Оригинальная статья / Original article

https://doi.org/10.21869/2223-1536-2023-13-3-122-134

УДК 004.052

Модель формирования динамической структуры для установления источника сообщений в памяти приемника

А. А. Чеснокова[1] ✉

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

✉ e-mail: chesnokova.50@yandex.ru

Резюме

Цель исследования *– повышение скорости процедур определения источника данных в режиме сцепления блоков за счет анализа динамической списочной структуры сообщений, формируемой в памяти приемника в результате промежуточных вычислений.*

Методы. *Модель формирования динамической списочной структуры строится на основе аппаратной реализации метода ограничения множества обрабатываемых приемником блоков данных. В состав сообщения входит специальное служебное слово, содержимое которого проверяется на предмет попадания в диапазон значений, формируемый приемником при поступлении каждого блока данных. Описанное ограничение позволяет снизить количество типовых операций сравнения служебных слов, выполняемых при определении источника сообщений, а также снижает вероятность возникновения ошибок определения источника данных.*

Результаты. *На основе модели формирования динамической древовидной списочной структуры получены распределения априорных вероятностей числа узлов определённого уровня в случае возникновения ошибок определения источника данных и без таковых. Это позволяет получить значащие апостериорные вероятности ошибки в зависимости от наблюдаемого числа узлов определённого уровня. Сформулированы критерии принятия решения об ошибке определения источника на основании подсчёта числа узлов до полного завершения формирования древовидной структуры и до этапа её анализа. Это позволяет уменьшить вычислительную сложность процедуры определения источника данных в режиме сцепления блоков и снизить затраты памяти на хранение промежуточных результатов.*

Заключение. *В ходе проведенного исследования было выявлено, что для последовательностей сообщений длиной более 20 обнаружение более чем 8 посторонних ветвей формируемой динамической списочной структуры позволяет с 90%-ной вероятностью утверждать, что процедура определения источника завершилась ошибкой. Отказ от передачи последующих сообщений последовательности и от выполнения операций обработки древовидной структуры позволяет повысить скорость проведения процедуры определения источника сообщений и снизать его вычислительную сложность.*

Ключевые слова: *источник сообщений; информационный поток; древовидная структура; модель; ошибка; априорные вероятности; апостериорная вероятность ошибки.*

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

Для цитирования: Чеснокова А. А. Модель формирования динамической структуры для установления источника сообщений в памяти приемника // Известия Юго-Западного государственного университета. Серия: Управление, вычислительная техника, информатика. Медицинское приборостроение. 2023. Т. 13, № 3. С. 122–134. https://doi.org/10.21869/2223-1536-2023-13-3-122-134.

Поступила в редакцию 11.07.2023 *Подписана в печать 09.08.2023* *Опубликована 29.09.2023*

A Model of Forming a Dynamic Structure for Establishing the Source of Messages in the Receiver's Memory

A. A. Chesnokova[1] ✉

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

✉ e-mail: chesnokova.50@yandex.ru

Abstract

The purpose of research *is increasing the speed of procedures for determining the data source in the block coupling mode, due to the analysis of the dynamic list structure of messages formed in the receiver's memory as a result of intermediate calculations.*

Methods. *The model of forming a dynamic list structure is based on the hardware implementation of the method of limiting the set of data blocks processed by the receiver. The data package includes a special service word, the contents of which are checked for falling into the range of values formed by the receiver when each data block is received. The described restriction reduces the number of typical comparison operations of service words performed when determining the source of messages, and also reduces the likelihood of errors in determining the data source.*

Results. *Based on the model of the formation of a dynamic tree-like list structure, distributions of a priori probabilities of the number of nodes of a certain level are obtained in case of errors in determining the data source and without them. This allows us to obtain significant a posteriori error probabilities depending on the observed number of nodes of a certain level. The criteria for making a decision on the error of determining the source based on the calculation of the number of nodes before the complete completion of the formation of the tree structure and before the stage of its analysis are formulated. This reduces the computational complexity of the procedure for determining the data source in the block coupling mode and reduces the memory costs for storing intermediate results.*

Conclusion. *In the course of the study, it was revealed that for sequences of messages with a length of more than 20, the detection of more than 8 extraneous branches of the dynamic list structure being formed allows us to state with a 90% probability that the procedure for determining the source ended in an error. The refusal to transmit subsequent sequence messages and to perform processing operations of the tree structure allows to increase the speed of the procedure for determining the source of messages and reduce its computational complexity.*

Keywords: *message source; information flow; tree structure; model; error; a priori probabilities; a posteriori error probability.*

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

For citation: Chesnokova A. A. A Model of Forming a Dynamic Structure for Establishing the Source of Messages in the Receiver's Memory. *Izvestiya Yugo-Zapadnogo gosudarstvennogo universiteta. Serija: Upravlenie, vychislitel'naja tekhnika, informatika. Meditsinskoe priborostroenie = Proceedings of the Southwest State University. Series: Control, Computer Engineering, Information Science. Medical Instruments Engineering.* 2023; 13(3): 122–134. (In Russ.) https://doi.org/10.21869/2223-1536-2023-13-3-122-134.

Received 11.07.2023 *Accepted 09.08.2023* *Published 29.09.2023*

***

Введение

Актуальным направлением развития распределенных информационных систем является создание специализированных устройств мониторинга, управления, оценки и анализа состояний технических систем. Работоспособность таких систем зависит от корректности информационного обмена между устройствами. Аутентификация источников является основополагающим элементом обеспечения корректности такого информационного обмена. Идентификация, выявление ошибок определения источника сообщений – одни из основных задач, решаемых устройствами, находящимися в составе таких систем. Корректная обработка поступающих данных повышает достоверность определения источника сообщений.

В случае, если для идентификации используются не методы обработки единичных блоков [1; 2; 3; 4; 5], а методы группового кодирования или кодирования в режиме сцепления блоков [6; 7; 8; 9], выполнение различных преобразований над поступающими данными требует хранения промежуточных результатов. В работе [10] используется матричная структура хранения. В результате обработки проверочной матрицы и значений, формирующихся блоков образуется третья матрица, на основе которой делается вывод о корректности идентификации источника. Для определения источника сообщений применим схожий метод, основанный на формировании квадратичной матрицы данных из отдельных блоков [11]. В работе [12] авторами предложена схема временного хранения данных: часть данных последовательно извлекается из памяти на основе анализа предыдущих данных.

При использовании кодирования в режиме сцепления блоков предпочтительным является использование древовидных структур хранения промежуточных результатов обработки [13].

Любое хранение подобной совокупности данных, находящихся друг с другом в сложных иерархических зависимостях, требует реализации в приёмнике специальных структур [14; 15]. Наиболее распространенные из них: древовидные и матричные структуры – применительно к необходимости хранения структурированных множеств сообщений имеют ряд недостатков. Матричное хранение промежуточных результатов требует дополнительных затрат памяти на хранение повторяющихся элементов множеств. Подобная избыточность затрат внутренней памяти обусловливает выбор древовидной структуры как основы для реализации подсистемы хранения промежуточных результатов [16; 17].

Как показано в [18], вероятность возникновения ошибки определения источника зависит от результатов промежуточных вычислений (числа коллизий в кодах аутентификации блока данных). От числа таких коллизий зависит и сложность формируемых древовидных структур (число ветвей в древовидной структуре, количество блоков данных в ветвях). Таким образом, можно говорить

о том, что формируемая структура промежуточных результатов определяет достоверность определения источника сообщений.

Материалы и методы

В предложенной модели [19] аутентификации сообщений длиной до нескольких байтов с использованием кодирования в режиме сцепления блоков для хранения и обработки сообщений используется древовидная структура, что, в свою очередь, приводит к ряду проблем:

– обработка длинных древовидных структур приводит к большому числу дополнительных вычислений;

– контроль древовидной структуры должен происходить при получении каждого сообщения, что требует дополнительных временных затрат;

– требуется длительное вычисление в случае использования указателей и дополнительные аппаратные затраты на хранение векторов на этапах предобработки древовидной структуры.

Для решения поставленных задач необходимы методы, которые позволяют сигнализировать об ошибке до окончания обработки древовидной структуры при её формировании [20].

В качестве объекта исследования взят алгоритм определения источников сообщений, использующий кодирование в режиме сцепления блоков. Результатами его работы являются формирование в приёмнике последовательностей сообщений и результат проверки условия их принадлежности определённому источнику [5]. В данном методе сравнивается код аутентификации проверяемого сообщения с предварительно сформированной из данных предшествующего сообщения кодовой последовательностью. На основе определения порядка следования сообщений в каждой конкретной паре формируется динамическая структура, представляющая собой ориентированный граф. Пример приведен ниже (рис. 1).

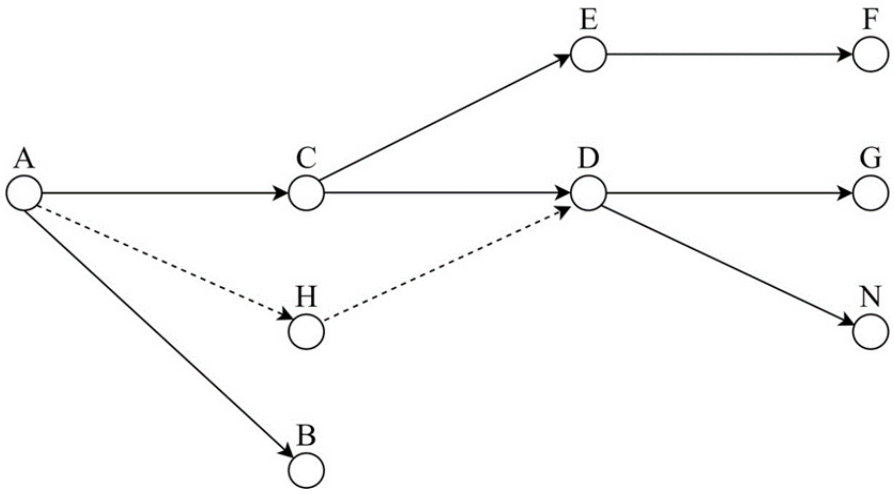

Рис.1. Пример древовидной структуры без ошибки

Fig. 1. Example of a tree structure without an error

Проверка условия возникновения ошибки определения источника происходит после получения последнего сообщения в группе. Предположим, что пришло сообщение H (рис. 1), содержание полей которого позволит добавить его после A, перед D.

Таким образом, формируются две цепочки, которые могут быть определены как последовательность сообщений от одного источника:

1. A – C – D – G.

2. A – H – D – G.

В рамках рассматриваемого подхода установить ту, которая сформирована целевым источником, из двух указанных невозможно, поэтому необходимо сформировать сигнал ошибки аутентификации.

Рассматриваемая в [19] модель хранения промежуточных данных, заключающаяся в комбинировании матричного и списочного подхода, имеющая целью повышение скорости их обработки, приводит к формированию древовидной структуры (рис. 2). Обусловлена такая избыточность тем, что на этапе формирования и хранения, а также на завершающем этапе работы алгоритма – этапе анализа – именно такая древовидная структура значительно эффективнее с точки зрения вычислительных затрат, чем структура с альтернативными маршрутами, представленными на рисунке 1.

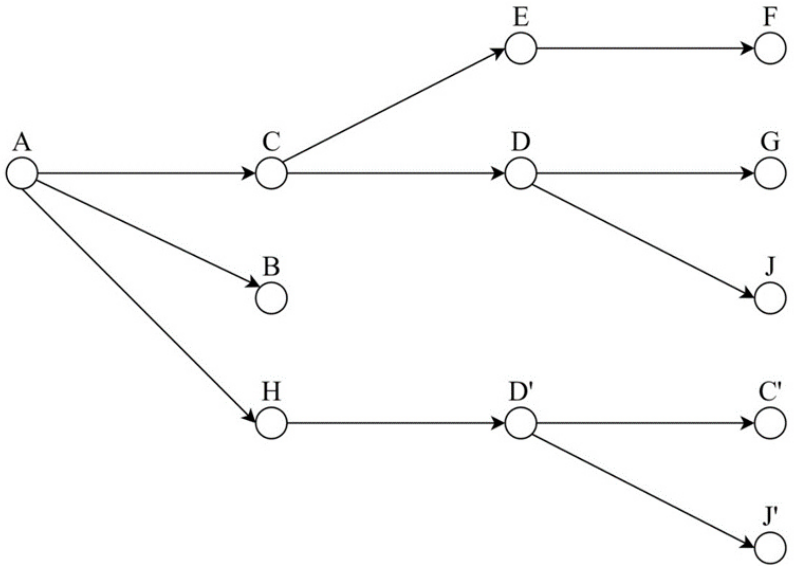

Рис. 2. Пример формирования древовидной структуры с ошибкой

Fig. 2. Example of forming a tree structure with an error

Возникновение ошибки удваивает количество ветвей в древовидной структуре, начиная с позиции, в которой два маршрута ориентированного графа объединились. Таким образом, для ветвей A – C – D – G и A – C – D – J появляются дублирующие их ветви:

1. A – H – D’ – C’.

2. A – H – D’ – J’.

В статье [6] приведена рекуррентная формула для расчета числа ветвей в древовидной структуре при отсутствии ошибок:

$$p_i\left(k_i\right)=\sum_{l=0}^{k_i} p_l^{\{1,\ldots\infty\}} p_{k_i-l}^{\langle 0\rangle},$$

$$p_0\left(k_0\right)=\frac{\left(K\cdot 2^{-H}\right)^{k_0}}{k_0!}e^{-K\cdot 2^{-H}}, \qquad (1)$$

где $p_i(k_i)$ – вероятность формирования ровно k_i ветвей в позиции i, начиная с корня дерева; $p_0(k_0)$ – вероятность формирования ровно k_i ветвей в позиции i, начиная с корня дерева; H – размер поля, входящего в состав каждого сообщения и содержащего аутентификационную информацию; K – параметр модели, равный отношению интенсивности поступления сообщений от всех источников к интенсивности поступления сообщений от целевого источника; $p_{k_i-l}^{\langle 0\rangle}$ – вероятность добавления $k_i - l$ ветвей к каждому сообщению в дереве; $p_l^{\{1,\ldots v\}}$ – вероятность добавления l сообщений к v ветвям, исчисляемая по рекуррентной формуле:

$$p_j^{\{1,\ldots v\}}=\sum_{l=1}^{j} p_{l-1}^{\{v\}} p_{j-l}^{\{v-1\}}. \qquad (2)$$

Вероятность ошибки определения источника $p^{\mathrm{err}}(i)$ после получения i сообщений в данной математической модели определится на основе вероятности возникновения ситуации, проиллюстрированной на рисунке 1:

$$p^{\mathrm{err}}\left(i\right)=\sum_{l=1}^{\infty} p_i\left(l\right)\left(1-2^{-H}\right)^l. \qquad (3)$$

С учётом вероятности возникновения ошибки в позиции $i-1$ и соответственно удвоения числа ветвей, отходящих от основной последовательности после данной позиции (сообщение D на рис. 1), распределение вероятностей $p'_i\left(k_i\right)$ числа ветвей в позиции i будет равно

$$p'_i\left(k_i\right)=\sum_{l=0}^{k_i}\left\{\left[p_l^{\{1,\ldots\infty\}} p_{k_i-l}^{\langle 0\rangle}\right]\times\right.$$

$$\left.\times\left(1-p^{\mathrm{err}}\left(i-1\right)\right)+p_{\left\lceil\frac{k_i-l}{2}\right\rceil}^{\langle 0\rangle} p^{\mathrm{err}}\left(i-1\right)\right\}. \qquad (4)$$

Таким образом, мы получаем априорные вероятности ошибки для случаев с возникновением удвоений ветвей (4) и без них (1). Из этих вероятностей по формуле Байеса

$$p_{\mathrm{apost}}^{\mathrm{err}}=\frac{p'_i\left(k_i\right)}{p_i\left(k_i\right)+p'_i\left(k_i\right)}. \qquad (5)$$

Сравнивая полученные вероятности, получаем значащие апостериорные вероятности ошибок в зависимости от наблюдаемого числа ветвей на определенных уровнях древовидной структуры.

Результаты и их обсуждение

На рисунке 3 приведены зависимости числа m узлов определённого уровня (число ветвей) древовидной структуры от уровня n узла (длины последовательности), при котором вероятность ошибки превышает 0,9.

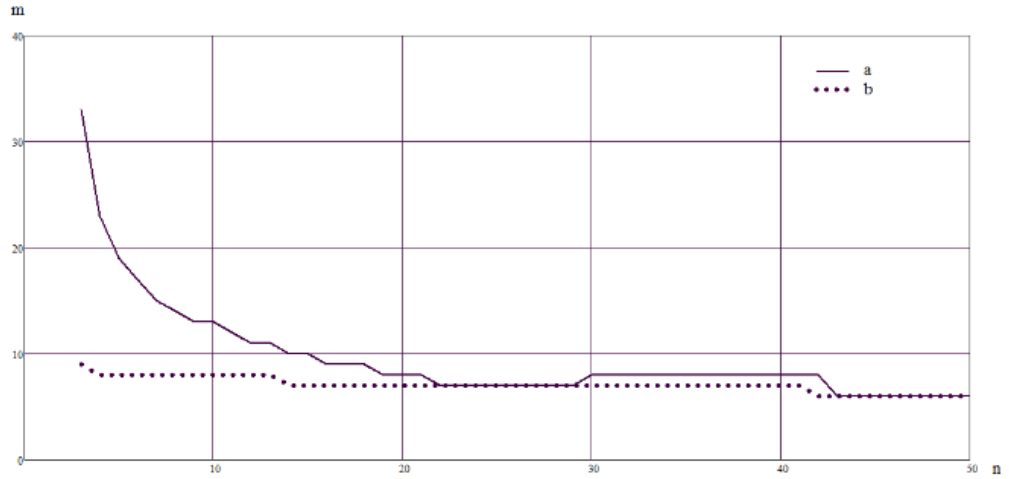

Рис. 3. Границы областей значений длины последовательности сообщений n и числа ветвей древовидной структуры m, при которых вероятность безошибочной идентификации p_{pl} > 90% при параметре модели K = 75 и длине поля, входящего в состав каждого сообщения: a – H = 7; b – H = 9

Fig. 3. The boundaries of the ranges of values of the length of the message sequence n and the number of branches of the tree structure m, at which the probability of error-free identification of p_{pl} > 90% with the model parameter K = 75 and the length of the field included in each message: a – H = 7; b – H = 9

Из графика (рис. 3) видно, что с увеличением длины поля H уменьшается количество посторонних ветвей, при которых можно с 90%-ной вероятностью говорить о возникновении ошибки идентификации источника сообщений. Особенно это заметно в области небольших значений длины последовательности сообщений от целевого источника ($n < 20$).

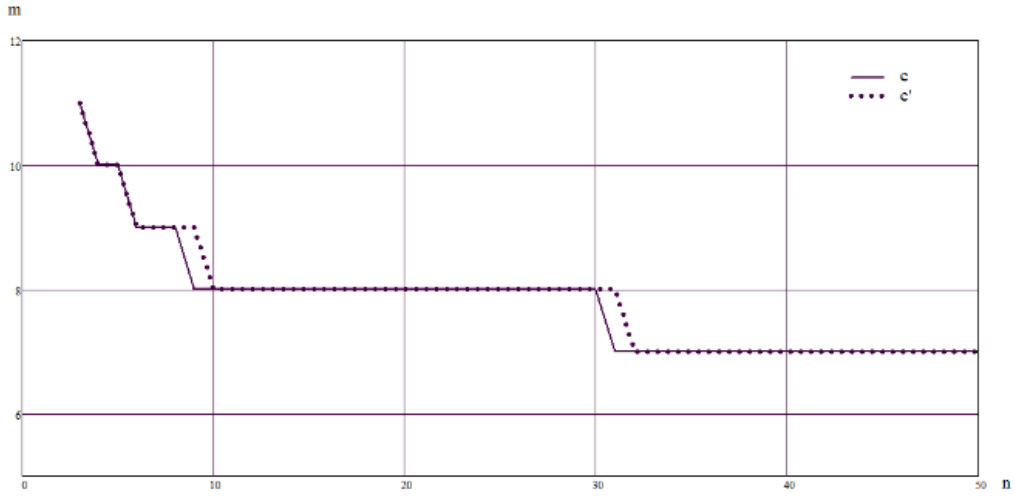

Рис. 4. Границы областей значений длины последовательности сообщений n и числа ветвей древовидной структуры m, при которых вероятность безошибочной идентификации p_{pl} > 90% при: c – K = 75, H = 8; c' – K = 80, H = 8

Fig. 4. The boundaries of the regions of values of the length of the message sequence n and the number of branches of the tree structure m, at which the probability of error-free identification of p_{pl} > 90% at: c – K = 75, H = 8; c' – K = 80, H = 8

Из графика, представленного на рисунке 4, видно, что отношение K интенсивности поступления сообщений от всех источников к интенсивности поступления сообщений от целевого источника не оказывает значимого влияния на размер и расположение на плоскости области, в которой вероятность безошибочной идентификации более 90%.

Выводы

Проведенное исследование показало следующее:

1. Метод определения ошибки может применяться для последовательностей длиной более 20.

2. Для последовательностей меньшей длины, для обнаружения ошибки требуется выполнение соотношения между длиной поля, содержащего аутентификационную информацию, и отношением интенсивностей поступления сообщением от всех источников и от целевого источника: $2^{H-2} > 2$, определенного как целесообразное с точки зрения затрат памяти для хранения элементов древовидной структуры. В то же время при таком соотношении между H и K вероятность формирования $m > 5$ ветвей ничтожно мала (менее 10^{-4}). В этом случае подсчет числа ветвей для обнаружения ошибки проводить нецелесообразно.

3. На основе п. 1 и п. 2 сформулированы критерии применимости рассматриваемого подхода. Для последовательностей, кодированных в режиме сцепления блоков, длиной более 20, при средней интенсивности поступления сообщений в приемник, превышающей интенсивность сообщений от источника не более чем в 2^{H-2} раз, ошибка идентификации обнаруживается с вероятностью более 90% при числе узлов древовидной структуры, обладающих одинаковым уровнем (числе ветвей на определенном расстоянии от корня дерева) больше 8.

В общем случае предложенный подход позволяет реализовывать алгоритмы обнаружения ошибок до этапа анализа древовидной структур, что снижает трудоёмкость процедур идентификации удалённого источника, снижает временные затраты на передачу заведомо ошибочной цепочки, которые были бы необходимы без использования анализа промежуточных структур данных. Наиболее эффективным его применение оказывается при обработке последовательностей большой длины, для которых использование кодирования в режиме сцепления блоков для идентификации источников данных сопряжено с высокими вычислительными затратами. В качестве направлений дальнейших исследований можно отметить разработку алгоритмов поиска дублирующих последовательностей в описанных древовидных структурах, что позволило бы повысить скорость и достоверность обнаружения ошибок идентификации.

Список литературы

1. Hashemipour-Nazari M., Goossens K., Balatsoukas-Stimming A. Multi-Factor Pruning for Recursive Projection-Aggregation Decoding of RM Codes // 2022 IEEE Workshop on Signal Processing Systems (SiPS). Rennes, France, 2022. P. 1–6. https://doi.org: 10.1109/SiPS55645.2022.9919209.

2. Пат. 2547628 Российская Федерация, H04L 9/32, H04L 12/801. Способ и устройство управления потоками данных распределенной информационной системы / Бухарин В. В., Дворядкин В. В., Пикалов Е. Д., Романюк О. В., Куленич А. И. Ступаков И. Г. Заявл. 05.08.13; опубл. 10.04.15.

3. Мыцко Е. А, Мальчуков А. Н., Иванов С. Д. Исследование алгоритмов вычисления контрольной суммы CRC8 в микропроцессорных системах при дефиците ресурсов // Приборы и системы. Управление, контроль, диагностика. 2018. № 6. С. 22–29.

4. Пат. 1140141 Российская Федерация, A1 SU G08C 19/28. Устройство для приема и обработки избыточной информации / Зубков Ю. П., Ключко В. И., Николаев Ю. И., Петухов В. Е. Устинов Г. Н. Заявл. 27.06.83; опубл. 15.02. 85.

5. Толоманенко Е. А. Дифференциальный анализ трех раундов шифра «Кузнечик» // Доклады Томского государственного университета систем управления и радиоэлектроники. 2018. Т. 21, № 2. С. 22–26. https://doi.org: 10.21293/1818-0442-2018-21-2-22-26.

6. WCCP: A congestion control protocol for wireless multimedia communication in sensor networks / S. M. Aghdam, M. Khansari, H. Rabiee, M. Salehi // Ad Hoc Networks. 2014. Vol. 13. P. 516–534.

7. Bellare M., Kilian J., Rogaway P. The security of the cipher block chaining message authentication code // JCSS. 1994. Vol. 3, N 3. P. 341–358.

8. Black J., Rogaway P. CBC MACs for arbitrary-length messages: The three-key constructions // J. Cryptol. 2005. Vol. 18, N 2. P. 111–131.

9. Stallings W. NIST Block Cipher Modes of Operation for Authentication and Combined Confidentiality and Authentication // Cryptologia. 2010. N 34. P. 225–235.

10. Panos Papadimitratos, Zygmunt J. Haas Secure message transmission in mobile ad hoc networks // Ad Hoc Networks. 2003. N 1(1). P. 193–209.

11. Premkumar P., Shanthi D. Block Level Data Integrity Assurance Using Matrix Dialing Method towards High Performance Data Security on Cloud Storage // Scientific Research Publishing. 2016. Vol. 7, N 11. P. 3626–3644.

12. A real-time motion estimation FPGA architecture / K. Babionitakis, G. A. Doumenis, G. Georgakarakos [et al.] // J. Real-Time Image Proc. 2008. N 3. P. 3–20. https://doi.org/10.1007/s11554-007-0070-9.

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

14. Черемисинов Д. И., Черемисинова Л. Д. Задачи обработки больших графов (graph mining) // Big Data and Advanced Analytics. 2019. № 5. С. 328–333.

15. Колганов А. С. Параллельная реализация алгоритма поиска минимальных остовных деревьев с использованием центрального и графического процессоров // Вестник Южно-Уральского государственного университета. Серия: Вычислительная математика и информатика. 2016. Т. 5, № 3. С. 5–19. https://doi.org/ 10.14529/cmse160301.

16. Tasci S., Demirbas M. Employing in-memory data grids for distributed graph processing // IEEE 2015 IEEE International Conference on Big Data (Big Data). Santa Clara, CA, USA: IEEE, 2015. P. 1856–1864. https://doi.org/10.1109/bigdata.2015.7363959.

17. Paradies M., Lehner W., Bornhövd C. GRAPHITE: an extensible graph traversal framework for relational database management systems // Proceedings of the 27th International Conference on Scientific and Statistical Database Management. New York, United States: Association for Computing Machinery, 2015. P. 1–15. https://doi.org/10.1145/2791347.2791383.

18. Повышение скорости обнаружения ошибок при формировании цепочек блоков данных на основе анализа числа совпадений хешей / М. О. Таныгин, Е. А. Кулешова, А. В. Митрофанов, Е. Ю. Гладилина // Прикаспийский журнал: управление и высокие технологии. 2022. № 1(57). С. 85–93. https://doi.org/10.54398/2074-1707_2022_1_85.

19. Метод ограничения множества обрабатываемых приёмником блоков данных для повышения достоверности операций определения их источника / М. О. Таныгин, О. Г. Добросердов, А. О. Власова, А. А. Ахмад // Труды МАИ. 2021. Т. 118, № 3. С. 15. https://doi.org/10.34759/trd-2021-118-14.

20. Таныгин М. О., Чеснокова А., Ахмад А. А. А. Снижение ресурсных затрат на обработку кодов аутентификации сообщений за счет ограничения числа обрабатываемых сообщений // Прикаспийский журнал: управление и высокие технологии. 2022. № 4(60). С. 22–29.

References

1. Hashemipour-Nazari M., Goossens K., Balatsoukas-Stimming A. Multi-Factor Pruning for Recursive Projection-Aggregation Decoding of RM Codes. 2022 IEEE Workshop on Signal Processing Systems (SiPS). Rennes, France, 2022, pp. 1–6. https://doi.org/ 10.1109/SiPS55645.2022.9919209

2. Bukharin V. V., e. a. Sposob i ustrojstvo upravleniya potokami dannyh raspredelennoj informacionnoj sistemy [Method and device for controlling data flows of a distributed information system]. Patent RF, no. 2547628, 2015.

3. Mytsko E. A., Malchukov A. N., Ivanov S. D. Issledovanie algoritmov vychisleniya kontrol'noj summy CRC8 v mikroprocessornyh sistemah pri deficite resursov [Investigation of algorithms for calculating the CRC8 checksum in microprocessor systems with a shortage of resources]. *Pribory i sistemy. Upravlenie, kontrol', diagnostika = Devices and Systems. Management, Control, Diagnostics*, 2018, no. 6, pp. 22–29.

4. Zubkov Yu. P., e. a. Ustrojstvo dlya priema i obrabotki izbytochnoj informacii [Device for receiving and processing redundant information]. Patent RF, no. 1140141, 2015.

5. Tolomanenko E. A. Differencial'nyj analiz trekh raundov shifra "Kuznechik" [Differential analysis of three rounds of the cipher "Grasshopper"]. *Doklady Tomskogo gosudarstvennogo universiteta sistem upravleniya i radioelektroniki = Reports of Tomsk State University of Control Systems and Radioelectronics*, 2018, vol. 21, no. 2, pp. 22–26. https://doi.org/10.21293/1818-0442-2018-21-2-22-26

6. Aghdam S. M., Khansari M., Rabiee H., Salehi M. WCCP: A congestion control protocol for wireless multimedia communication in sensor networks. *Ad Hoc Networks*, 2014, vol. 13, pp. 516–534.

7. Bellare M., Kilian J., Rogaway P. The security of the cipher block chaining message authentication code. *JCSS*, 1994, vol. 3, no. 3, pp. 341–358.

8. Black J., Rogaway P. CBC MACs for arbitrary-length messages: The three-key constructions. *J. Cryptol*, 2005, vol. 18, no. 2, pp. 111–131.

9. Stallings W. NIST Block Cipher Modes of Operation for Authentication and Combined Confidentiality and Authentication. *Cryptologia*, 2010, no. 34, pp. 225–235.

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

11. Premkumar P., Shanthi D. Block Level Data Integrity Assurance Using Matrix Dialing Method towards High Performance Data Security on Cloud Storage. *Scientific Research Publishing*, 2016, vol. 7(11), pp. 3626–3644.

12. Babionitakis K., Doumenis G. A., Georgakarakos, G. eds. A real-time motion estimation FPGA architecture. *J. Real-Time Image Proc.*, 2008, no. 3, pp. 3–20. https://doi.org/10.1007/s11554-007-0070-9

13. Tanygin M. O., Chesnokova A. A., Ahmad A. A. A. Povyshenie skorosti opredeleniya istochnika soobshchenij za schet ogranicheniya mnozhestva obrabatyvaemyh blokov dannyh [Increasing the speed of determining the source of messages by limiting the set of processed data blocks]. *Trudy MAI = Proceedings of MAI*, 2022, no. 125. https://doi.org/10.34759/trd-2022-125-20

14. Cheremisinov D. I., Cheremisinova L. D. Zadachi obrabotki bol'shih grafov (graph mining) [Tasks of processing large graphs (graph mining)]. *Big Data and Advanced Analytics*, 2019, no. 5, pp. 328-333.

15. Kolganov A. S. Parallel'naya realizaciya algoritma poiska minimal'nyh ostovnyh derev'ev s ispol'zovaniem central'nogo i graficheskogo processorov [Parallel implementation of the algorithm for finding minimum threshold values using centralized and graphical processes]. *Vestnik Yuzhno-Ural'skogo gosudarstvennogo universiteta. Seriya: Vychislitel'naya matematika i informatika = Bulletin of the South Ural University. Series: Computational Mathematics and Computer Science*, 2016, vol. 5, no. 3, pp. 5–19. https://doi.org/10.14529/cmse160301

16. Tasci S., Demirbas M. Employing in-memory data grids for distributed graph processing // IEEE 2015 IEEE International Conference on Big Data (Big Data). Santa Clara, CA, USA, IEEE Publ., 2015, pp. 1856–1864. https://doi.org/10.1109/bigdata.2015.7363959

17. Paradies M., Lehner W., Bornhövd C. GRAPHITE: an extensible graph traversal framework for relational database management systems. Proceedings of the 27th International Conference on Scientific and Statistical Database Management. New York, United States, Association for Computing Machinery Publ., 2015, pp. 1–15. https://doi.org/10.1145/2791347.2791383

18. Tanygin M. O., Kuleshova E. A., Mitrofanov A. V., Gladilina E. Y. Povyshenie skorosti obnaruzheniya oshibok pri formirovanii cepochek blokov dannyh na osnove analiza chisla sovpadenij heshej [Increasing the speed of error detection in the formation of data block chains based on the analysis of the number of hash matches]. *Prikaspijskij zhurnal: upravlenie i vysokie tekhnologii = Caspian Journal: Management and High Technologies*, 2022, no. 1(57), pp. 85–93. https://doi.org/10.54398/2074-1707_2022_1_85

19. Tanygin M. O., Dobroserdov O. G., Vlasova A. O., Ahmad A. A. Metod ogranicheniya mnozhestva obrabatyvaemyh priyomnikom blokov dannyh dlya povysheniya dostovernosti operacij opredeleniya ih istochnika [Method of limiting the set of data blocks processed by the receiver to increase the reliability of operations for determining their source]. *Trudy MAI = Proceedings of MAI*, 2021, vol. 118, no. 3, p. 15. https://doi.org/10.34759/trd-2021-118-14

20. Tanygin M. O., Chesnokova A. A., Akhmad A. A. A. Snizhenie resursnyh zatrat na obrabotku kodov autentifikacii soobshchenij za schet ogranicheniya chisla obrabatyvaemyh soobshchenij [Reduction of resource costs for processing message authentication codes by limiting the number of processed messages]. *Prikaspijskij zhurnal: upravlenie i vysokie tekhnologii = Caspian Journal: Management and High Technologies*, 2022, no. 4(60), pp. 22–29.

Информация об авторе / Information about the Author

Чеснокова Алина Андреевна, ассистент
кафедры информационной безопасности,
Юго-Западный государственный университет,
г. Курск, Российская Федерация,
e-mail: chesnokova.50@yandex.ru,
ORCID: 0000-0003-1183-4572

Alina A. Chesnokova, Assistant
of the Department of Information Security,
Southwest State University,
Kursk, Russian Federation,
e-mail: chesnokova.50@yandex.ru,
ORCID: 0000-0003-1183-4572