traffic analysis using machine learning algorithms in an automated information system for rapid response to information security incidents and network traffic filtering. *Elektronnyi nauchnyi zhurnal «Potomki Al'-Fargani»*

Ferganskogo filiala TATU imeni Mukhammada Al'-Khorazmi = The electronic scientific journal «Descendants of Al-Fargani» of the Fergana Branch of the Muhammad Al-Khorazmi TATU. 2024;1(2):281–285. (In Russ.)

19. Kostin D.V., Shelukhin O.I. Comparative analysis of machine learning algorithms for classifying network encrypted traffic. *T-Comm – Telekommunikatsii i transport = T-Comm – Telecommunications and Transport*. 2016;10(9):43–52. (In Russ.)

20. Tanygin M.O., Dobritsa V.P., Mitrofanov A.V., Akhmat H.I. Mathematical interpretation of the results of cognitive analysis of metadata network packets. *Izvestiya Yugo-Zapadnogo gosudarstvennogo universiteta = Proceedings of the Southwest State University*. 2023;27(3):66–78. (In Russ.) https://doi.org/10.21869/2223-1560-2023-27-3-66-78

Информация об авторах / Information about the Authors

Таныгин Максим Олегович, доктор технических наук, декан факультета фундаментальной и прикладной информатики, Юго-Западный государственный университет, г. Курск, Российская Федерация, e-mail: tanygin@yandex.ru, ORCID: 0000-0002-4099-1414

Maxim O. Tanygin, Doctor of Sciences (Engineering), Dean of the Faculty of Fundamental and Applied Informatics, Southwest State University, Kursk, Russian Federation, e-mail: tanygin@yandex.ru, ORCID: 0000-0002-4099-1414

Добрица Вячеслав Порфирьевич, доктор физико-математических наук, профессор кафедры информационной безопасности, Юго-Западный государственный университет, г. Курск, Российская Федерация, e-mail: dobritsa@mail.ru, ORCID: 0000-0001-7533-3684

Vyacheslav P. Dobritsa, Doctor of Sciences (Physics and Mathematics), Professor of the Department of Information Security, Southwest State University, Kursk, Russian Federation, e-mail: dobritsa@mail.ru, ORCID: ID: 0000-0001-7533-3684

Митрофанов Алексей Васильевич, преподаватель кафедры информационной безопасности, Юго-Западный государственный университет, г. Курск, Российская Федерация, e-mail: mitro3000@rambler.ru, ORCID: 0000-0001-7200-6418

Aleksey V. Mitrofanov, Lecturer of the Department of Information Security, Southwest State University, Kursk, Russian Federation, e-mail: mitro3000@rambler.ru, ORCID: 0000-0001-7200-6418

Хаua Ибрахим Ахмат, аспирант кафедры информационной безопасности, Юго-Западный государственный университет, г. Курск, Российская Федерация, e-mail: ib-swsu@yandex.ru

Khaua Ibrahim Ahmat, Post-Graduate Student of the Department of Information Security, Southwest State University, Kursk, Russian Federation, e-mail: ib-swsu@yandex.ru