Оригинальная статья / Original article

https://doi.org/10.21869/2223-1560-2022-26-3-81-97

Метод определения источника сообщений на основе обработки времени их поступления

М. О. Таныгин [1], А. В. Плугатарев [1] ✉, С. И. Егоров [1], А. П. Локтионов [1]

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

✉ e-mail: aplugatarev@bk.ru

Резюме

Целью исследования *является создание метода определения источника сообщений в приёмнике, позволяющего на основе анализа характеристик распределения времени поступления сообщений повысить достоверность определения источника.*

Методы. *Аутентификация источника сообщений происходит на основе статистического анализа значений метаданных, которыми в данном исследовании и являются интервалы времени между сообщениями. За основу модели обработки метаданных взята известная модель поступления сообщений от целевого источника в сетях LoRaWAN. При этом определение источника производилось с помощью методов кодирования в режиме сцепления блоков, которые обеспечивают более высокую достоверность идентификации для сообщений небольшой длины, характерных для указанного типа сетей. С помощью численного моделирования были определены закономерностей изменения характеристик времени поступления сообщений в случае возникновения ошибки идентификации. Так же сформулировано правило принятия решения в случае невозможности проведения аутентификации на основе обработки содержимого идентификационных полей. Исследования показали эффективность применения модели определения источника в различных диапазонах параметров формирования последовательностей сообщений.*

Результаты. *Итогом проведенных исследований является разработка метода аутентификации, основанного на анализе времени поступления сообщений на приёмник, который отличается тем, что в качестве анализируемых данных использует характеристики распределения моментов высоких порядков для рядов временных задержек. Его использование в сочетании с методами кодирования в режиме сцепления сообщений обеспечивает снижение вероятности возникновения ошибки единичной замены сообщения в последовательности в 4 - 6 раз, по сравнению с методами, выполняющими идентификацию только по результатам обработки идентификаторов самих сообщений.*

Заключение. *Результат экспериментальных исследований показал возможность при помощи разработанного метода повысить достоверность определения аутентичности источника сообщений, возможность снижения числа переспросов, возникающих при обнаружении ошибок, возможность уменьшения размеров дополнительных полей идентификаторов в каждом сообщении. Результирующий эффект будет выражаться в общем повышении пропускной способности канала связи между удаленными компонентами распределенной системы.*

Ключевые слова: *сетевое взаимодействие; аутентификация; анализ метаданных.*

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

Для цитирования*:* 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.

Поступила в редакцию 17.06.2022 *Подписана в печать 05.07.2022* *Опубликована 30.09.2022*

Method of Determining the Source of Messages Based on Processing the Time of Their Receipt

Maxim O. Tanygin [1], Aleksey V. Plugatarev [1] ✉, Sergey I. Egorov [1], Askold P. Loktionov [1]

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

✉ e-mail: aplugatarev@bk.ru

Abstract

Purpose of research *is to create a method for determining the source of messages in the receiver, which allows, based on the analysis of the characteristics of the distribution of the time of receipt of messages, to increase the reliability of determining the source.*

Methods. *Authentication of the message source is based on statistical analysis of metadata values, which in this study are the time intervals between messages. The metadata processing model is based on the well-known model of receiving messages from the target source in LoRaWAN networks. At the same time, the source was determined using coding methods in the block coupling mode, which provide higher identification reliability for short-length messages characteristic of the specified type of networks. With the help of numerical modeling, the patterns of changes in the characteristics of the time of receipt of messages in the event of an identification error were determined. The decision-making rule is also formulated in case of impossibility of authentication based on processing the contents of identification fields. Studies have shown the effectiveness of the application of the source detection model in various ranges of parameters for the formation of message sequences.*

Results. *The result of the conducted research is the development of an authentication method based on the analysis of the time of receipt of messages to the receiver, which differs in that it uses the characteristics of the distribution of moments of high orders for a series of time delays as the analyzed data. Its use in combination with coding methods in the message concatenation mode reduces the probability of a single message replacement error in a sequence by 4-6 times, compared with methods that perform identification only based on the results of processing the identifiers of the messages themselves.*

Conclusion. *The result of experimental studies has shown the possibility of using the developed method to increase the reliability of determining the authenticity of the source of messages, the possibility of reducing the number of re-inquiries that occur when errors are detected, the possibility of reducing the size of additional identifier fields in each message. The resulting effect will be expressed in a general increase in the bandwidth of the communication channel between remote components of a distributed system.*

Keywords: *network interaction; authentication; metadata analysis.*

Conflict of interest. *The authors declare the absence of obvious and potential conflicts of interest related to the publication of this article.*

For citation: 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.

Received 17..06.2022 *Accepted 05.07.2022* *Published 30.09.2022*

***

Введение

В большинстве информационных систем, где происходит обмен данными между её субъектами, используются механизмы для контроля целостности и аутентичности передаваемых данных. Подобный контроль, осуществляется с использованием соответствующих полей с дополнительной служебной информацией. Стремительное развитие науки и техники, крупных промышленных организаций и частных компаний привело к автоматизации большинства этапов деятельности и повышению требований к надёжности и экономии вычислительных ресурсов и ресурсов хранения данных. Процессы аутентификации в таких системах требуют использования ресурсов, которые напрямую не направлены на непосредственное выполнение задач, для которых система была спроектирована [1, 2]. Как правило, ко всем системам аутентификации предъявляются высокие требования к надёжности и производительности. Размер полей служебной информации должен быть минимальным, чтобы сократить избыточ-ность данных и повысить пропускную способность коммутационного канала [3]. Таким образом, актуальным является исследование механизмов определения источника сообщений и контроля их целостности, основанных на метаданных самих сообщений или, иными словами, на информации, характеризующей непосредственно процедуры обработки и передачи сообщений.

Предпосылками к созданию подобных моделей и методов является то, что информационные сообщения, передаваемые по каналам связи, несут в себе не только полезную нагрузку и рассматриваемые служебные поля, но и некую метаинформацию, анализ которой может позволить понизить вероятность возникновения ошибки определения источника, или, наоборот, при сохранении требуемой достоверности, уменьшить размер дополнительных служебных полей и минимизировать вычислительные ресурсы и ресурсы хранения данных системы. К метаинформации единиц сетевого взаимодействия, которую предлагается использовать в данном исследовании, предлагается использовать временной интервал между поступлением сообщений на приёмник [4].

Предложенный в статье подход к повышению достоверности идентификации источника основан на анализе характеристик центральных моментов распределений высокого порядка, который сформирован на основе накопленных данных о временных диапазонах между поступлениями сообщений на приёмник.

Материалы и методы

Рассмотрим систему, в которой взаимодействуют источник и приёмник информации, при этом задача приёмника – контролировать аутентичность, целостность и порядок следования всех поступающих сообщений, игнорируя те

из них, которые выданы посторонними источниками. Источник, генерируя сообщения, добавляет к полезной нагрузке значение хеш-функции, формируемой из данных предыдущего сообщения. В приёмнике при проверке данных, хеш из полученного сообщения сравнивается с хешами, формируемыми из данных всех поступающих в течение некоторого сеанса связи сообщений [5, 6].

В научных работах ранее был предложен метод, достоверность принятия решения об атрибутах в котором определяется исходя из вероятности случайного совпадения, рассчитанной для блока целевого источника метрики с аналогичной метрикой для любого блока из множества анализируемых приёмником. Вероятность ошибки для них определится исходя из формулы 1, где степень $|U|$ определяется как произведение числа взаимодействующих устройств b на длину фрагментированного сообщения n, а длина атрибутивных данных обозначена H [7-8].

$$P^{col}=1-\left(1-\frac{1}{2^{H}-1}\right)^{|U|}. \quad (1)$$

В описанном методе предполагается вероятность ошибки аутентификации. В свою очередь, модель определения источника сообщений, описываемая в данной работе, предлагается как следующий этап указанного метода, для повышения достоверности принятия решения.

На приёмник в некоторое временное окно поступает множество сообщений, которые формируют сеанс длиной N. Каждое принятое сообщение получает уникальный порядковый номер i.

На первом этапе буферизации сообщений на приёмнике необходимо сформировать цепочки последовательностей сообщений. В процессе сетевого взаимодействия в течение одного сеанса, каждое поступившее сообщение n_i сравнивается с имитовставкой (хешем) всех уже пришедших сообщений, порядковый номер поступления которых меньше i. Условием для включения сообщения в последовательности является равенство хеша (имитовставки), сформированной из данных предыдущего блока цепочки содержимого [9-10]. При совпадении хэша, считаем принятое сообщение продолжением формируемой цепочки сообщений. При этом фиксируется временной интервал между n_i и n_{i-1}.

Для дальнейшей обработки данных на основе разницы поступления сообщений на приёмник необходимо сформировать граф сеанса. Каждый сеанс представляет из себя ориентированный взвешенный граф

$$G = \{V, R\}, \quad (2)$$

где V – множество сообщений, а R – множество пар сообщений v, v’ ∈ V, а дуга (v,v') – это два сообщения с совпадающей имитовставкой, так что время поступления $t(v_{i-1})< t(v_i)$.

Новое сообщение n_i добавляет вершину v_i в множество V, соединённую с ребром (v,v') из множества R если имитовставки n_{i-1} и n_i совпадают. Вес ребра определяем по формуле

$$r_{v_i-v_{i-1}}=t(v_i)-t(v_{i-1}). \quad (3)$$

Следующий этап – фиксация всех путей графа длиной N – количества сообщений в сеансе. В рамках описываемого алгоритма фиксация происходит при полном переборе путей.

Наличие сообщений, сформированных посторонними источниками или злоумышленником, может привести к ситуации, когда несколько сообщений подходят для продолжения одной цепочки, что делает необходимым выбор между несколькими такими цепочками. В оригинальном методе подобная ситуация вызывает ошибку определения источника сообщений. В связи с этим возникает задача определения той цепочки сообщений, которая состоит полностью из сообщения от целевого источника. На рис. 1 проиллюстрирован пример сформированного графа сообщений, поступивших в течение сеанса связи. Видно, что анализ хешей привёл к формированию двух последовательностей сообщений длиной N=5 из-за того, что в промежуток времени t_3 и t_1 в приёмник поступило два сообщения с подходящими значениями полей основных данных и атрибутов (поля, в котором размещено значение хеша предыдущего сообщения). Для определения цепочки, состоящей только из сообщений целевого источника, можно использовать различие времени поступления отличающихся элементов и то, что интервалы между поступлениями таких сообщений подчинены разным законам распределения.

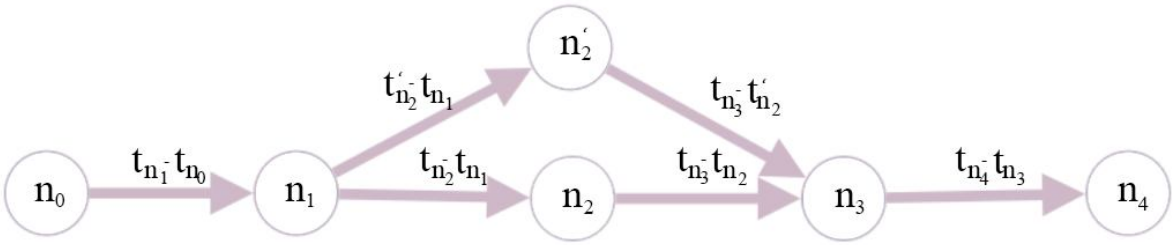

Рис. 1. Пример графа сеанса

Fig. 1. A session graph example

В работах [11–12] была определена функция распределения длительности интервалов между сообщениями от одного источника интенсивности генерации λ = 0,4 сообщений в секунду, что соответствует средним наблюдаемым значениям для сетей LoRaWAN [13]. Данный результат получен с учётом того, что передача данных осуществляется в режиме с подтверждениями успешной передачи, с механизмом повторной передачи в случае неудачи и контролем занятости канала связи передачей данных от других источников.

Как было сказано выше, цепочки, содержащие сообщения от неизвестного источника, формируются путём замены сообщений целевого источника в исход-

ной цепочке. Это проиллюстрировано добавлением вершин сообщений в граф, показывающий формируемую в приёмнике динамическую структуру (рис. 1), вершины v_i', где i является целым числом, равномерно распределённым в диапазоне [0; N-1]. Рёбра графа, характеризующие длительность интервала между соответствующими сообщениями, которыми соединено постороннее сообщение v_i' с сообщениями целевого источника, для проведения моделирования могут быть определены по формуле

$$t(v_i')=\text{random}\left(0;\ t(v_i)+ t(v_{i+1})\right), \qquad (4)$$

где random – функция выбора случайной величины в указанном диапазоне по закону равномерного распределения.

Это показывает случайность момента времени, в который поступило постороннее сообщение, добавленное в цепочку сообщений формируемой структуры. Соответственно:

$$t(v_{i+1}')=\left(t(v_i)+ t(v_{i+1})\right)- t(v_i'). \qquad (5)$$

В рамках вышеизложенного метода на этапе принятия решения о том, что сформированная цепочка сообщений выдана целевым источником, возникает задача сравнения двух малых выборок одинакового размера, у которых все элементы совпадают кроме 1-3 подряд идущих. Математические модели формирования ошибок аутентификации показали, что для рассматриваемой модели сетевого взаимодействия вероятность возникновения последовательностей замен в цепочках снижается на порядки с увеличением числа отличающихся элементов. Это обусловливает то, что в рассматриваемой модели возникновения ошибок мы рассматривали ситуации, когда в последовательность сообщений от целевого источника встроено 1 – 3 посторонних сообщения. В результате сформированные выборки временных интервалов между сообщениями будут отличаться на соответствующее число элементов при небольшой (от 10 до 30) длине самих выборок. Такое утверждение делается на основании результатов достоверности и трудоёмкости методов аутентификации для цепочек сообщений, показывающих, что рост длины цепочек может быть критичен для вероятности корректного определения источника [14].

Поэтому стандартные характеристики, такие, как математическое ожидание или дисперсия, рассчитаны для таких выборок, не могут явиться основой для формирования решающих правил.

В работах [15, 16] исследуются характеристики моментов высоких порядков для классификации различных законов распределения, в том числе по коэффициентам асимметрии и эксцесса. Учитывая то, что сообщения от целевого источника формируются по модели типа ALOHA, значения временных интервалов между поступлением сообщения от него подчинены некоторому закону распределения [17].

Кроме того, выводы, сделанные из исследований однородностей выборок при случайных процессах [18] и исследований аномалий значений выборки,

полученной из совокупностей выборок [19], позволяют воспользоваться значениями моментов высокого порядка для анализа и сравнения малых выборок, каковыми являются временные интервалы между получениями сообщений одной цепочки. Анализ вышеуказанных источников позволил предложить метод определения источника сообщений, в качестве анализируемых данных в котором используются такие характеристики распределения моментов высоких порядков для временных интервалов, как коэффициент асимметрии и коэффициент эксцесса.

Результаты и их обсуждение

При анализе результатов, полученных на основе описанной модели формирования временных интервалов между сообщениями, замечено, что значения коэффициентов асимметрии и эксцесса для цепочки с включёнными в её состав сообщениями посторонних источников(n_0–n_1–n_2'–n_3–n_4 на рис. 1), меньше в сравнении с аналогичными значениями для цепочки из сообщений целевого источника (n_0–n_1–n_2–n_3–n_4 на рис. 1). Проиллюстрирована тенденция уменьшения значений коэффициентов асимметрии и эксцесса для цепочек с посторонними сообщениями с помощью графика, на котором представлены точки в общей системе координат, где горизонтальная ось – коэффициент асимметрии, вертикальная – коэффициент эксцесса (рис. 2). На рисунке приведены результаты пяти экспериментов при $N = 32$.

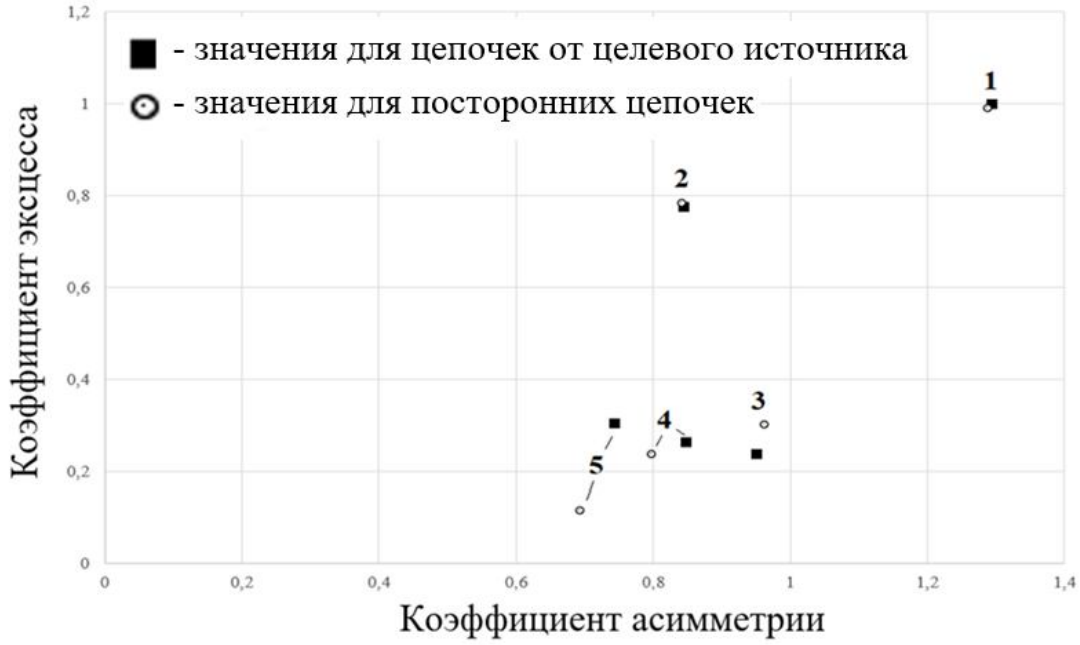

Рис. 2. Примеры значений коэффициентов эксцесса и асимметрии для цепочек, полученных от целевого источника и посторонних цепочек

Fig. 2. Examples of kurtosis and skewness coefficient values for target and unauthorized chains

Несмотря на тенденцию уменьшения значений коэффициента асимметрии и коэффициента эксцесса у посторонних цепочек (цепочек, в которых присутствуют иные, помимо сообщений целевого источника, сообщения), встречаются случаи, как например, в точке 3, когда оба коэффициента возрастают. В предлагаемом методе определения источника сообщений на основе формирования цепочек сообщений и анализа времени их поступления данная ситуация приведёт к возникновению ошибки: цепочка сообщений от целевого источника будет отвергнута, а цепочка с посторонними сообщениями будет опознана как полностью сформированная целевым источником. Для определения достоверности метода анализа времени поступления сообщений с помощью имитационной модели моделировались ситуации, когда исходный метод, основанный только на формировании цепочек сообщений [20] приводил к формированию двух и более цепочек (рис. 1). Так как формирование цепочек происходит на основе декодирования поступающего сообщения и проверки содержимого его полей, то добавление постороннего сообщения в цепочку происходит случайным образом. Для получения достоверного результата, при котором средняя доля ошибок могла бы характеризовать вероятность возникновения ошибки общее число экспериментов для каждого значения длины цепочки N равнялось 10^4.

Различия в значениях коэффициентов позволяют сформировать различные решающие правила для выделения цепочки сообщений целевого источника из двух альтернатив. Исследовались различные сочетания мажоритарных правил: соотношения больше-меньше для значений коэффициентов асимметрии и эксцесса без учёта их абсолютных значений. Показатели успешных аутентификаций на основе имитационного моделирования представлены в табл. 1, где:

N – количество сообщений в цепочке;

K_a – процент опытов, при котором у посторонней цепочки меньше коэффициент асимметрии;

$K_э$ – процент опытов, при котором у посторонней цепочки меньше коэффициент эксцесса;

S – процент опытов, при котором у посторонней цепочки меньше либо коэффициент асимметрии, либо коэффициент эксцесса.

В процессе моделирования, исходя из данных табл. 1, доля верных решений относительно цепочек при использовании решающего правила на основе коэффициента асимметрии была около 0,65, в зависимости от параметров модели передачи сообщений [20]. В свою очередь, использование в качестве данных, на основе которых принимается решение, значения коэффициента эксцесса давало приблизительно такую же достоверность. В то же время, если принять условием уменьшение хотя бы одного из двух коэффициентов, то вероятность верного определения цепочки сообщений целевого источника достигает 0,8.

Таблица 1. Результаты численного моделирования

Table 1. Results of numerical simulation

№п/п	N	$K_а$	$K_э$	S	№ п/п	N	$K_а$	$K_э$	S
1	5	63	61	81	7	40	68	66	80
2	10	66	66	82	8	45	65	63	83
3	15	72	70	79	9	50	61	68	81
4	20	65	63	81	10	55	69	60	82
5	25	54	72	82	11	60	73	73	84
6	30	60	69	84	12	64	61	74	85

Таким образом, максимальный процент успешного определения цепочки сообщений от целевого источника в рассматриваемом методе достигается при использовании правила, формализованного как:

$$\text{auth} = \left(K_A > K'_A\right) \text{ or } \left(K_Э > K'_Э\right), \qquad (6)$$

где K_A и $K_Э$ – коэффициенты асимметрии и эксцесса, рассчитанные для цепочки сообщений, которую, согласно обсуждаемому методу, определяем как цепочку сообщений целевого источника, а K'_A и $K'_Э$ – коэффициенты асимметрии и эксцесса, рассчитанные для последовательности сообщений, определяемой как последовательность, включающая сообщения нецелевого источника. Иными словами, цепочкой сообщений целевого источника признаётся цепочка, у которой больше рассчитанный для неё либо коэффициент асимметрии, либо коэффициент эксцесса.

Таким образом метод определения источника сообщений на основе анализа времени их поступления может быть представлен следующими этапами:

1) буферизация сообщений и фиксация времени поступления каждого из них на приёмнике;

2) формирование на основании анализа кодов аутентификации сообщений и временных интервалов сообщений взвешенного графа (1);

3) в случае, когда в графе сеанса присутствует более чем одна цепочка требуемой длины, находим коэффициенты эксцесса и асимметрии из выборок, представленных весами дуг соответствующих цепочек;

4) считать ту цепочку сообщений от целевого источника, которая удовлетворяет условию (6) минимальности коэффициентов эксцесса или асимметрии.

Результаты численного моделирования представлены на рис. 3, на котором приведены зависимости вероятности ошибки для метода выделения атрибутов при обработке цепочки сообщений для одинаковых значений длин $H = 7$ поля атрибутивных данных (параметр, влияющий на достоверность исходного метода определения источника сообщений) с применением анализа времени поступления сообщений и

без него при $N = 10$ (данные по оси ординат представлены в логарифмическом масштабе).

Из рис. 3 видно, что использование анализа времени поступления сообщений даёт фиксированное снижение вероятности ошибки в сравнении с методами, определяющими источник цепочки сообщений только на основании построения цепочек сообщений, кодированных в режиме сцепления блоков. При этом эффект от анализа времени поступления сообщений не зависит от числа источников, формирующих сообщения для рассматриваемого приёмника и параметров кодирования сообщений.

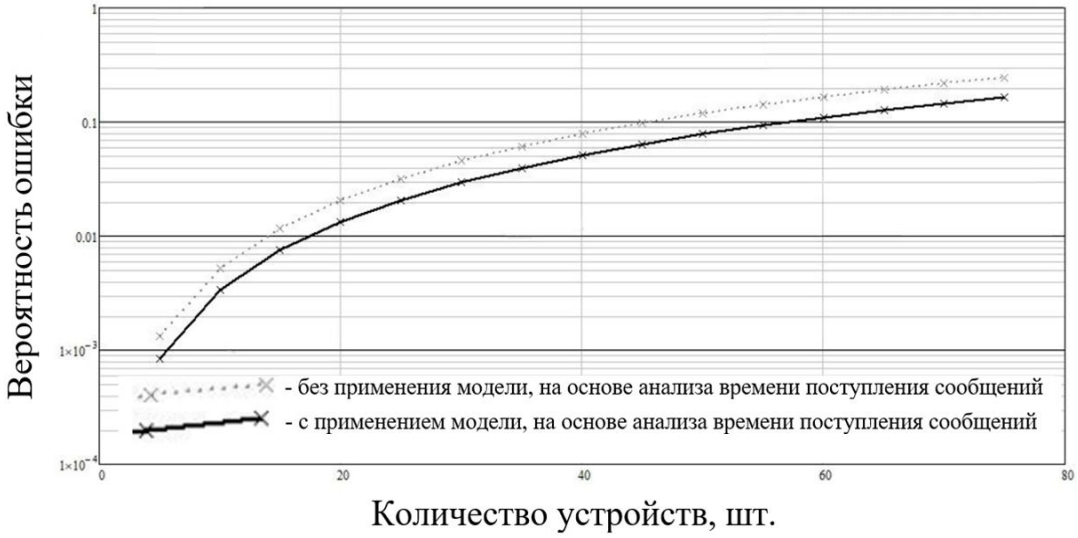

Рис. 3. Зависимость вероятности ошибки с применением предложенной модели от числа устройств при одинаковой длине фрагментированного сообщения n и длине поля атрибутивных данных

Fig. 3. Dependence of the error probability using the proposed model on the number of devices for the same length of the fragmented message n and the length of the attribute data field

Наиболее близкий к описанному метод представлен в работе [21]. В основе метода определения истинной цепочки сообщений, аналогично, лежит анализ временных задержек поступления сообщений на приёмник. Решающее правило формируется на основе подсчёта площади трапеции, построенной из линий, которые ограничивают показатели сравниваемых временных рядов на графике зависимости временных задержек от длины цепочки. Ошибка метода фиксировалась, если площадь, выстроенная по описанным формулам, для массива временных промежутков доставки сообщений на приёмник больше или равна альтернативному массиву временных задержек, в котором один элемент временной задержки отличается.

На рис. 4 проиллюстрированы зависимости возникновения ошибок аутентификации от длины анализируемого

числового ряда временных задержек с использованием числовых характеристик моментов высоких порядков, описанная в данной работе, и с использованием подсчёта площади трапеции для массива временных задержек. Из графика прослеживается, что при больших значениях длины цепочки (начиная от N = 30) показатели методов примерно равные, однако при низких значениях предложенный метод имеет преимущество в 5 - 15 %, в зависимости от N.

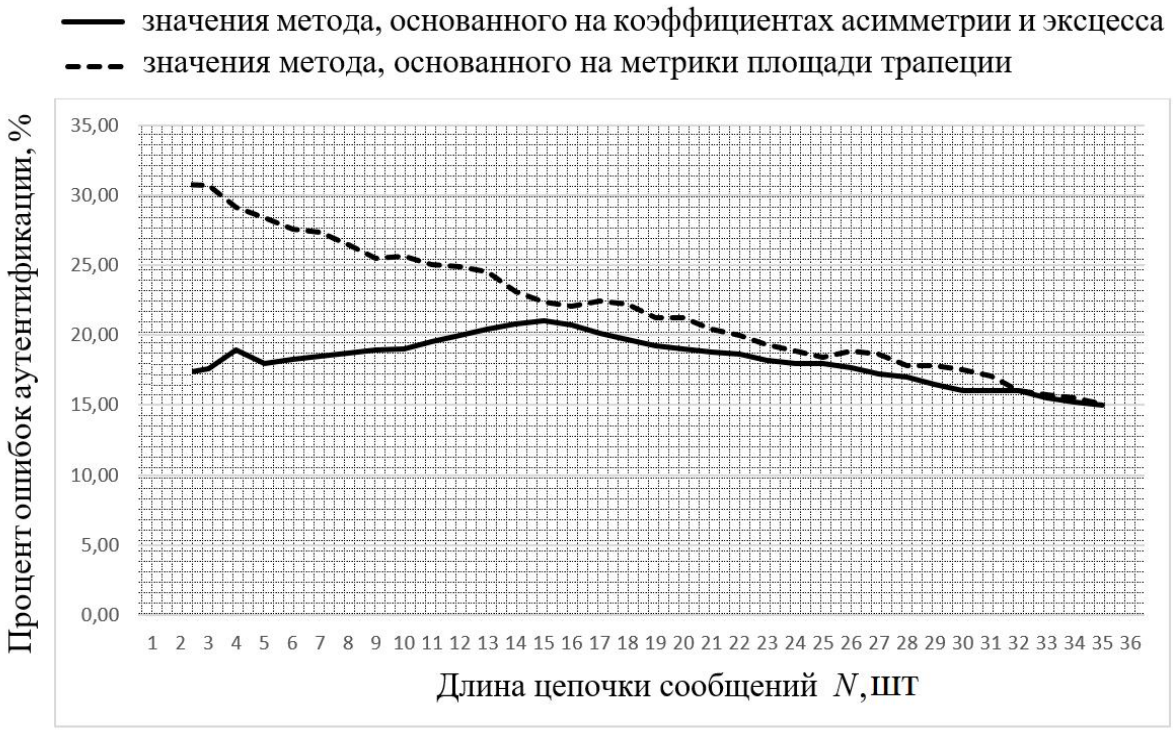

Рис. 4. Зависимость вероятности ошибки аутентификации от длины цепочки сообщений для различных методов определения источника сообщений

Fig. 4. Dependence on the probability of authentication failure from message chains for different methods of discovering message sources

Связано это с тем, что при отсутствии длительных задержек график массива становится более ровным, лишённым значительных отклонений времени доставки от тренда, на фоне чего пакет постороннего источника, время доставки которого распределено в широком диапазоне, даёт резкое увеличение значения метрики площади. В свою очередь, предложенный в данной работе метод, а именно коэффициенты асимметрии и эксцесса дают отклонение в цепочках с посторонними сообщениями, при намного меньшем значении длины самой цепочки значений задержек, а значит представляется возможность использовать метод в информационных системах с низкой пропускной способностью.

Таким образом, предложенный в данной работе метод анализа метаинформации о поступающих в приёмник

сообщениях позволяет повысить надёжность аутентификации источника данных. Однако в реальных информационных системах возможны ситуации, когда ложные сообщения могут формировать побочные цепочки большей длины. В таком случае, одним из возможных продолжений данного исследования является определение вероятности ложных сообщений на этапе формирования цепочки сообщений, и принятие решения об отклонении аутентификации на этапе обработки только части цепочки сообщения.

Выводы

В данной работе рассмотрена возможность использования числовых характеристик распределения, а именно коэффициента асимметрии и коэффициента эксцесса для исправления ошибок аутентификации при сетевом взаимодействии на основе метаданных. В качестве метаданных используются показатели времени поступления сообщения в приёмник. Применен метод оценки выборок при использовании характеристик моментов высоких порядков (таких как коэффициент асимметрии и коэффициент эксцесса), которая является действенным средством анализа выборок небольшого размера. Показано, что сочетание режима сцепления блоков для аутентификации с использованием анализа времени поступления в сетевой модели типа ALOHA позволяет снизить вероятность ошибки определения источника сообщений по сравнению с методами, использующими только режим сцепления блоков.

Список литературы

1. Информационная безопасность предприятия / А. В. Бабаш, Е. К. Баранова, Д. Ларин, Н.В. Гришина. М.: Форум, 2018. 118 с.

2. Буренин А.Н., Легков К.Е. Основные проблемы безопасности подсистем обеспечения единым временем элементов систем управления сложными организационно-техническими объектами // T-comm: телекоммуникации и транспорт. 2019. С. 48.

3. Gligor V.D., Donescu P. Fast encryption and authentication: XCBC encryption and XECB authentication modes // Manuscript, August 2002. P. 92–108.

4. Установление доверительного канала обмена данными между источником и приёмником информации с помощью модифицированного метода одноразовых паролей / М.О. Таныгин, Х.Я. Алшаиа, В.А. Алтухова, А.Л. Марухленко // Известия Юго-Западного государственного университета. Серия: Управление, вычислительная техника, информатика. Медицинское приборостроение. 2018. № 4(29). С. 63-71.

5. Колегов Д.Н. Общий метод аутентификации HTTP-сообщений в веб-приложениях на основе хеш-функций // Прикладная дискретная математика. Приложение. 2014. № 7. С. 85-89.

6. Вариант разграничения доступа к информационным ресурсам на основе неявной аутентификации / А.Л. Марухленко, А.В. Плугатарев, М.О. Таныгин, Л.О. Марухленко, М.Ю. Шашков // Известия Юго-Западного государственного университета. 2020;24(2):108-121. https://doi.org/10.21869/2223-1560-2020-24-2-108-121

7. Panagiotis Papadimitratos, Zygmunt J. Haas Secure message transmission in mobile ad hoc networks // Ad Hoc Networks. 2003. №1. P. 193–209

8. Shi X., D. Xiao A reversible watermarking authentication scheme for wireless sensor networks // Information Sciences. 2013. Vol. 240. P. 173-183. https://doi.org/10.1016/j.ins.2013.03.031

9. Анализ системы контроля целостности цепочек информационных блоков на основе хэшей / М. О. Таныгин, М.С. Брусов, Е.О. Ефремова, Ю.В. Сухорукова // Инфокоммуникации и космические технологии: состояние, проблемы и пути решения: материалы III Всероссийской научно-практической конференции. Курск, 2019. С.373 – 378.

10. Гузеев А.В. Формирование распределения вероятностей появления отдельных сообщений источника при статистическом кодировании // T-Comm: Телекоммуникации и транспорт. 2010. Т. 4. № 6. С. 12-16.

11. Mytsko E.A., Malchukov A.N., Ivanov S.D. Research of algorithms for calculating the CRC8 checksum in microprocessor systems with a shortage of resources // Devices and systems. Management, control, diagnostics. 2018. No. 6. P. 22-29.

12. Bankov D., Khorov E., Lyakhov A. On the Limits of LoRaWAN Channel Access. Engineering and Telecommunication (EnT), 2016 International Conference on IEEE. 2016. Pp. 10–14

13. lantado Ferran, Vilajosana Xavier, Tuset Pere et al. Understanding the Limits of LoRaWAN // IEEE Communications Magazine. 2017.

14. Tanygin M.O., Efremov M.A., Tanygina E.A. The Computational Complexity of the Algorithm for Identifying the Source of Data Transmitted by Limited Length Blocks // Proceedings - 2021 International Russian Automation Conference, RusAutoCon 2021, 2021, pp. 298–302.

15. 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.

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

17. Vangelista Lorenzo. Frequency Shift Chirp Modulation: The LoRa Modulation // IEEE Signal Processing Letters. 2017. Vol. 24, no. 12. Pp. 1818–1821.

18. Urazbakhtin A.I., Urazbakhtin I.G. Algorithm for checking the homogeneity of the sample and its representativeness to the random process under study // Infocommunication technologies. 2006. V. 4. No. 3. S. 10-14.

19. Tatyana I. Lapina, Ildus G. Urazbahtin Time series forecasting based on data normalization methods // Proceedings Volume 6277, Optical Technologies for Telecommunications 2005; 62770C (2006).

20. Jorke Pascal, Bocker Stefan, Liedmann Florian, Wietfeld Christian. Urban channel models for smart city IoT-networks based on empirical measurements of LoRa-links at 433 and 868 MHz // 2017 IEEE 28th Annual International Symposium on Personal, Indoor, and Mobile Radio Communications (PIMRC) / IEEE. 2017. Pp. 1–6.

21. Таныгин М. О., Хемраев Д., Казакова О. В. Повышение достоверности определения источника фрагментированных сообщений за счёт использования методов анализа времени поступления отдельных фрагментов // Известия Юго-Западного государственного университета. Серия: Управление, вычислительная техника, информатика. Медицинское приборостроение. 2021. Т. 11, № 4. С. 46–60.

References

1. Babash A. V., Baranova E. K., Larin D., Grishina N.V. *Informatsionnaya bezopasnost' predpriyatiya* [Information security of the enterprise]. Moscow, Forum Publ., 2018. 118 p.

2. Burenin A.N., Legkov K.E. Osnovnye problemy bezopasnosti podsistem obespecheniya edinym vremenem elementov sistem upravleniya slozhnymi organizatsionno-tekhnicheskimi ob"ektami [The main problems of security of subsystems for ensuring the elements of control systems for complex organizational and technical objects with a single time]. *T-comm: telekommunikatsii i transport = T-comm: Telecommunications and Transport*, 2019, 48 p.

3. 6. Gligor V.D., Donescu P. Fast encryption and authentication: XCBC encryption and XECB authentication modes. *Manuscript*, August 2002, pp. 92–108.

4. Tanygin M.O., Alshaia Kh.Ya., Altukhova V.A., Marukhlenko A.L. Ustanovlenie doveritel'nogo kanala obmena dannymi mezhdu istochnikom i priemnikom informatsii s pomoshch'yu modifitsirovannogo metoda odnorazovykh parolei [Establishment of a trusted data exchange channel between the source and receiver of information using a modified method of one-time passwords]. *Izvestiya Yugo-Zapadnogo gosudarstvennogo universiteta. Seriya: Upravlenie, vychislitel'naya tekhnika, informatika. Meditsinskoe priborostroenie =*

Proceedings of the Southwest State University. Series: Control, Computing Engineering, Information Science. Medical Instruments Engineering, 2018, no. 4 (29), pp. 63-71.

5. Kolegov D.N. Obshchii metod autentifikatsii HTTP-soobshchenii v veb-prilozheniyakh na osnove khesh-funktsii [A general method for authenticating HTTP messages in web applications based on hash functions]. *Prikladnaya diskretnaya matematika. Prilozhenie = Applied Discrete Mathematics, Appendix*, 2014, no. 7, pp. 85-89.

6. Marukhlenko A.L., Plugatarev A.V., Tanygin M.O., Marukhlenko L.O., Shashkov M.Yu. Variant razgranicheniya dostupa k informatsionnym resursam na osnove neyavnoi autentifikatsii [Option to restrict access to information resources based on implicit authentication]. *Izvestiya Yugo-Zapadnogo gosudarstvennogo universiteta = Proceedings of the Southwest State University*. 2020;24(2):108-121. https://doi.org/10.21869/2223-1560-2020-24-2-108-121.

7. Panagiotis Papadimitratos, Zygmunt J. Haas Secure message transmission in mobile ad hoc networks. *Ad Hoc Networks*, 2003, no. 1, pp. 193–209.

8. Shi X., D. Xiao A reversible watermarking authentication scheme for wireless sensor networks. *Information Sciences*, 2013, vol. 240, pp. 173-183. DOI:10.1016/j.ins.2013.03.031

9. Tanygin M. O., Brusov M.S., Efremova E.O., Sukhorukova Yu.V. [Analysis of the system for monitoring the integrity of chains of information blocks based on hashes]. *Infokommunikatsii i kosmicheskie tekhnologii: sostoyanie, problemy i puti reshe-niya: Materialy III Vserossiiskoi nauchno-prakticheskoi konferentsii* [Infocommunications and space technologies: status, problems and solutions. Proceedings of the III All-Russian Scientific and Practical Conference]. Kursk, 2019, pp. 373 - 378 (In Russ.).

10. Guzeev A.V. Formirovanie raspredeleniya veroyatnostei poyavleniya otdel'nykh soobshchenii istochnika pri statisticheskom kodirovanii [Formation of the probability distribution of the occurrence of individual source messages during statistical coding]. *T-Comm: Telecommunications and transport*, 2010, vol. 4,no. 6, pp. 12-16.

11. Mytsko E.A., Malchukov A.N., Ivanov S.D. Research of algorithms for calculating the CRC8 checksum in microprocessor systems with a shortage of resources. *Devices and systems. Management, control, diagnostics*, 2018, no. 6, pp. 22-29.

12. Bankov Dmitry, Khorov Evgeny, Lyakhov Andrey. On the Limits of LoRaWAN Channel Access. Engineering and Telecommunication (EnT). *2016 International Conference on IEEE*, 2016, pp. 10–14.

13. lantado Ferran, Vilajosana Xavier, Tuset Pere et al. Understanding the Limits of LoRaWAN. *IEEE Communications Magazine*. 2017.

14. Tanygin M.O., Efremov M.A., Tanygina E.A. The Computational Complexity of the Algorithm for Identifying the Source of Data Transmitted by Limited Length Blocks. *Pro-*

ceedings - 2021 International Russian Automation Conference, RusAutoCon 2021, 2021, pp. 298–302.

15. 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]. *Nauchno-metodicheskii elektronnyi zhurnal "Kontsept" = Scientific and methodological electronic journal Concept*, 2015, no. 8, pp. 56-60.

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

17. Vangelista Lorenzo. Frequency Shift Chirp Modulation: The LoRa Modulation. *IEEE Signal Processing Letters*, 2017, vol. 24, no. 12, pp. 1818–1821.

18. Urazbakhtin A.I., Urazbakhtin I.G. Algorithm for checking the homogeneity of the sample and its representativeness to the random process under study. *Infocommunication technologies*, 2006, vol. 4, no. 3, pp. 10-14.

19. Tatyana I. Lapina, Ildus G. Urazbahtin Time series forecasting based on data normalization methods. *Proceedings Volume 6277, Optical Technologies for Telecommunications*, 2005; 62770C (2006).

20. Jorke Pascal, Bocker Stefan, Liedmann Florian, Wietfeld Christian. Urban channel models for smart city IoT-networks based on empirical measurements of LoRa-links at 433 and 868 MHz // *2017 IEEE 28th Annual International Symposium on Personal, Indoor, and Mobile Radio Communications (PIMRC)* / IEEE. 2017. Pp. 1–6.

21. Tanygin M. O., Hemrayev D., Kazakova O. V. Povyshenie dostovernosti opredeleniya istochnika fragmentirovannykh soobshchenii za schet ispol'zovaniya metodov analiza vremeni postupleniya otdel'nykh fragmentov [Increasing the Reliability of Determining the Source of Fragmented Messages by Using Methods for Analyzing the time of Receipt of Individual Fragments]. *Izvestiya Yugo-Zapadnogo gosudarstvennogo universiteta. Seriya: Upravlenie, vychislitel'naya tekhnika, informatika. Meditsinskoe priborostroenie = Proceedings of the Southwest State University. Series: Control, Computing Engineering, Information Science. Medical Instruments Engineering*. 2021; 11(4): 46–60.

Информация об авторах / Information about the Authors

Таныгин Максим Олегович, кандидат технических наук, доцент, заведующий кафедрой информационной безопасности, Юго-Западный государственный университет, г. Курск, Российская Федерация, e-mail: tanygin@yandex.ru

Плугатарев Алексей Владимирович, аспирант кафедры информационной безопасности, Юго-Западный государственный университет, г. Курск, Российская Федерация, e-mail: aplugatarev@bk.ru, ORCID: https://orcid.org/0000-0002-8549-4382

Егоров Сергей Иванович, доктор технических наук, доцент, профессор кафедры вычислительной техники, Юго-Западный государственный университет, г. Курск, Российская Федерация, e-mail: sie58@mail.ru, ORCID: https://orcid.org/0000-0001-5859-1024

Локтионов Аскольд Петрович, доктор технических наук, профессор кафедры электроснабжения, Юго-Западный государственный университет, г. Курск, Российская Федерация, e-mail: loapa@mail.ru, ORCID: https://orcid.org/0000-0003-1108-4185, Researcher ID: P-5434-2015

Maxim O. Tanygin, Cand. of Sci. (Engineering), Associate Professor of Fundamental and Applied Computer Science Department, Southwest State University, Kursk, Russian Federation, e-mail: tanygin@yandex.ru

Aleksey V. Plugatarev, Post-Graduate Student of Fundamental and Applied Computer Science Department, Southwest State University, Kursk, Russian Federation, e-mail: aplugatarev@bk.ru, ORCID: https://orcid.org/0000-0002-8549-4382

Sergey I. Egorov, Dr. of Sci. (Engineering), Associate Professor, Professor of Computer Engineering Department, Southwest State University, Kursk, Russian Federation, e-mail: sie58@mail.ru, ORCID: https://orcid.org/0000-0001-5859-1024

Askold P. Loktionov, Dr. of Sci. (Engineering), Professor of the Department of Power Supply, Southwest State University, Kursk, Russian Federation, e-mail: loapa@mail.ru, ORCID: https://orcid.org/0000-0003-1108-4185, Researcher ID: P-5434-2015