Оригинальная статья / Original article

https://doi.org/10.21869/2223-1560-2023-27-3-66-78

CC BY 4.0

Математическая интерпретация результатов когнитивного анализа метаданных сетевых пакетов

М.О. Таныгин [1] ✉, В.П. Добрица [1], А.В. Митрофанов [1], Х.И. Ахмат [1]

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

✉ e-mail: tanygin@yandex.com

Резюме

Цель исследования. *В статье рассматривается возможность повышения вероятности корректной аутентификации удалённого источника сообщений на основе анализа метаданных формируемых им сетевых пакетов. При передаче данных по сетям с низким энергопотреблением величины межпакетных интервалов времени подчинены известным законам распределения. На основе данных законов и принципов формирования аутентичных сообщений определено, что ошибка аутентификации приводит к формированию в приёмнике двух последовательностей пакетов, отличающихся одним элементом, для которых невозможно однозначно определить ту, которая полностью состоит из пакетов источника. Анализ времени поступления пакетов данных в двух последовательностях позволяет выработать решающее правило, на основании которого из двух последовательностей определяется аутентичная.*

Методы. *Анализ метаданных проводится для последовательностей размером 5 – 20 пакетов данных, что делает информативным лишь моменты высоких порядков для выборок межпакетных интервалов времени для таких последовательностей. Используется карта коэффициентов асимметрий и эксцессов, анализ которой позволил сформулировать гипотезу о том, что решающее правило для определения аутентичной последовательности можно принять на основании минимума расстояния до параболы, являющейся картой распределения коэффициентов эксцессов и асимметрий для распределения Пуассона.*

Результаты. *На основе разработанной математической модели поступления данных в приёмник получены наборы данных для проверки сформулированного критерия выбора аутентичной последовательности. Анализ доли принятых верных решений по критерию минимальности расстояния и доли случаев, в которых решающее правило может быть применено, позволил сформулировать критерий применимости правила минимального расстояния до параболы на карте коэффициентов эксцесса и асимметрии, который заключается в том, что правило применяется, если минимум расстояния для одной последовательности в 3 – 4 раза меньше, чем минимум для второй последовательности пары.*

Заключение. *В работе показано, что использование критерия кратного превышения минимального расстояния до карты распределения коэффициентов эксцесса и асимметрии позволяет повысить достоверность определения аутентичных последовательностей длиной 5 – 20 пакетов данных для распределения Пуассона, позволяет повысить точность принятия правильного решения до 90-95% при возможности использования метода в 60% – 80% случаев.*

Ключевые слова: *обработка данных; аутентификация; карта распределений; коэффициент эксцесса; коэффициент асимметрии; имитационное моделирование.*

© Таныгин М.О., Добрица В.П., Митрофанов А.В., Ахмат Х.И., 2023

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

Для цитирования: 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; 27(3): 66-78. https://doi.org/10.21869/ 2223-1560-2023-27-3-66-78.

Поступила в редакцию 02.09.2023 *Подписана в печать 27.09.2023* *Опубликована 28.10.2023*

Mathematical Interpretation of the Results of Cognitive Analysis of Network Packet Metadata

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

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

✉ e-mail: tanygin@yandex.com

Abstract

Purpose of research*. The article discusses the possibility of increasing the probability of correct authentication of a remote message source based on the analysis of metadata of network packets generated by it. When transmitting data over networks with low power consumption, the values of inter-packet time intervals are subject to known distribution laws. Based on these laws and principles for the formation of authentic messages, it has been determined that an authentication error leads to the formation in the receiver of two sequences of packets that differ in one element, for which it is impossible to unambiguously determine the one that consists entirely of source packets. Analysis of the arrival time of data packets in two sequences allows us to develop a decision rule, on the basis of which the authentic one is determined from the two sequences.*

Methods. *Metadata analysis is carried out for sequences of 5–20 data packets in size, which makes only high-order moments for samples of inter-packet time intervals for such sequences informative. A map of coefficients of asymmetries and kurtosis is used, the analysis of which allowed us to formulate the hypothesis that the decisive rule for determining the authentic sequence can be adopted based on the minimum distance to the parabola, which is a map of the distribution of coefficients of kurtosis and asymmetries for the Poisson distribution.*

Results. *Based on the developed mathematical model of data arrival at the receiver, data sets were obtained to test the formulated criterion for selecting an authentic sequence. Analysis of the proportion of correct decisions made according to the minimum distance criterion and the proportion of cases in which the decision rule can be applied allowed us to formulate a criterion for the applicability of the rule of the minimum distance to a parabola on the map of kurtosis and asymmetry coefficients, which consists in the fact that the rule is applied if the minimum distance for one sequences are 3 – 4 times less than the minimum for the second sequence of the pair.*

Conclusion. *The work shows that using the criterion of multiple excess of the minimum distance to the map of distribution of kurtosis and skewness coefficients makes it possible to increase the reliability of determining authentic sequences with a length of 5–20 data packets for the Poisson distribution, and makes it possible to increase the accuracy of making the right decision to 90-95% with the possibility of using the method in 60% – 80% of cases.*

Keywords: *data processing; authentication; distribution map; kurtosis coefficient; skewness coefficient; simulation modeling.*

Conflict of interest. *The authors declare 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., Ahmat Kh.I. Mathematical Interpretation of the Results of Cognitive Analysis of Network Packet Metadata. *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.

Received 02.09.2023 *Accepted 27.09.2023* *Published 28.10.2023*

***

Введение

Традиционным средством выполнения аутентификации источников сетевых пакетов является введение в заголовки пакетов кодов аутентификации сообщений или имитовставок. Отправитель формирует пакет данных и на основе его содержимого формирует и имитовставку. Приёмник проводит анализ полученного пакета и его имитовставки, определяя, является ли отправитель носителем некоторого секретного для третьей стороны идентификатора сеанса обмена данными (пароля). В общем случае вероятность преодоления имитозащиты, навязывания ложных данных или ошибки первого рода при проведении процедуры аутентификации определяется разрядностью кода аутентификации. Если же актуален вопрос сокращения передаваемого объёма данных (для протоколов промышленного интернета, протоколов дальней радиосвязи с низкой пропускной способностью, протоколов интернета вещей), тогда ограниченность размеров имитовставки в ряде случаев не позволяет обеспечить требуемую вероятность такой ошибки [1-4]. Это вынуждает использовать для алгоритмы установления подлинности, основанные на кодировании в режиме сцепления блоков, которые при равном размере имитовставки дают меньшую вероятность ошибки, но отличаются более высокой вычислительной сложностью [5-8]. Для ряда систем и протоколов связи остро встаёт необходимость сокращения размера заготовки из-за ограниченности размеров передаваемого кадра данных. Другим направлением повышения достоверности процедуры аутентификации является использование метаинформации, то есть информации, которую приёмник может извлечь из самого факта получения пакета или нескольких пакетов. Это может быть размер дополнительной информации, передаваемой по альтернативному каналу связи [9], статистических характеристик сигнала в канале связи [10], время поступления пакетов данных в приёмник [11], пространственное расположение источников пакетов данных [12].

Наиболее перспективным представляется анализ времени поступления пакетов данных в приёмник, так как каждый протокол передачи информации обладает собственными характеристиками распределения частоты межпакетных интервалов, что в сочетании с методами контроля аутентичности позволяет сформировать решающие правила для выделения аутентичных пакетов данных в случаях, когда анализ кодов

аутентификации сообщений не позволяют этого сделать. При этом анализироваться должны не только непосредственно значения межпакетных интервалов как значения случайной величины с некоторым законом распределения, а значения моментов данной случайной величины как наиболее информативные [13].

Материалы и методы

В рассмотренном методе анализа моментов высоких порядков для небольших по размеру выборок межпакетных интервалов времени [11] использовался подход, описанный в работе [14], при котором значения коэффициентов асимметрии и эксцесса для каждой выборки размещались на координатной плоскости, а затем производился их анализ, исходя из выявленных зависимостей между указанными параметрами. При моделировании передачи данных в LoRaWAN-сетях использовалась модель, описанная в [15, 16], которая модифицировалась с учётом использования для аутентификации кодирования в режиме сцепления блоков [17]. В результате последовательности сообщений, передаваемые от источника в приёмник, позволяют использовать дополнительную метаинформацию для повышения достоверности аутентификации – интервалы времени моментами получения сообщений последовательности. Для выборок, формируемых такими временными интервалами, рассчитывались коэффициенты асимметрии и эксцесса [18]. При анализе отличий законов распределения малых выборок, которые из себя представляют величины межпакетных интервалов при поступлении пакетов в приёмник, наиболее информативным являются моменты высоких порядков, которые, в отличие от моментов низких порядков, чувствительны в небольшим отклонениям в законах распределения элементов выборок [19] При этом, в случае возникновения ошибки аутентификации, значения времени поступления пакета, вызвавшего коллизию кодов аутентификации сообщений, изменяет значения двух интервалов времени в выборке, соответствующей последовательности аутентичных сообщений. Таким образом формируются отличия в карте коэффициентов асимметрии и эксцесса для множества выборок, образованных интервалами между временем поступления аутентичных пакетов данных (рис. 1 а) и множества выборок, образованных межпакетными интервалами для последовательностей, содержащих пакет постороннего источника (рис. 1 б).

Визуальный анализ карт коэффициентов асимметрии и эксцесса позволяет сделать вывод, что указанные параметры лежат в окрестности некоторой параболы. Данное наблюдение согласуется с исходными данными для составления модели поступления пакетов данных в приёмник: в её основе лежит предположение о том, что передача данных источником есть случайное событие, не зависящее от предыстории [16], что делает

распределение межпакетных интервалов времени подчинённым распределению Пуассона [20]. Распределение же Пуассона характеризуется квадратичной зависимостью между коэффициентами эксцесса E и асимметрии A: $E = A^2$.

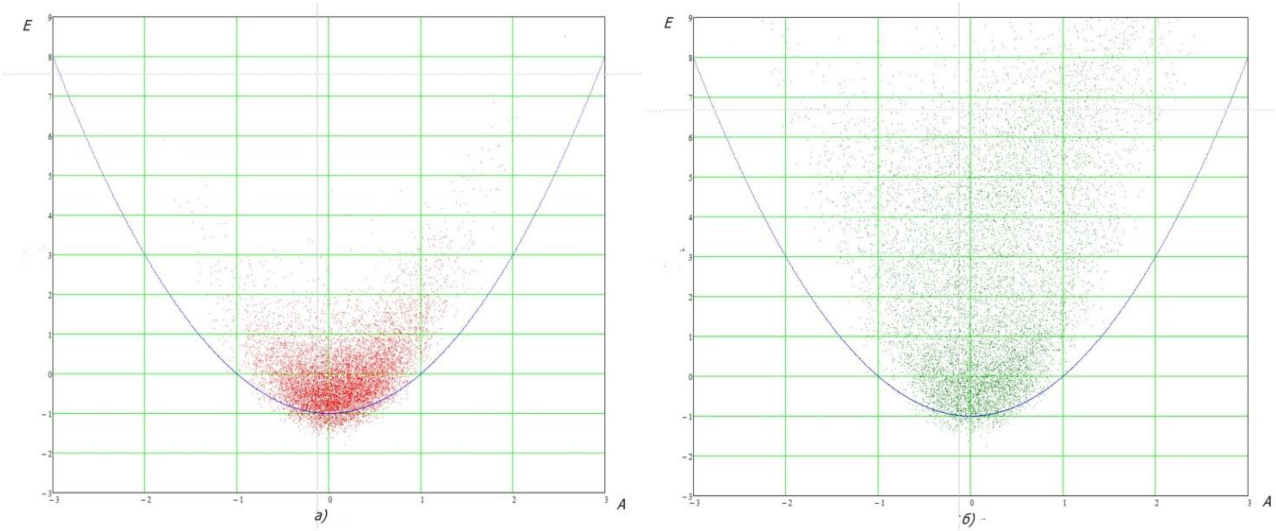

Рис. 1. Карта коэффициентов эксцесса и асимметрии для множества выборок, образованных интервалами между временем поступления пакетов данных: **а –** для множества аутентичных пакетов данных; **б –** для множества последовательностей, содержащих пакет постороннего источника

Fig. 1. Map of kurtosis and skewness coefficients for a set of samples formed by intervals between the arrival times of data packets: **а–** for many authentic data packets; **б –** for a set of sequences containing a packet from an extraneous source

Исследования показали, что замена в последовательности аутентифицированных сообщений одного сообщения на постороннее изменяет два элемента выборки величины межпакетных интервалов времени, делая распределение этих величин более похожим на равномерное. Это приводит к увеличению коэффициента эксцесса и незначительному изменению абсолютного значения коэффициента асимметрии [18].

Соответственно, когнитивный анализ карты распределений коэффициентов эксцесса и асимметрии и контекст формирования такой карты позволяет сформулировать гипотезу настоящего исследования: критерием для принятия решения об аутентичности последовательности сообщений может быть минимальность расстояния до некоторой параболы, построенной в той же системе координат.

Математическое описание сформулированной гипотезы выглядит следующим образом. Имеем параболу $E = f(A) = A^2 - A_0$ и точку v с координатами (A^v, E^v), необходимо найти минимальное расстояние от параболы до точки. Пусть это длина отрезка v – w, где w – точка параболы с координатами (A^w, E^w). Квадрат длины отрезка v – w равен

$$\left(E^w - E^v\right)^2 + \left(A^w - A^v\right)^2 = \\ = \left(\left(A^w\right)^2 - 1 - E^w\right)^2 + \left(A^w - A^v\right)^2. \quad (1)$$

Продифференцировав выражение по A^w и приравняв к нулю, получим кубическое уравнение вида:

$$\left(A^w\right)^3 + A^w\left(-\frac{3}{2} - E^w\right) + \frac{1}{2}A^v = 0, \qquad (2)$$

которое имеет 1 действительный корень (существует только одна точка на минимальном удалении от параболы при исключении из рассмотрения точек, лежащих на оси симметрии). Решая его, находим метрику D для пары коэффициентов (A^w, E^w):

$$D\left(A^w, E^w\right) = \left(Q - A^w\right)^2 + \left(Q^2 - 1 - W^w\right)^2,$$

$$Q = \left(\frac{1}{4}A^w + \left(\left(-\frac{3}{2} - E^w\right)^3 + \frac{1}{4}\left(A^w\right)^2\right)^{\frac{1}{2}}\right)^{\frac{1}{3}} +$$

$$+ \left(\frac{1}{4}A^w - \left(\left(-\frac{3}{2} - E^w\right)^3 + \frac{1}{4}\left(A^w\right)^2\right)^{\frac{1}{2}}\right)^{\frac{1}{3}}. \qquad (3)$$

Соответственно, аутентичной последовательностью из двух, сформированной целевым источником, будем считать ту, для которой метрика $D(A^w, E^w)$ будет минимальна.

Результаты и их обсуждение

Сформулированный критерий был проверен на тестовых наборах для различных размеров выборок M. Каждый набор состоял из 10 тысяч сгенерированных на основе описанной в [17, 18] модели передачи данных по беспроводной сенсорной сети при использовании кодирования в режиме сцепления блоков. Результат показал корректность принятия решения от 80% до 85% при 100%-м охвате критерием всех выборок. Это определило направление дальнейшего исследования – увеличение достоверности принятия решений при сокращении доли случаев, когда такой более строгий критерий может быть применён. Так как ошибка возникает, когда расстояние от параболы для последовательности, содержащей посторонние сообщения меньше, чем аутентичной последовательности, то средством уменьшения такой ошибки является введение мультиплицирующего коэффициента n для меньшего расстояния от точки до параболы. То есть условие применимости правила для пары точек (A1, E1) и (A2, E2) запишется в виде:

$$D\left(A_1, E_1\right) > n \cdot D\left(A_2, E_2\right) \vee$$
$$\vee D\left(A_2, E_2\right) > n \cdot D\left(A_1, E_1\right). \qquad (4)$$

При этом аутентичной последовательностью, будет признаваться та, чья точка на карте коэффициентов эксцесса и асимметрии будет минимальна. Доля правильно опознанных последовательностей P целевого источника в зависимости от длины последовательности M приведена на рис. 2.

Доля R последовательностей, которые удовлетворяли критерию (4) для различных значений размера выборки M и коэффициента n приведена на рис. 3.

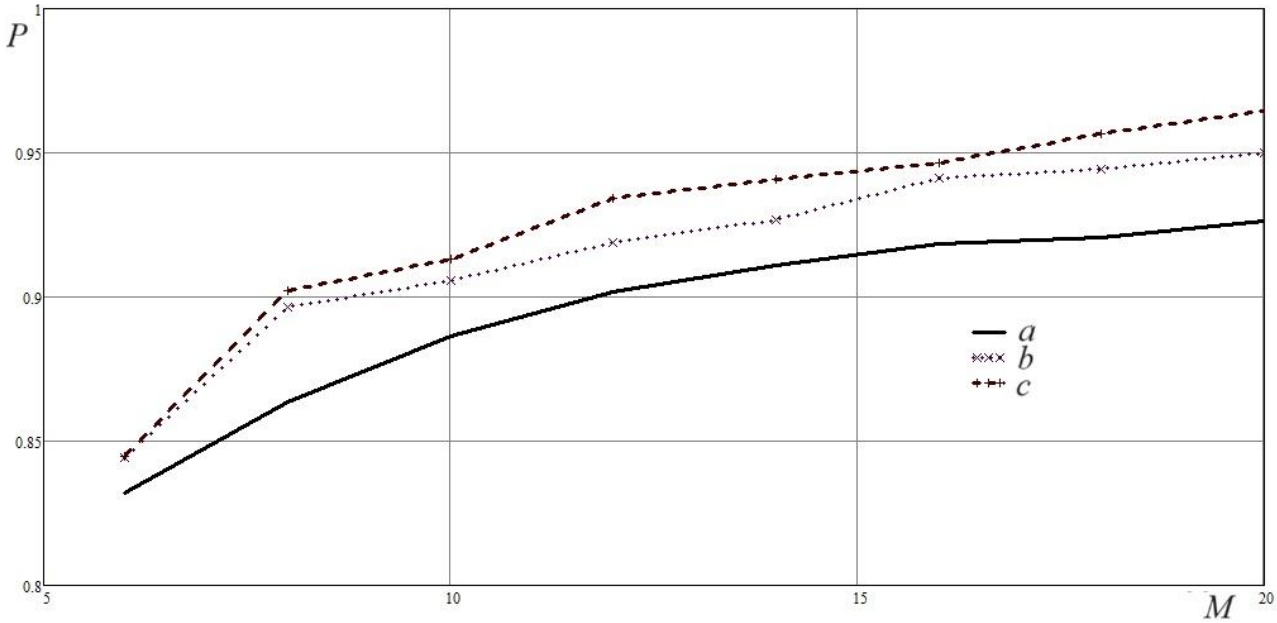

Рис. 2. График зависимости вероятности *P* правильного определения последовательностей целевого источника от длины последовательности *M* и значения коэффициента *n:* **a –** *n* = 2; **b –** *n* = 3; **c–** *n* = 4

Fig. 2. Graph of the dependence of the probability P of correct identification of target source sequences on the sequence length M and the value of the coefficient n: **a –** *n* = 2; **b –** *n* = 3; **c–** *n* = 4

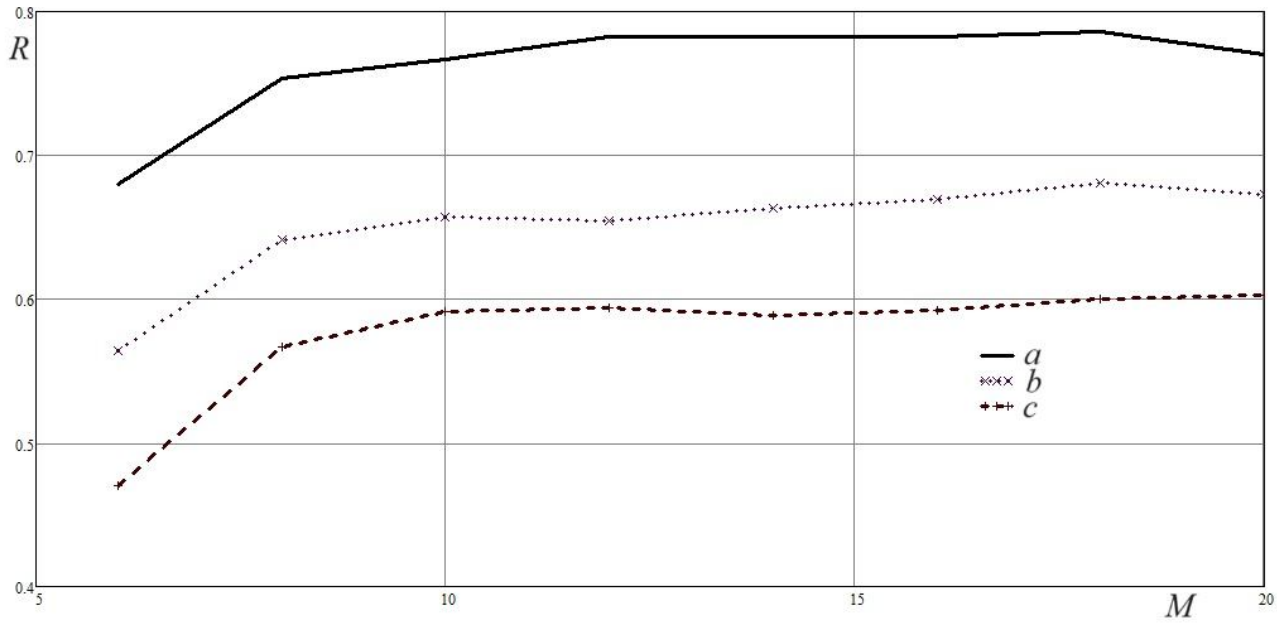

Рис. 3. Доля *R* последовательностей, которые удовлетворяют модифицированному критерию близости к параболе на карте эксцессов и асимметрий в зависимости от длины последовательности *M* и значения коэффициента *n:* **a –** *n* = 2; **b –** *n* = 3; **c –** *n* = 4

Fig. 3. The share R of sequences that satisfy the modified criterion of proximity to a parabola on the map of kurtosis and asymmetries depending on the sequence length M and the value of the coefficient n: **a –** *n* = 2; **b –** *n* = 3; **c –** *n* = 4

Из анализа графиков видно, что для определения аутентичной последовательности целесообразно выбирать коэффициент n в уточнённом критерии (4) из диапазона 2…3, так как меньший коэффициент не обеспечивает достоверности выше 90%, а увеличение коэффициента не ведёт к дальнейшему росту достоверности принятых решений, а лишь уменьшает долю случаев, когда решающее правило может быть применено.

Если сравнивать рассматриваемый метод в сравнении с рассмотренными ранее методами анализа коэффициентов эксцесса и асимметрии (табл. 1), то можно сделать вывод, что использование математической интерпретации сформулированной когнитивной гипотезы позволяет повысить достоверность принятия решений и долю случаев, когда метод анализа карт коэффициентов эксцесса и асимметрии может быть применён.

Таблица 1. Сравнение характеристик методов обработки коэффициентов эксцесса и асимметрии

Table 1. Comparison of characteristics of methods for processing kurtosis and skewness coefficients

Метод обработки данных / Data processing method	Процент верных принятия решений / Percentage of correct decisions	Доля случаев, когда метод может быть применён / Proportion of cases when the method can be applied
Сравнение абсолютных значений [18]	80%...90%	30%...40%
Сравнения абсолютных значений для множества выборок	85%...90%	60%...80%
Расстояние до параболы	90%...95%	60%...80%

Выводы

Выполненная в настоящей работе проверка гипотезы о возможности использования геометрического метода обработки коэффициентов эксцесса и асимметрии для выборок, содержащих значения межпакетных интервалов для последовательности аутентичных пакетов данных целевого источника, и для последовательности, содержащей один пакет от постороннего источника. В результате имитационного моделирования определены целесообразные параметры критерия принятия решения об аутентичной последовательности данных.

Таким образом, описанный подход, отличаясь простотой реализации (в нём требуется только вычисление метрики последовательности по формуле (3)), позволяет повысить достоверность аутентификации до 90%...95% в 60%...80% случаев

коллизий кодов аутентификации сообщений. В случае, если разрядность кода аутентификации сообщения обеспечивает достоверность аутентификации на уровне определённых известными стандартами беспроводной связи для целевого класса информационных систем в 10% [21, 22], то это означает снижение доли ошибочно выполненных процедур аутентификации с означенных 10% [23] до диапазона 4%...5%, то есть практически вдвое.

Направлениями дальнейших исследований может быть выбрано адаптация формы кривой, расстояние до которой находится по карте коэффициентов эксцесса и асимметрии к наблюдаемым значениям коэффициентов эксцесса и асимметрии для выборок, содержащих межпакетные интервалы времени.

Список литературы

1. Semtech Corporation. LoRa® and LoRaWAN®: A Technical Overview. URL: https://lora-developers.semtech.com/uploads/documents/files/ LoRa_and_LoRaWAN-A_Tech_ Overview-Downloadable.pdf.

2. IEEE Standard for Low-Rate Wireless Networks // IEEE Std 802.15.4-2020, pp.1-800, 23 July 2020, doi: 10.1109/IEEESTD.2020.9144691

3. Петров Д. Стандарты беспроводной связи диапазона ISM // Электронные компоненты. 2010. № 10. С. 28-32.

4. IEEE P802.11ahTM Standard for Information technology – Telecommunications and information exchange between systems Local and metropolitan area networks – Specific requirements – Part 11: Wireless LAN Medium Access Control (MAC) and Physical Layer (PHY) Specifications – Amendment 2: Sub 1 GHz License Exempt Operation, 2017.

5. Stallings W. NIST Block Cipher Modes of Operation for Authentication and Combined Confidentiality and // Cryptologia. 2010. № 34. P. 225 – 235. doi: 10.1080/01611191003598295.

6. Iwata T., Kurosawa K. OMAC: one-key CBC MAC / // Fast Software Encryption, 10th International Workshop. 2003. P. 129 – 153. doi 10.1007/978-3-540-39887-5_11.

7. Dworkin M. SP 800-38D: Recommendation for Block Cipher Modes of Operation: Galois/Counter Mode (GCM) and GMAC / Computer Security Division Information Technology Laboratory National Institute of Standards and Technology Gaithersburg, MD 20899-8930, 2007.

8. Ifzarne S., Imad H., Idrissi N. Homomorphic Encryption for Compressed Sensing in Wireless Sensor Networks // SCA '18, October 10–11, 2018, Tetouan, Morocco DOI 10.1145/3286606.3286857

9. Никешин А.В., Шнитман В.З. Обзор расширяемого протокола аутентификации и его методов // Труды ИСП РАН, т. 30, вып. 2, 2018, с. 113-148. DOI: 10.15514/ISPRAS-2018-30(2)-7

10. Лэндби С. А., Разумов Л., Бао Ганг. Патент 2422998 Российская Федерация H04B 7/216. Способ и устройство для высокоскоростной передачи пакетных данных и передачи данных с малой задержкой; заявл. 17.07.2006, опубл. 27.06.2011

11. 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. DOI 10.54398/20741707_2022_4_30

12. Воробьев А. В. Концепция информационного пакетного взаимодействия в многоуровневой системе цифровых двойников // Известия Саратовского университета. Новая серия. Серия: Математика. Механика. Информатика. 2021. Т. 21, вып. 4. С. 532–543. https://doi.org/10.18500/1816-9791-2021-21-4-532-543

13. Уразбахтин А.И., Уразбахтин И.Г. Алгоритм проверки однородности выборки и ее репрезентативности исследуемому случайному процессу // Инфокоммуникационные технологии. 2006. Т. 4. № 3. С. 10-14.

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

15. Khorov Evgeny, Lyakhov Andrey, Krotov Alexander, Guschin Andrey. A survey on IEEE 802.11 ah: An enabling networking technology for smart cities // Computer Communications. 2015. Vol. 58. Pp. 53–69. DOI:10.1016/j.comcom.2014.08.008.

16. Khorov Evgeny, Krotov Alexander, Lyakhov Andrey. Modelling Machine Type Communication in IEEE 802.11ah Networks // Communication Workshop (ICCW), 2015 IEEE International Conference on / IEEE. 2015. Pp. 1149–1154. DOI: 10.1109/ICCW.2015.7247332

17. Plugatarev A. V., Tanygin M. O. Model for Determining the Message Source by Analyzing Their Arrival Time // 2022 International Russian Automation Conference (RusAutoCon), 2022, pp. 388-392, doi: 10.1109/RusAutoCon54946.2022.9896326.

18. Метод определения источника сообщений на основе обработки времени их поступления / М. О. Таныгин, А. В. Плугатарев, С. И. Егоров, А. П. Локтионов // Известия Юго-Западного государственного университета. 2022; 26(3): 81-97. https://doi.org/10.21869/2223-1560-2022-26-3-81-97.

19. Захаров И.С., Уразбахтин А.И. Метод обнаружения и исключения аномальных значений выборки, полученной из однородной генеральной совокупности // Телекоммуникации. 2007. № 7. С. 14-23.

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

21. IEEE Standard for Low-Rate Wireless Networks // IEEE Std 802.15.4-2020, pp.1-800, 23 July 2020, doi: 10.1109/IEEESTD.2020.9144691

22. Петров Д. Стандарты беспроводной связи диапазона ISM // Электронные компоненты. 2010. № 10. С. 28-32.

23. Таныгин М.О. Восстановление порядка следования информационных пакетов на основе анализа хеш-последовательностей // Известия Юго-Западного государственного университета. 2020; 24(1): 175-188. https://doi.org/10.21869/2223-1560-2020-24-1-175-188.

References

1. Semtech Corporation. LoRa® and LoRaWAN®: A Technical Overview. Available at: https://lora-developers.semtech.com/uploads/documents/files/LoRa_and_LoRaWAN-A_Tech_Overview-Downloadable.pdf.

2. IEEE Standard for Low-Rate Wireless Networks. *IEEE Std 802.15.4*-2020, pp.1-800, 23 July 2020, doi: 10.1109/IEEESTD.2020.9144691

3. Petrov D. Standarty besprovodnoi svyazi diapazona ISM [Wireless communication standards of the ISM range]. *Elektronnye komponenty = Electronic Components*, 2010, no. 10, pp. 28-32.

4. IEEE P802.11ahTM Standard for Information technology – Telecommunications and information exchange between systems Local and metropolitan area networks – Specific requirements – Part 11: Wireless LAN Medium Access Control (MAC) and Physical Layer (PHY) Specifications – Amendment 2: Sub 1 GHz License Exempt Operation, 2017.

5. Stallings W. NIST Block Cipher Modes of Operation for Authentication and Combined Confidentiality and Cryptologia. 2010, no. 34, pp. 225 - 235. doi: 10.1080/01611191003598295.

6. Iwata T., Kurosawa K. OMAC: one-key CBC MAC. *Fast Software Encryption*, *10th International Workshop*, 2003, pp. 129 – 153. doi 10.1007/978-3-540-39887-5_11.

7. Dworkin M. SP 800-38D: Recommendation for Block Cipher Modes of Operation: Galois/Counter Mode (GCM) and GMAC. Computer Security Division Information Technology Laboratory National Institute of Standards and Technology Gaithersburg, MD 20899-8930, 2007.

8. Ifzarne S., Imad H., Idrissi N. Homomorphic Encryption for Compressed Sensing in Wireless Sensor Networks. *SCA* '18, October 10–11, 2018, Tetouan, Morocco DOI 10.1145/3286606.3286857

9. Nikeshin A.V., Shnitman V.Z. Obzor rasshiryaemogo protokola autentifika-tsii i ego metodov [Overview of the Extensible Authentication Protocol and its methods]. *Trudy ISP RAN = Proceedings of ISP RAS*, 2018, vol. 30, is. 2, pp. 113-148. DOI: 10.15514/ISPRAS-2018-30(2)-7.

10. Landby S.A., Razumov L., Bao Gang Patent 2422998 Russian Federation H04B 7/216. Sposob i ustroistvo dlya vysokoskorostnoi peredachi paketnykh dan-nykh i peredachi dannykh s maloi zaderzhkoi [Method and device for high-speed packet data transmission and low-latency data transmission]; application 07/17/2006, published 06/27/2011

11. Plugatarev A. V. Model' opredeleniya istochnika soobshchenii na osnove statisticheskogo analiza metadannykh v otkrytom kanale svyazi [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, no. 4(60), pp. 30-37. DOI 10.54398/20741707_2022_4_30

12. Vorobyov A. V. Kontseptsiya informatsionnogo paketnogo vzaimodeistviya v mnogourovnevoi sisteme tsifrovykh dvoinikov [Concept of information packet interaction in a multi-level system of digital twins]. *Izvestiya Saratovskogo universiteta. Novaya seriya. Seriya: Matematika. Mekhanika. Informatika = News of Saratov University. New Episode. Series: Mathematics. Mechanics. Computer Science*, 2021. T. 21, is. 4. pp. 532–543. https://doi.org/10.18500/1816-9791-2021-21-4-532-543

13. Urazbakhtin A.I., Urazbakhtin I.G. Algoritm proverki odnorodnosti vyborki i ee reprezentativnosti issleduemomu sluchainomu protsessu [Algorithm for checking the homogeneity of the sample and its representativeness of the random process under study]. *Infokommunikatsionnye tekhnologii = Infocommunication Technologies*, 2006, vol. 4, no. 3, pp. 10-14

14. Zhukova G.N. Karta koeffitsientov asimmetrii i ekstsessa v prepodavanii teorii veroyatnostei i matematicheskoi statistiki [Map of skewness and kurtosis coefficients in teaching probability theory and mathematical statistics]. *Kontsept. Nauchno-metodicheskii elek-tronnyi zhurnal = Concept. Scientific and methodological electronic journal.* 2015, no. 8, pp. 56-60.

15. Khorov Evgeny, Lyakhov Andrey, Krotov Alexander, Guschin Andrey. A survey on IEEE 802.11 ah: An enabling networking technology for smart cities. *Computer Communications*, 2015,vol. 58, pp. 53–69. DOI:10.1016/j.comcom.2014.08.008.

16. Khorov Evgeny, Krotov Alexander, Lyakhov Andrey. Modeling Machine Type Communication in IEEE 802.11ah Networks. *Communication Workshop (ICCW)*, 2015 *IEEE International Conference on IEEE*. 2015. pp. 1149–1154. DOI: 10.1109/ICCW.2015.7247332

17. Plugatarev A. V. Tanygin M. O., “Model for Determining the Message Source by Analyzing Their Arrival Time”. *2022 International Russian Automation Conference (RusAutoCon)*, 2022, pp. 388-392, doi: 10.1109/RusAutoCon54946.2022.9896326.

18. Politov E. N., Rukavitsyn A. N., Lomas Arciniega W. P., Terán Acosta G. R., Ávalos Cascante F. E., Puebla Puebla R. E. Method of Determining the Source of Messages Based on Processing the Time of Their Receipt. *Izvestiya Yugo-Zapadnogo gosudarstvennogo universiteta = Proceedings of the Southwest State University*. 2022; 26(3): 81-97 (In Russ.). https://doi.org/ 10.21869/2223-1560-2022-26-3-81-97

19. Zakharov I.S., Urazbakhtin A.I. Metod obnapuzheniya i isklyucheniya anomal'nykh znachenii vybopki, poluchennoi iz odnopodnoi genepal'noi sovokupnosti [Method for detecting and excluding anomalous values in a sample obtained from a homogeneous population]. *Telekommunikatsii = Telecommunications*, 2007, no. 7, pp. 14-23.

20. Zhukova G.N. Identifikatsiya raspredeleniya po koeffitsientam asimmetrii i ekstsessa [Identification of distribution by skewness and kurtosis coefficients]. Avtomatizatsiya. *Sovremennye tekhnologii = Automation. Modern Technologies*, 2016, no.5, pp. 26-33.

21. IEEE Standard for Low-Rate Wireless Networks. *IEEE Std 802.15.4*-2020, pp.1-800, 23 July 2020, doi: 10.1109/IEEESTD.2020.9144691

22. Petrov D. Standarty besprovodnoi svyazi diapazona ISM [Wireless communication standards of the ISM range]. *Elektronnye komponenty = Electronic Components*, 2010, no. 10, pp. 28-32.

23. 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.). https://doi.org/10.21869/2223-1560-2020-24-1-175-188.

Информация об авторах / Information about the Authors

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

Maxim O. Tanygin, Dr. of Sci. (Engineering), Associate Professor, Dean of Fundamental and Applied Informatics Faculty, Southwest State University, Kursk, Russian Federation, e-mail: tanygin@yandex.ru, ORCID: http://orcid.org/0000-0002-4099-1414

Добрица Вячеслав Порфирьевич, доктор физико-математических наук, профессор кафедры «Информационная безопасность», Юго-Западный государственный университет, г. Курск, Российская Федерация, e-mail: dobritsa@mail.ru, ORCID: http://orcid.org/0000-0001-7533-3684

Vyacheslav P. Dobritsa, Dr. of Sci. (Physical and Mathematical), Professor of Information Security Department, Southwest State University, Kursk, Russian Federation, e-mail: dobritsa@mail.ru, ORCID: http://orcid.org/0000-0001-7533-3684

Митрофанов Алексей Васильевич, аспирант кафедры «Информационная безопасность», Юго-Западный государственный университет, г. Курск, Российская Федерация, e-mail: mitro3000@rambler.ru, ORCID: http://orcid.org/0000-0001-7200-6418

Aleksey V. Mitrofanov, Post-Graduate Student of Information Security Department, Southwest State University, Kursk, Russian Federation, e-mail: mitro3000@rambler.ru, ORCID: http://orcid.org/0000-0001-7200-6418

Хауа Ибрахим Ахмат, аспирант кафедры «Информационная безопасность», Юго-Западный государственный университет, г. Курск, Российская Федерация, e-mail: ib-swsu@yandex.ru

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