Труды МАИ. 2022. № 125
Trudy MAI, 2022, no. 125

Научная статья
УДК 004.052
DOI: 10.34759/trd-2022-125-20

ПОВЫШЕНИЕ СКОРОСТИ ОПРЕДЕЛЕНИЯ ИСТОЧНИКА СООБЩЕНИЙ ЗА СЧЕТ ОГРАНИЧЕНИЯ МНОЖЕСТВА ОБРАБАТЫВАЕМЫХ БЛОКОВ ДАННЫХ

Максим Олегович Таныгин[1], Алина Андреевна Чеснокова[2]✉,

Ахмад Али Айед Ахмад[3]

[1,2,3]Юго-Западный государственный университет,

Курск, Россия

[1]tanygin@yandex.ru

[2]chesnokova.50@yandex.ru✉

[3]aliayid2013@gmail.ru

Аннотация. Цель исследования состоит в разработке математической модели, позволяющий оценить вычислительную сложность оригинального метода идентификации источника сообщений, в основе которого лежит формирование групп сообщений и проверка для всей группы условия принадлежности целевому источнику. Повышение достоверности и снижение вычислительной сложности в исследуемом методе достигается за счёт предположения о сохранении очерёдности следования сообщений от источника к приёмнику. Это позволяет сократить число

сообщений, участвующих в формировании группы, и, соответственно, сократить число вариантов формирования таких групп.

Для исследования вычислительной сложности алгоритма формирования групп сообщений исследовалось число элементарных операций сравнения хешей таких сообщений – основной операции, определяющей принадлежности конкретного сообщения формируемому структурированному множеству. В качестве параметров модели выступили: длина хеша сообщения, число взаимодействующих субъектов распределённой системы, число сообщений в группе, а также параметр, ограничивающий множество анализируемых сообщений. Процесс поступления сообщений в приёмник был представлен как линейный динамический процесс, характеризуемый в каждый дискретный момент времени вероятностями поступления определённого числа сообщений от целевого источника и от всех остальных источников распределённой системы. Полученные с помощью данной модели результаты позволяют утверждать, что условие гарантированности сохранения последовательности сообщений, поступающих в устройство не изменяет сложность определения источника сообщения, она остаётся линейно зависящей от длины группы сообщений и от числа взаимодействующих в рамках системы устройств. В то же время в абсолютных цифрах число операций сравнения уменьшает на два порядка по сравнению с методом формирования групп, в котором не используется свойство стационарности информационных потоков между компонентами распределённой системы.

Ключевые слова: идентификация источника, вычислительная сложность, математическое моделирование

Для цитирования: Таныгин М.О., Чеснокова А.А., Ахмад А.А. Повышение скорости определения источника сообщений за счет ограничения множества обрабатываемых блоков данных // Труды МАИ. 2022. № 125. DOI: 10.34759/trd-2022-125-20

Original article

INCREASING THE SPEED OF DETERMINING THE SOURCE OF MESSAGES BY LIMITING THE SET OF PROCESSED DATA BLOCKS

Maxim O. Tanygin[1], Alina A. Chesnokova[2]✉, Ahmad Ali Ayed Ahmad[3]

[1.2.3]Southwest State University,

Kursk, Russia

[1]tanygin@yandex.ru

[2]chesnokova.50@yandex.ru✉

[3]aliayid2013@gmail.ru

Abstract. The purpose of the study consists in developing a mathematical model, which allows evaluating the computational complexity of the original method of i the messages source identifying, which is based on forming the groups of messages and checking the condition of belonging to the target source for the entire group. An increase in reliability and decrease in computational complexity in the method under study is being achieved by assuming that the sequence of messages from the source to the receiver is maintained. This allows cutting down the number of messages involved in the group forming, and, accordingly, reduces the number of options for such groups' formation.

To study the computational complexity of the algorithm for the groups of messages forming, the number of elementary operations for comparing hashes of such messages was studied, i.e. of the basic operation determining membership of a particular message to the structured set being formed. The length of the message hash, the number of interacting subjects of the distributed system, a number of messages in the group, as well as the parameter limiting the set of messages being analyzed, were the parameters of the model. The process of messages receipt to the receiver was represented as a linear dynamic process characterized in each discrete time instant by the probabilities of a certain number of messages receipt from the target source and all other sources of the distributed system.

The results obtained with this model allow asserting that the condition of warranty of the messages sequence, received by the device, does not change complexity of the message source detection. It stays linearly dependent on the length of the group of messages and a number of devices interacting in the framework of the system of devices. At the same time, in absolute numbers, the number of comparison operations is reduced by two orders of magnitude compared to the group forming method, which does not employ the stationary property of information flows between the distributed system components.

***Keywords**:* Source identification, computational complexity, mathematical modeling

For citation: Tanygin M.O., Chesnokova A.A., Akhmad A.A. Increasing the speed of determining the source of messages by limiting the set of processed data blocks. *Trudy MAI*, 2022, no. 125. DOI: 10.34759/trd-2022-125-20

Введение

Процедура обработки сообщений, в том числе определения источника сообщений, состоит из трёх основных фаз: приёма сообщения, обработки сообщения и повторной передачи, если обработка была произведена с ошибкой [1]. При этом для конкретного случая третья фаза может отсутствовать, а может повторяться несколько раз [2]. В любом случае её длительность будет определяться достоверностью используемых методов определения источника и длительностью первых двух [3]. В этой связи актуальной становится задача повышения скорости определения источников данных для систем, в которых существует объективное противоречие между размерами сообщений и достоверностью разделения информационных потоков [4, 5]. Указанное противоречие характерно для любого метода, в которых из-за недостаточного размера полей атрибутов или иных служебных данных снижается обработка сообщений происходит не на основании содержимого слов в таких полях, а на основании исчисляемых метрик, формируемых, зачастую не для отдельного сообщения, а для их групп [12 – 15].

Примером могут быть сети связи, обеспечивающие взаимодействие с подвижными объектами, для которых характерна динамическая конфигурация сетей и уровней иерархии абонентов [6]. Данные в них передаются пакетами, для которых может быть сформирован свой маршрут. В результате части одного информационного потока могут быть приняты в разные временные интервалы, перемежаясь пакетами от других устройств [7]. В работе [8] предобработка отдельных сообщений групп осуществляется на основе операций в полях Галуа над двумя матрицами: проверочной, которая может быть сеансовым ключом связи двух

взаимодействующих субъектов, и второй, образуемой векторами сообщений. Результирующая метрика описывает взаимное расположение сообщений в группе друг. Если говорить о сложности алгоритма, то она имеет вид O(A_m^n), где: m – число сообщений, полученных приёмником, n – длина группы сообщений от источника ($n<m$)

Альтернативный метод определения источника сообщений основан на матричных преобразованиях на уровне отдельных блоков [9]. При отправке сообщения объединяются в квадратную матрицу по оригинальному алгоритму, и для такой матрицы исчисляется некоторая метрика. Она отправляется в приёмник и на её основе тот, последовательно переставляя получаемые блоки, получает совпадение с данной метрикой. Подход обладает сложностью O(n!) для восстановления исходной последовательности на стороне приёмника, что делает невозможным его применение для групп из большого числа сообщений. А именно увеличение размера группы позволяет повысить достоверность [19] обработки и определения источника. При определении источника отдельных сообщений, как, например, в изобретениях [9, 10] использована обработка на основе формируемой для каждого сообщения метрики. В первом изобретении данная метрика рассчитывается на основании слова, идентифицирующего абонента, во втором – путём проверки результата декодирования сообщения на основе идентификатора и проверки ошибок за счёт помехоустойчивого кодирования. Эти методы обеспечивают достоверность обработки сообщений, определяемом разрядностью дополнительных полей в сообщении. Для систем [4, 5] она не позволяет достоверно

обрабатывать сообщения, удлиняя эффективную длительность фазы переспроса обработанных с ошибками сообщений.

Формулировка задачи

В качестве предмета исследования был выбран метод определения источника сообщений на основе ограничения множества обрабатываемых приемником блоков данных [12]. В основе метода лежит описанный в [18] подход, заключающийся в построении на основании некоторого решающего правила $\boldsymbol{B}$ (используется совпадение хешей, полученных из предыдущего сообщения группы со значение, записанным в последующем сообщении) из множества поступивших в приёмник сообщений U множества X сообщений целевого источника на основании анализа содержимого аутентифицирующего кода, содержащегося в каждом сообщении множества X, и некоторого слова-идентификатора сеанса связи S^{key}:

$$\begin{aligned} &\exists!\, X \subset U, |X| = n, \quad \boldsymbol{B}\left(X, S^{\text{key}}\right) = 1, \\ &\forall Y \subset U, Y \neq X, |Y| = n, \quad \boldsymbol{B}\left(Y, S^{\text{key}}\right) = 0, \end{aligned} \tag{1}$$

При дополнительной проверке содержимого аутентифицирующего кода, входящего в сообщение, на попадание в динамически формируемый приемником диапазон значений снижается общее число сообщений, анализируемых приемником и повышается достоверность определения источника [12]. За счёт, а так же за счёт уменьшения разрядности H аутентифицирующего кода, достигается общее снижение длительности операции обработки отдельного сообщения. В тоже время выполненный в работе [18] анализ вычислительной сложности исходного метода

показал ограничения, связанные с ростом вычислительной сложности при выполнении условия

$$H < \boldsymbol{log}_2 b, \qquad (2)$$

где b – число взаимодействующих в рамках системы абонентов. Реализованное в модифицированном методе ограничение числа анализируемых блоков за счёт предположения о стационарности свойств информационных потоков от каждого компонента системы позволяет сформировать новые зависимости между вычислительной сложностью и разрядностью аутентифицирующего кода как основа для дальнейшего снижения длительности определения источника сообщений.

Описание метода повышения скорости определения источника сообщения

Согласно [16] метод ограничения множества обрабатываемых сообщений выглядит следующим образом. Для каждого сообщения блока определяется его порядковый номер Q в группе от 1 до n. . Если принять за $M_{\max}$ максимальный порядковый номер всех сообщений, формирующих множество U к произвольному моменту времени, то текущее сообщение будет добавлено ко множеству U, если выполнится условие

$$\boldsymbol{min}(M_{\max} - V, 0) \le Q \le M_{\max} + W, \qquad (3)$$

где V и W – параметры обработки сообщений, ограничивающие множество U

Исследование показали, что метод наиболее чувствителен к параметру V [17], тогда как параметр W, определяющий, на какую величину номер сообщения может превышать максимальный, чтобы сообщение было обработано, не оказывает

значительного влияния на величину ошибки. Кроме того, многие протоколы беспроводной связи созданы по принципу «асинхронная Алоха» [20 – 22], что позволяет при определении вычислительной сложности метода $W = 1$.

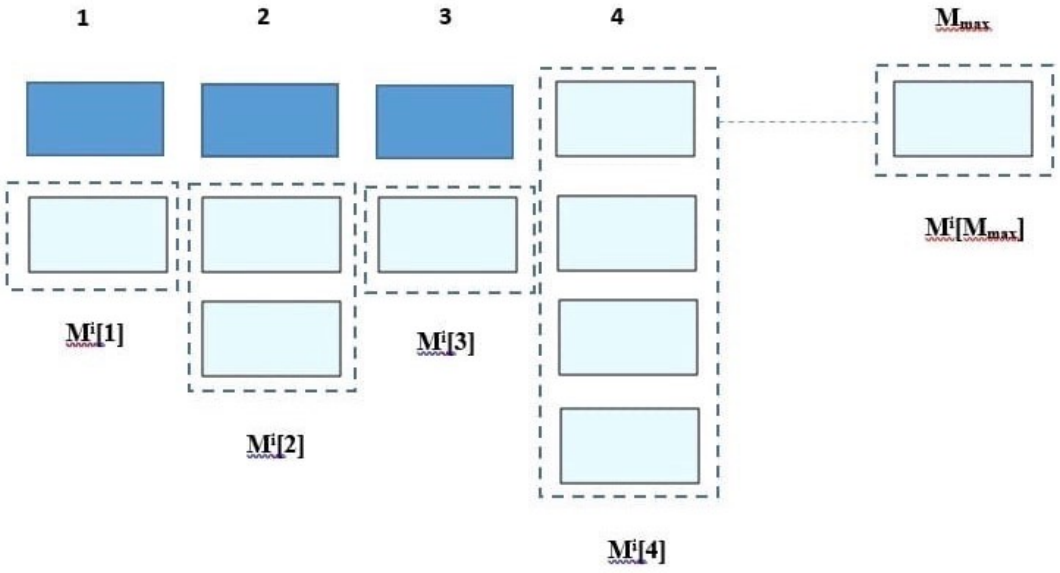

Рисунок 1 – Схематическая структура множества U обрабатываемых сообщений

Для оценки вычислительной сложности метода определения источника с ограничением на число обрабатываемых блоков, рассмотрим сравнение хешей как линейный динамический процесс с дискретным временем. Состояния изменяются внешним событием g, заключающимся в добавлении сообщения в множество U: $G_{i+1} = g(G_i)$. В каждый момент времени $i = \overline{0...b \cdot n}$ процесс характеризуется определенным состоянием. При этом в модели: b число взаимодействующих устройств, $b \cdot n$ – число сообщений, обрабатываемых приёмником за время передачи группы n сообщений целевого источника. В качестве параметров состояния будем использовать: математическое ожидание числа сообщений с номером j, выданных не целевым источником, а посторонними абонентами, в каждой позиции в i-й

момент времени $M^i[j]=0, j=\overline{M_{\max}...n}$; $\gamma^i[j], j=\overline{0...n}$ – вероятности добавления в множество U j – го сообщения из группы n сообщений целевого источника; $\varphi^i[j], j=\overline{0...n}$ – вероятность добавления в множество U сообщения с номером j или вероятность того, что в момент времени i $M_{\max} = j$:

$$G_i=\left\{M^i;\gamma^i;\varphi^i\right\}=\left\{\left\{M^i[1],\gamma^i[1],\varphi^i[1]\right\},...,\left\{M^i[n],\gamma^i[n],\varphi^i[n]\right\}\right\} \quad (4)$$

При каждом поступлении сообщения, хеш, содержащийся в нём, сравнивается с хешами, формируемыми из сообщений, чьи номера находятся в диапазоне, определяемом выражением (1). Математическое ожидание числа операций сравнения хеша в таком случае запишется как:

$$N^i=n^{-1}\sum_{j=1}^{n}(M^i[j]+\gamma^i[j])\cdot(1-\varphi^i[\boldsymbol{min}(j+V,n)]) \quad (5)$$

В формуле учитывается, что номер сообщения с вероятностью n^{-1} примет значение j, такое сообщение должно сравниться с хешем из сообщений целевого источника (вероятность $\gamma^i[j]$) и с хешем из $M^i[j]$ посторонних сообщений. Причём это сравнение происходит с вероятностью $(1-\varphi^i[\boldsymbol{min}(j+V,n)])$, определяемой как вероятность того, что $j > V + M_{\max}$.

Далее, нам необходимо установить соотношения между параметрами состояний i и $i+1$. Отсутствие сообщения источника в позиции j в момент $i+1$ есть вероятность наступления события противоположного совместному наступлению двух событий:

1. Отсутствие сообщения источника в позиции j в момент i;

2. Одновременное отсутствие сообщения в позиции *j-1* и не поступлению очередного сообщения.

Тогда:

$$\gamma^{i+1}(j) = 1 - (1 - \gamma^i(j))(1 - \gamma^i(j-1)b^{-1}), j = \overline{1...n+1} \tag{6}$$

Аналогично получаем выражение для других параметров:

$$\begin{gathered} M^{i+1}(j) = M^i(j) + \left(\gamma^i(j-1) + M^i(j-1)\right) \cdot \frac{b-1}{2^H b} \\ \varphi^{i+1}(j) = 1 - (1 - \varphi^i(j))(1 - \gamma^i(j-1)b^{-1})\left(1 - (\gamma^i(j-1) + M^i(j-1))\frac{b-1}{2^H b}\right), \end{gathered} \tag{7}$$

С учетом формулы (4) математическое ожидание общего числа сравнений хеша имеет вид:

$$N^i = \sum_{i=1}^{b \cdot n} \sum_{j=0}^{[n+1]} \left(M^i[j] + \gamma^i[j]\right) \cdot \left(1 - \varphi^i\left[\boldsymbol{min}(j+V, n)\right]\right) \tag{8}$$

Результаты и их обсуждения

Полученные на основе расчета зависимости числа сравнений от условий передачи приведены на графиках на рисунках 2 и 3

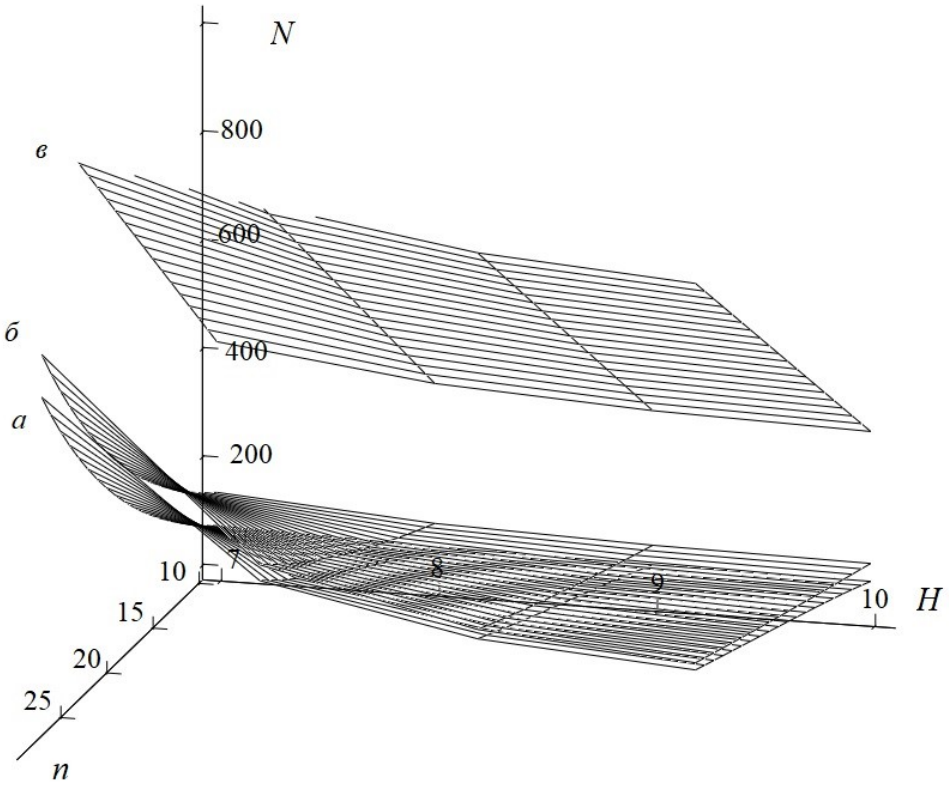

Рисунок 2 – Зависимость числа операций сравнения хешей от размера группы сообщений n и длины хеша сообщения H и значениях параметра V метода ограничения множества обрабатываемых сообщений

а) $V = n - 7$; *б)* $V = n - 2$; *в)* $V = n$ (нет ограничения множества обрабатываемых сообщений)

Из рисунка 2 видно, что уже незначительное ограничение числа сообщений, анализируемых при определении источника, в сочетании с условием сохранения порядка следования сообщений даёт кратное уменьшение (до 4 – 5 раз) снижение числа операций сравнения хешей при выполнении условия (2). Как только вышеозначенное ограничение не соблюдается, наблюдается значительный рост числа сравнений вне зависимости от величины параметра V метода ограничения множества обрабатываемых сообщений.

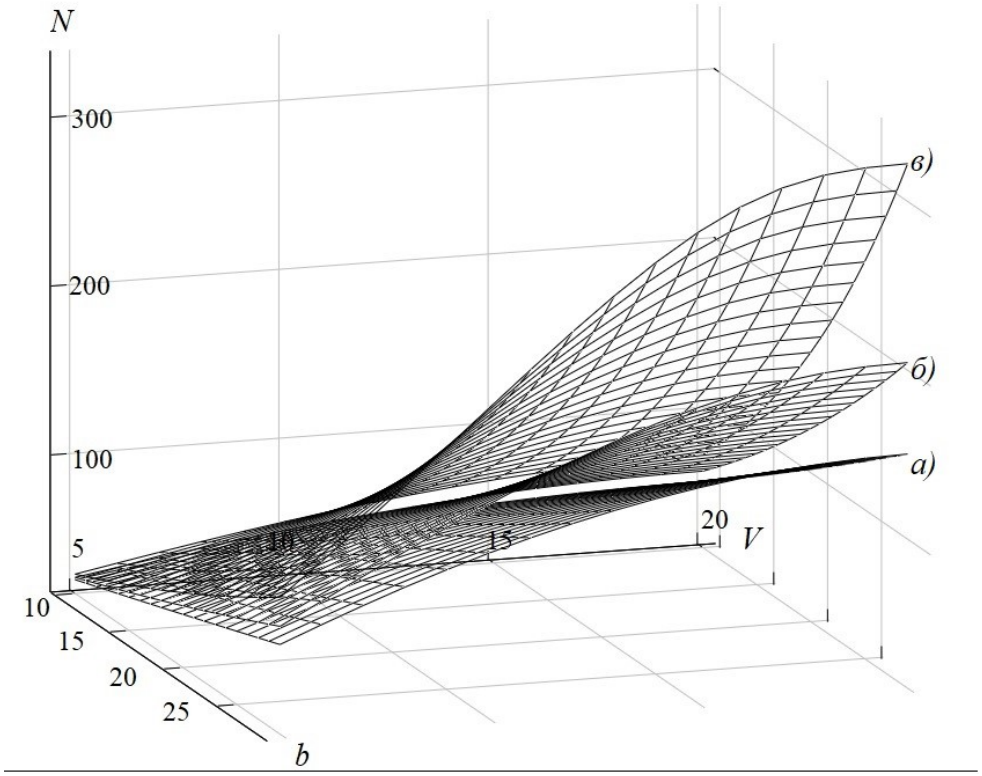

Рисунок 3 – Зависимость числа операций сравнения хешей от параметра V и число взаимодействующих в рамках системы абонентов b при длине группы сообщений n =20 и длине хеша сообщения:

а) H = 10; *б)* H = 8; *в)* H = 7

Более детально влияние длины хеща, используемого для формирования групп сообщений, показано на рисунке 3. Видно, что при выполнении условия (2) зависимость между числом взаимодействующих устройств и числом сравнений линейная. Аналогичная зависимость и межу числом сравнений и параметром V. Проведённые исследования показали, что вычислительная сложность алгоритма определения источника сообщений имеет вид $O(n \cdot V \cdot b)$, как и в оригинальном методе, не предусматривающем ограничения числа поступающих сообщений. Но при этом в абсолютных значениях наблюдается снижение числа типовых операций сравнения хешей в 4 – 5 раз.

Заключение

На основе созданной математической модели обработки сообщений и определения их источника установлено, что использование порядка следования сообщений в потоке в качестве априорной информации, что характерно для метода передачи данных в современных беспроводных сетях [22, 0], используемом в множестве протоколов связи, можно добиться кратного снижения вычислительной сложности алгоритмов определения источника. Следствием этого является повышение общей скорости выполнения операций обработки сообщений для методов, в основе которых для повышения достоверности используется кодирование сообщений в режиме связи блоков. Основной областью применения указанного подхода к обработке сообщений является приёмо-передающее оборудование сетей связи и распределённых систем, в которых из-за физических ограничений и используемых протоколов требуется уменьшение размеров единичного сообщения до значений, при которых таких сообщений невозможно дополнять аутентифицирующими кодам без значительного падения пропускной способности канала связи.

Список источников

1. Волков А.С., Солодков А.В., Суслова К.О., Стрельников А.П. Прототипирование помехоустойчивых кодов в системах связи с кодовым разделением каналов // Труды МАИ. 2021. № 119. https://trudymai.ru/published.php?ID=159789. DOI: 10.34759/trd-2021-119-11

2. Борзов Д.Б., Дюбрюкс С.А., Соколова Ю.В. Метод и методика беспроводной передачи данных в мультипроцессорных системах для нестационарных объектов обмена // Труды МАИ. 2020. № 114. URL: https://trudymai.ru/published.php?ID=118998. DOI: 10.34759/trd-2020-114-13

3. Спеваков А.Г., Калуцкий И.В. Устройство формирования уникальной последовательности, используемой при обезличивании персональных данных // Труды МАИ. 2020. № 115. URL: https://trudymai.ru/published.php?ID=119939. DOI: 10.34759/trd-2020-115-13

4. Предварительный национальный стандарт РФ. Информационные технологии. Интернет вещей. Протокол обмена для высокоемких сетей с большим радиусом действия и низким энергопотреблением. URL: https://drive.google.com/uc?id=12kPw5_ndO8zav7_BP_EXKdytu7uEyy3x&export=download

5. 802.15.4-2015 – IEEE Standard for Low-Rate Wireless Personal Area Networks // IEEE Computer Society. DOI:10.1109/ieeestd.2016.7460875.

6. Кривченко Т. Особенности новой спецификации ZigBee Pro Feature Set // Электронные компоненты. 2006. № 2.

7. Chung-Hua Chu, Yen-Chieh Ouyang and Chang-Bu Jang Secure data transmission with cloud computing in heterogeneous wireless networks // Security and Communication Networks, 2012, vol. 5, issue 12, pp. 1325–1336.

8. Panagiotis Papadimitratos, Zygmunt J. Haas Secure message transmission in mobile ad hoc networks // Ad Hoc Networks, 2003, no. 1, pp. 193–209. DOI:10.1145/941311.941318

9. Shant D., Premkumar P. Block Level Data Integrity Assurance Using Matrix Dialing Method towards High Performance Data Security on Cloud Storage // Circuits and System, 2016, vol. 7, no. 11, pp. 3626-3644. DOI:10.4236/cs.2016.711307

10. Бухарин В.В., Дворядкин В.В., Пикалов Е.Д. и др. Способ и устройство управления потоками данных распределенной информационной системы. Патент RU 2547628 C2, 10.04.2015.

11. Горохов А. Кхандекар Аамод, Борран Мохаммад Д., Пракаш Раджат. Способы и системы для сокращения непроизводительных затрат для обработки для пакетов канала управления. Патент RU 2419219 C2, 20.05.2011.

12. Гавришев А.А., Жук А.П. Обобщенный алгоритм защищенного информационного обмена для бесперебойных систем безопасности с усложненной имитовставкой // Вестник Новосибирского государственного университета. Серия: Информационные технологии. 2019. Т. 17. № 1. С. 18-27. DOI: 10.25205/1818-7900-2019-17-1-18-27

13. Shi X., Xiao D. 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

14. Ben Othman, S., Alzaid H., Trad A., Youssef H. An efficient secure data aggregation scheme for wireless sensor networks // Conference: Information, Intelligence, Systems and Applications, IISA 2013. DOI:10.1109/iisa.2013.6623701

15. Bhattacharjee Arghya, Lopez C.M., List E., Nandi M. The Orbatida v1.3 Family of Lightweight Authenticated Encryption Schemes // Journal of Mathematical Cryptology, 2021, no. 15(1), pp. 305-344. DOI: 10.1515/jmc-2020-0018

16. Таныгин М.О., Добросердов О.Г., Власова А.О., Ахмад А.А. Метод ограничения множества обрабатываемых приёмником блоков данных для повышения достоверности операций определения их источника // Труды МАИ. 2021. № 118. URL: https://trudymai.ru/published.php?ID=158253. DOI: 10.34759/trd-2021-118-14

17. Таныгин М.О. Алшаиа Х.Я., Митрофанов А.В. Сложность алгоритма определения источника данных // Труды МАИ. 2021. № 117. URL: https://trudymai.ru/published.php?ID=156256. DOI: 10.34759/trd-2021-117-12

18. Таныгин М.О. Теоретические основы идентификации источников информации, передаваемой блоками ограниченного размера. - Курск: Университетская книга, 2020. – 198 с.

19. Tanygin M.O., Ali Ayid Ahmad, Dobritsa V.P., Huseyin Polat, Ahmad Ayid Ahmad. Reliability Improvement of Communication Channels Between the Components of Distributed Information Systems // Webology, 2022, vol. 19, no. 2, pp. 5230-5240. DOI 10.34759/trd-2021-117-12

20. Liberg Olof, Sundberg Marten, Wang Eric et al. Cellular Internet of Things: Technologies, Standards, and Performance. Academic Press, 2017.

21. Cellular System Support for Ultra-Low Complexity and Low Throughput Internet of Things: technical report 45.820 v 13.0.0: 3GPP, 2016. URL: https://itectec.com/archive/3gpp-specification-tr-45-820/

22. Pham Congduc. Investigating and Experimenting CSMA Channel Access Mechanisms for LoRa IoT Networks // 2018 IEEE Wireless Communications and Networking Conference (WCNC), 2018. URL: https://doi.org/10.1109/wcnc.2018.8376997

23. Bista R., Jo K., Chang J. A New Approach to Secure Aggregation of Private Data in Wireless Sensor Networks // IEEE International Conference on Dependable, Autonomic and Secure Computing, 2009, pp. 394-399. DOI:10.1109/CIT.2010.79

24.Vikas Kaul V.A., Bharadi P., Dhvani Shah, Narayankhedkar S.K. Security Enhancement for Data Transmission in 3G/4G Networks // International Conference on Computing Communication Control and Automation Pune, India, 2015, pp. 95 - 102. DOI:10.1109/ICCUBEA.2015.25

References

1. Volkov A.S., Solodkov A.V., Suslova K.O., Strel'nikov A.P. *Trudy MAI,* 2021, no. 119. https://trudymai.ru/eng/published.php?ID=159789. DOI: 10.34759/trd-2021-119-11

2. Borzov D.B., Dyubryuks S.A., Sokolova Yu.V. *Trudy MAI*, 2020, no. 114. URL: https://trudymai.ru/eng/published.php?ID=118998. DOI: 10.34759/trd-2020-114-13

3. Spevakov A.G., Kalutskii I.V. *Trudy MAI*, 2020, no. 115. URL: https://trudymai.ru/eng/published.php?ID=119939. DOI: 10.34759/trd-2020-115-13

4. *Predvaritel'nyi natsional'nyi standart RF. Informatsionnye tekhnologii. Internet veshchei. Protokol obmena dlya vysokoemkikh setei s bol'shim radiusom deistviya i nizkim energopotrebleniem*. URL: https://drive.google.com/uc?id=12kPw5_ndO8zav7_BP_EXKdytu7uEyy3x&export=download

5. 802.15.4-2015 – IEEE Standard for Low-Rate Wireless Personal Area Networks, *IEEE Computer Society*. DOI:10.1109/ieeestd.2016.7460875.

6. Krivchenko T. *Elektronnye komponenty*, 2006, no. 2.

7. Chung-Hua Chu, Yen-Chieh Ouyang and Chang-Bu Jang Secure data transmission with cloud computing in heterogeneous wireless networks, *Security and Communication Networks*, 2012, vol. 5, issue 12, pp. 1325–1336.

8. Panagiotis Papadimitratos, Zygmunt J. Haas Secure message transmission in mobile ad hoc networks, *Ad Hoc Networks,* 2003, no. 1, pp. 193–209. DOI:10.1145/941311.941318

9. Shant D., Premkumar P. Block Level Data Integrity Assurance Using Matrix Dialing Method towards High Performance Data Security on Cloud Storage, *Circuits and System,* 2016, vol. 7, no. 11, pp. 3626-3644. DOI:10.4236/cs.2016.711307

10. Bukharin V.V., Dvoryadkin V.V., Pikalov E.D. et al. *Patent RU 2547628 S2*, 10.04.2015.

11. Gorokhov A. Kkhandekar Aamod, Borran Mokhammad D., Prakash Radzhat. *Patent RU 2419219 C2*, 20.05.2011.

12. Gavrishev A.A., Zhuk A.P. *Vestnik Novosibirskogo gosudarstvennogo universiteta. Seriya: Informatsionnye tekhnologii*, 2019, vol. 17, no. 1, pp. 18-27. DOI: 10.25205/1818-7900-2019-17-1-18-27

13. Shi X., Xiao D. 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

14. Ben Othman S., Alzaid H., Trad A., Youssef H. An efficient secure data aggregation scheme for wireless sensor networks, *Conference: Information, Intelligence, Systems and Applications*, IISA 2013. DOI:10.1109/iisa.2013.6623701

15. Bhattacharjee Arghya, Lopez C.M., List E., Nandi M. The Orbatida v1.3 Family of Lightweight Authenticated Encryption Schemes, *Journal of Mathematical Cryptology,* 2021, no. 15(1), pp. 305-344. DOI: 10.1515/jmc-2020-0018

16. Tanygin M.O., Dobroserdov O.G., Vlasova A.O., Akhmad A.A. *Trudy MAI*, 2021, no. 118. URL: https://trudymai.ru/eng/published.php?ID=158253. DOI: 10.34759/trd-2021-118-14

17. Tanygin M.O. Alshaia Kh.Ya., Mitrofanov A.V. *Trudy MAI*, 2021, no. 117. URL: https://trudymai.ru/eng/published.php?ID=156256. DOI: 10.34759/trd-2021-117-12

18. Tanygin M.O. *Teoreticheskie osnovy identifikatsii istochnikov informatsii, peredavaemoi blokami ogranichennogo razmera* (Theoretical foundations of identification of information sources transmitted by blocks of limited size), Kursk, Universitetskaya kniga, 2020, 198 p.

19. Tanygin M.O., Ali Ayid Ahmad, Dobritsa V.P., Huseyin Polat, Ahmad Ayid Ahmad. Reliability Improvement of Communication Channels Between the Components of Distributed Information Systems, *Webology*, 2022, vol. 19, no. 2, pp. 5230-5240. DOI 10.34759/trd-2021-117-12

20. Liberg Olof, Sundberg Marten, Wang Eric et al. *Cellular Internet of Things: Technologies, Standards, and Performance.* Academic Press, 2017

21. *Cellular System Support for Ultra-Low Complexity and Low Throughput Internet of Things: technical report 45.820 v 13.0.0: 3GPP*, 2016. URL: https://itectec.com/archive/3gpp-specification-tr-45-820/

22. Pham Congduc. Investigating and Experimenting CSMA Channel Access Mechanisms for LoRa IoT Networks, *2018 IEEE Wireless Communications and Networking Conference (WCNC)*, 2018. URL: https://doi.org/10.1109/wcnc.2018.8376997

23. Bista R., Jo K., Chang J. A New Approach to Secure Aggregation of Private Data in Wireless Sensor Networks, *IEEE International Conference on Dependable, Autonomic and Secure Computing*, 2009, pp. 394-399. DOI:10.1109/CIT.2010.79

24. Vikas Kaul V.A., Bharadi P., Dhvani Shah, Narayankhedkar S.K. Security Enhancement for Data Transmission in 3G/4G Networks, *International Conference on Computing Communication Control and Automation Pune*, India, 2015, pp. 95 - 102. DOI:10.1109/ICCUBEA.2015.25

Статья поступила в редакцию 28.06.2022
Статья после доработки 30.06.2022
Одобрена после рецензирования 15.07.2022
Принята к публикации 25.08.2022
The article was submitted on 28.06.2022; approved after reviewing on 15.07.2022; accepted for publication on 25.08.2022