Оригинальная статья / Original article

https://doi.org/10.21869/2223-1560-2023-27-4-62-78

Сегментация древовидных структур данных и их параллельная обработка в методах аутентификации, основанных на кодировании в режиме сцепления блоков

М.О. Таныгин [1] ✉, А.А. Чеснокова [1]

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

✉ e-mail: tanygin@yandex.ru

Резюме

Цель исследования. *В задачах аутентификации групп сообщений, кодированных в режиме сцепления блоков, возникает необходимость формирования и обработки специфических древовидных структур. Содержимое таких структур, помимо информации о размещении данных во внутренней памяти вычислителей, описывает взаимное расположение сообщений в потоке данных между абонентами одноранговой сети. Данная информация необходима для выделения из всего потока сообщений в приёмник структурированного множества, для которого однозначно определён его источник. Использование подходов к сегментации древовидных структур позволяет распараллелить процессы добавления элементов в неё и поиска участков, соответствующих ошибке аутентификации.*

Методы. *В основе разбиения древовидной структуры на области, подлежащие модификации, и участки для анализа, лежит динамически формируемая из кодов аутентификации сообщений метрика – позиция конкретного сообщения в структурированном множестве сообщений, предаваемых от источника в приёмник. Значение данной метрики определяет расстояние от корня дерева, определяющее границу между двумя названными областями.*

Результаты. *За счёт изолирования модифицируемого и анализируемого участков древовидной структуры исключаются гонки процессов, реализующих независимые алгоритмы работы с ней. Показана возможность обнаружения ошибок аутентификации до получения последнего сообщения в структурированном множестве сообщений. В результате отпадает необходимость передачи тех сообщений группы, отправка которых предполагалась после момента обнаружения ошибки. Приведены формулы оценки среднего времени передачи множества сообщений при последовательной и параллельной реализации процедур формирования и обработки древовидной структуры, содержащей описатели поступающих в приёмник сообщений.*

Заключение. *В работе показано, что параллельная реализация алгоритмов добавления элементов в древовидную структуру и алгоритма поиска участков, соответствующих ошибке, позволяет уменьшить среднее время передачи группы сообщений на 5 -12% по сравнению с последовательной реализацией указанных алгоритмов. Это снижает нагрузку на канал связи для целевого класса систем, использующих для аутентификации кодирование в режиме сцепления блоков.*

Ключевые слова: *аутентификация; кодирование; древовидные структуры данных; сегментация данных; параллелизм.*

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

Для цитирования: Таныгин М.О., Чеснокова А.А. Сегментация древовидных структур данных и их параллельная обработка в методах аутентификации, основанных на кодировании в режиме сцепления блоков // *И*звестия Юго-Западного государственного университета. 2023; 27(4): 62-78. https://doi.org/10.21869/2223-1560-2023-27-4-62-78.

Поступила в редакцию 18.10.2023 *Подписана в печать 07.11.2023* *Опубликована 21.12.2023*

Segmentation of Tree-Like Data Structures and Their Parallel Processing in Authentication Methods Based on Block Coupling Encoding

Maxim O. Tanygin [1] ✉, Alina A. Chesnokova [1]

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

✉ e-mail: tanygin@yandex.ru

Abstract

Purpose of reseach. *In the tasks of authenticating groups of messages encoded in the mode of chaining blocks, there is a need for the formation and processing of specific tree-like structures. The contents of such structures, in addition to information about the placement of data in the internal memory of the calculators, describes the relative location of messages in the data stream between subscribers of a peer-to-peer network. This information is necessary to isolate a structured set from the entire message stream to the receiver, for which its source is uniquely determined. Using approaches to segmentation of tree structures allows you to parallelize the processes of adding elements to it and searching for areas corresponding to an authentication error.*

Methods*. The division of the tree structure into areas subject to modification and areas for analysis is based on a metric dynamically formed from message authentication codes – the position of a specific message in a structured set of messages transmitted from the source to the receiver. The value of this metric determines the distance from the root of the tree, which defines the boundary between the two named areas*

Results*. By isolating the modified and analyzed sections of the tree structure, races of processes implementing independent algorithms for working with it are excluded. The possibility of detecting authentication errors before receiving the last message in a structured set of messages is shown. As a result, there is no need to transmit those group messages that were supposed to be sent after the error was detected. Formulas for estimating the average transmission time of multiple messages with sequential and parallel implementation of procedures for the formation and processing of a tree structure containing descriptors of incoming messages to the receiver are given.*

Conclusion*. The paper shows that the parallel implementation of algorithms for adding elements to the tree structure and the algorithm for searching for areas corresponding to an error reduces the average transmission time of a group of messages by 5-12% compared with the sequential implementation of these algorithms. This reduces the load on the communication channel for the target class of systems using block coupling encoding for authentication.*

Keywords: *authentication; coding; tree-like data structures; data segmentation; parallelism.*

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

For citation: Tanygin M. O., Chesnokova A. A. Segmentation of Tree-Like Data Structures and Their Parallel Processing in Authentication Methods Based on Block Coupling Encoding. *Izvestiya Yugo-Zapadnogo gosudarstvennogo universiteta = Proceedings of the Southwest State University*. 2023; 27(4): 62-78 (In Russ.). https://doi.org/10.21869/2223-1560-2023-27-4-62-78.

Received 18.10.2023 *Accepted 07.11.2023* *Published 21.12.2023*

***

Введение

Использование кодирования в режиме сцепления блоков для задач аутентификации абонентов распределённых сетей впервые было предложено Белларом, Килианом и Роджавэем [1]. Он основан на использовании при формировании кодов аутентификации текущего сообщения данных предшествующего. Идея объединения сообщений для их последующей аутентификации получила дальнейшее развитие в работах [2-6]. Основное направление данного подхода – повышение достоверности аутентификации в условиях ограниченного размера кодов аутентификации сообщений, который при использовании традиционных криптографических протоколов, ориентированных на аутентификацию источника изолированного сообщения, не обеспечивает требуемую достоверность [7]. Недостатком метода является высокая вычислительная сложность алгоритмов обработки групп сообщений и большие временные задержки, возникающие из-за необходимости реализовывать такие алгоритмы только после получения последнего сообщения в последовательности. С учетом вышесказанного практическое применение данного подхода возможно в сетях связи с низкой пропускной способностью [8]: в сенсорных сетях и сетях интернета вещей. Для них эффект от сокращения размеров дополнительных служебных полей, содержащих коды аутентификации сообщений, нивелирует указанные дополнительные временные затраты.

При реализации методов аутентификации в сетях, работающих по принципу peer-to-peer, задача определения источника сообщений сводится к задаче формирования и обработке списочной древовидной структуры, которая описывает варианты взаимного расположения поступающих сообщений в потоке данных от источника в приёмник [9]. С учётом того, что устройства, реализующие указанные процедуры, обладают невысокой производительностью и аппаратной сложностью, определение принципов обработки древовидной структуры должно, подходов к синтезу аппаратных модулей, выполняющих обработку, должно осуществляться с учётом необходимости оптимизации ресурсов для её хранения. В работах [10-12] представлены подходы к хранению и обработке списочных структур, в которых повышение производительности и скорости обработки обеспечивается путём парализации процесса перебора маршрутов перемещения по графу. В то же время поиск маршрута есть операция доступа на чтение к графовой структуре (порожда-

емая процессом-потребителем), тогда как добавление элемента (порождаемое процессом производителем) в дерево подразумевает модификацию данных. Соответственно, параллельная реализация процедур обработки маршрутов и добавления сообщений могут порождать гонки [13]. Соответственно, при реализации алгоритмов ускоренной обработки формируемых при проведении аутентификации графов, будут требоваться механизмы синхронизации двух указанных типов процессов [14]. Подобная проблема рассмотрена в статье [15], где описана схема, в которой для анализа предыдущих данных предварительно извлекается часть информации и хранится в кеше с высокой скоростью доступа. Таким образом разрешается задача изоляции структур данных, в которые производится запись и структур, из которых происходит чтение.

В то же время решение задач полного перебора, к которым относятся задачи поиска элементов в графе, подразумевает необходимость реализации методов и алгоритмов, учитывающих особенности формируемых графов и особенности осуществления обращения к ним [16, 17]. В нашем случае подходом к минимизации числа операций сравнения кодов аутентификации при добавлении элементов в граф является ограничение области, куда добавление элемента может происходить. Он лежит в основе метода ограничения числа обрабатываемых сообщений при выполнении процедуры аутентификации [18], в котором происходит отказ от обработки сообщений, которые не удовлетворяют динамически вычисляемому критерию для содержимого поля аутентификации. Применительно к задаче формирования древовидного графа это выражается в невозможности встраивания нового элемента в определённые его позиции. В конечном итоге это выражается в уменьшении числа элементов такого дерева и уменьшении числа отдельных его ветвей.

При этом влияние методов повышения производительности будет выражаться не столько в повышении скорости операций обработки кодов аутентификации, что важно для анонимных peer-to-peer сетей [19], но в общем повышении производительности канала связи за счёт повышения скорости обнаружения ошибки аутентификации и скорости переспроса таких ошибочно переданных данных [20]. Снижение времени, прошедшего между началом передачи пакетов данных и временем возникновения переспроса наиболее критично для сетей с низкой пропускной способностью [21], для которых и целесообразно применение аутентификации на основе кодирования в режиме сцепления блоков данных

Это же является предпосылкой к разработке алгоритмов и технических решений, обеспечивающих повышение скорости формирования и обработки древовидной структуры в задачах аутентификации за счёт сегментации такой структуры на области, к которым в асин-

хронном режиме осуществляют доступ независимые потоки управления, реализующие операции добавления элементов в структуру (формирования графа) и операции его анализа (поиска участков, соответствующих ошибке аутентификации).

Материалы и методы

Согласно принципам обработки поступающих сообщений, для управления их обработкой используется косвенная адресация, при которой само сообщение буферизируется в оперативную память, а адреса хранятся в регистровой памяти [9] в виде специальных записей $\{Q_i\}$ $i = 1\ldots$ U^{rec} , U^{rec} – количество принятых и обработанных приёмником сообщений (рис. 1), объединённых в динамическую древовидную структуру-граф, формируемую при поступлении сообщений и обрабатываемую при выполнении процедуры аутентификации их источника [23]. Кроме адреса Q^{adr}, по которому в буферном ОЗУ записано сообщение, в такой записи содержится ещё ряд вспомогательных полей, требуемых для процедур обработки сообщений: Q^{aut}, Q^{next}, которые используются для проверки кодов аутентификации поступающих сообщений, а также массив G (рис. 1), содержащий указатели на элементы древовидной структуры, следующими за текущей. С учётом целесообразности комбинации списочной (в которой адресация выполняется за счёт указателей) и матричной (с адресацией за счёт индексов элемента) систем хранения множества структуру $\{Q\}$ [9], элементы массива G представляют собой номера $\{g_1 \ldots g_n\}$ строк матричной памяти, в которых элементы древовидной структуры, следующими за текущей. При этом номер столбцов предшествующей и последующей записи отличается на один.

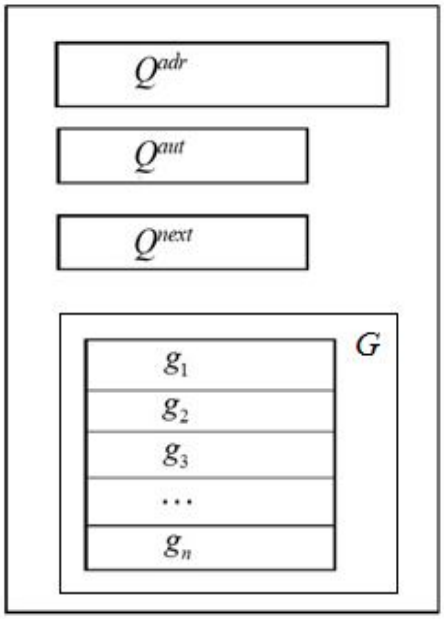

Рис. 1. Структура записи, ассоциированной с буферизованным в оперативной памяти сообщением

Fig. 1. The structure of the record associated with the message buffered in RAM

Формируется древовидная структура в результате выполнения итерационного алгоритма обработки поступающих сообщений, представленного на рис. 2. В его основе лежит метод обработки групп сообщений [22], кодированных в режиме сцепления блоков.

Используемые при описании алгоритма обозначения:

f^{md} – операция декодирования содержимого поля блока, в котором содержится индекс;

$W^{i,j}$ – множество сформированных указателей на следующий элемент в графе сообщений у элемента, размещённого в *i*-й строке и *j*-м столбце регистровой памяти, каждый указатель – номер строки в *j*+1 столбце, в котором содержится последующий элемент последовательности сообщений;

$g_k^{i,\text{y}}$ – содержимое указателя с номером *k* у элемента, размещённого в *i*-й строке и *j*-м столбце регистровой памяти, совокупность таких указателей образует множество $W^{i,j}$;

$Q_{i,j}$ – отдельный элемент регистровой памяти, размещённый в её *i*-й строке и *j*-м столбце, размер элемента в битах определяется, исходя из реальных условий эксплуатации вычислителя;

$s_{i,y}^{\text{inf}}$ – данные сообщения, описатель которого размещён в *i*-й строке и *j*-м столбце регистровой памяти;

$s_{i,y}^{aut}$ – КПДПБ блока, описатель которого размещён в *i*-й строке и *j*-м столбце регистровой памяти;

$Q^{\langle y \rangle}$ – содержимое *j*-го столбца регистровой памяти;

$\left|Q^{\langle y \rangle}\right|$ – число занятых регистров в *j*-м столбце регистровой памяти.

Особенности аппаратной реализации процедуры формирования динамической структуры заключаются в асинхронном доступе различных вычислительных модулей к блокам памяти, хранящим записи $\{Q_i\}$ $i = 1 \ldots U^{\text{rec}}$, используемые для косвенной адресации буферизированных сообщений. При этом доступ на запись в блоки памяти реализуется блоками, которые формируют динамическую списочную структуру. Модули, которые осуществляют анализ динамической структуры, обращаются к указателям только в режиме чтения. Такой режим позволяет реализовывать процедуру анализа динамической структуры параллельно с её формированием. Результатом анализа динамической структуры является поиск в ней участков, представленных на рис. 3. На рисунке:

j – порядковый номер сообщения в последовательности, в котором образовалась структура, соответствующая ошибке идентификации;

i_1 и i_2 – номера записи в столбце *j*, в которых произошли коллизии в полях: $Q_{i_1,j}^{aut}$ и $Q_{i_2,j}^{aut}$, $Q_{i_1,j}^{next}$ и $Q_{i_2,j}^{next}$ соответственно;

k_1 и k_2 – порядковые номера указателей в записи $Q_{i_3,j-1}$ ссылающиеся на записи $Q_{i_1,j}$ и $Q_{i_2,j}$ в столбце *j*, образуя структуру, соответствующую ошибки определения источника сообщений и тот же элемент $Q_{i_4,j+1}$ +1;

k_3 и k_4 – порядковые номера указателей в записях $Q_{i_1,j}$ и $Q_{i_2,j}$ ссылающиеся на один и тот же элемент $Q_{i_4,j+1}$ в столбце *j*+1.

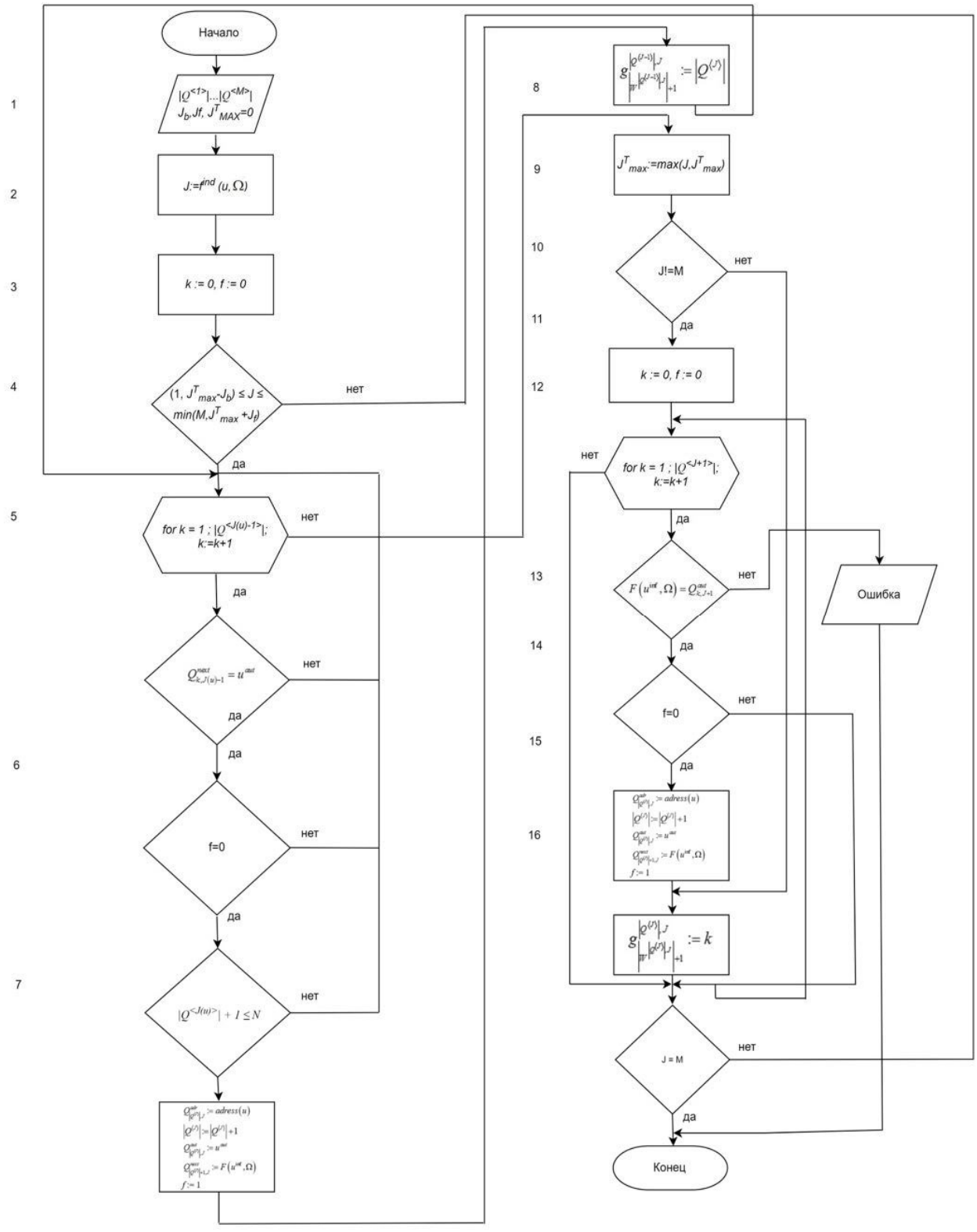

Рис. 2. Формализованный алгоритм формирования динамической структуры, содержащей промежуточные результаты вычислений при аутентификации источника последовательности сообщений

Fig. 2. A formalized algorithm for forming a dynamic structure containing intermediate results of calculations when authenticating the source of a message sequence

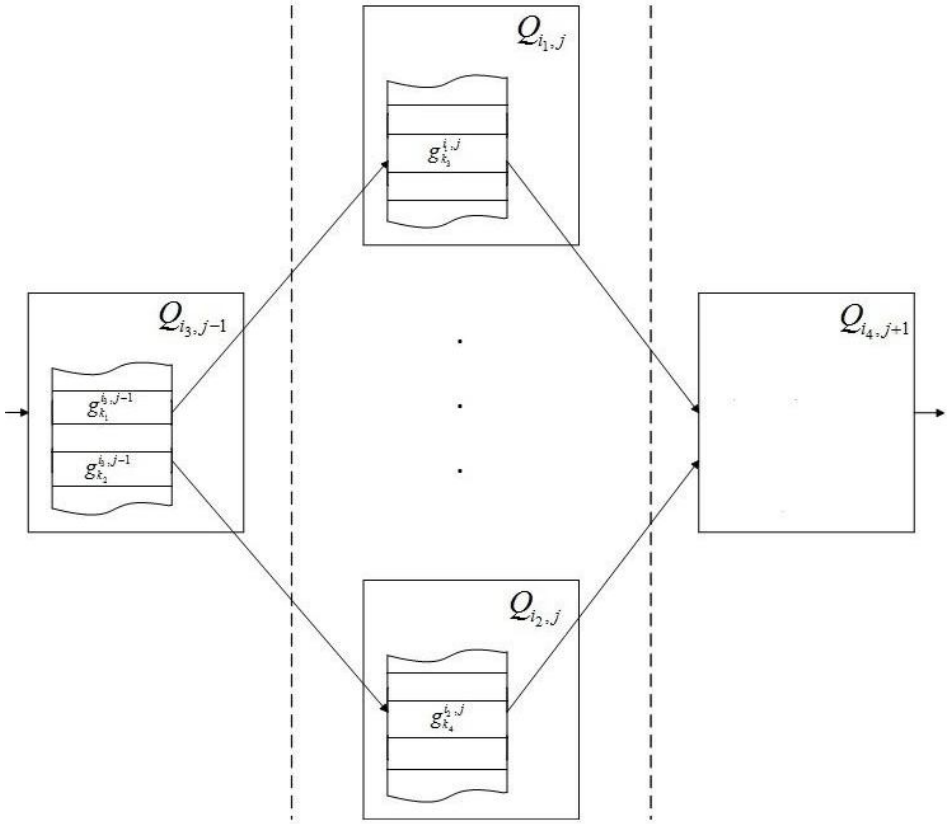

Рис. 3. Пример участка динамической структуры, соответствующий ошибке аутентификации

Fig. 3. An example of a section of a dynamic structure corresponding to an authentication error

При такой конфигурации во всей динамической древовидной структуре могут быть сформированы две и более последовательности определённой протоколом передачи длины *M*. Метод аутентификации не позволяет определить ту последовательность, которая образована сообщениями, сформированными целевым источником.

Условие возникновение ошибки в принятых нами обозначениях выглядит следующим образом:

$$g_k^{i,j} = W^{i,j} = \left\{ g_1^{i,j}, g_2^{i,j}, \ldots \right\}$$

$$g_k^{i,j} = W^{i,j} = \left\{ g_1^{i,j}, g_2^{i,j}, \ldots \right\} \qquad (1)$$

$$x1, x2 \in 0 \ldots G^{i3,j-1}, x1 \neq x2 .$$

При этом пренебрежимо мала (менее 10^{-3}) вероятность формирования коллизий, при которых в альтернативных ветвях содержится две и более структуры. Поэтому в настоящей работе мы не рассматриваем такие варианты возникновения ошибок аутентификации

Это же свойство методов аутентификации, основанных на кодировании в режиме сцепления блоков, является предпосылкой для формирования методов ограничений на добавление в древовидную структуру сообщений в позиции, отстоящей на фиксированное число позиций J от окончания самой длинной ветви [24]. Таким образов после записи в память древовидной структуры блока с номером позиции $J_{\max}$, для её элементов с порядковыми номерами $J_{\max}$–J можно производить поиск кон-

струкций, приведённых на рис. 3 в соответствии с формулами (1). Тем самым осуществляется изоляция двух областей динамической структуры: находящихся на расстоянии, меньшем чем J_{max}–J от корня дерева, в которой возможен анализ структуры, и находящихся на расстоянии большем J_{max}–J от корня – для которой реализуется алгоритм добавления элементов (см. рис. 3) Алгоритм, реализующий поиск структур, соответствующих ошибке идентификации, приведён на рис. 4.

Номер в позиции, в которой произошла ошибка определения источника сообщения, распределён по равномерному закону. Формула для определения вероятности возникновения ошибки в определенной позиции выглядит следующим образом:

$$p\left(J^{err}\right)=\frac{1}{M}. \quad (2)$$

Описанный выше алгоритм определения ошибки позволяет определять ошибки с порядковым номером, не превышающим $M - J_{max}$. Прекращая дальнейшее формирование и обработку динамической структуры, содержащей указатели на оперативную память.

Результаты и их обсуждение

Пусть T^{rec}- время передачи последовательности из M сообщений, для которых выполняется процедура аутентификации. Тогда ошибка в позиции, большей M-J , обнаруживается лишь после получения сообщения последовательности и среднее время получения группы сообщений с такой ошибкой равно T^{rec}.

Если ошибка происходит в позиции с номером $1 \le j \le M - J$, то она обнаруживается после получения сообщения с номером j+J. Тогда, с учетом равномерного закона распределения номера позиции ошибки, среднее время получения группы сообщений будет $\frac{J+1+M}{2}$. Тогда математическое ожидание получения группы сообщений с учетом досрочного прекращения передачи после обнаружения ошибки, равно $T^{err}=\frac{J}{M}T^{rec}+\frac{M-J}{M}\cdot\frac{M+J+1}{2}$.

Для математического ожидания времени передачи группы сообщений с учетом вероятности ошибки p^{err}

$$T_1^{rec}=T^{rec}\cdot\left(1-p^{err}\right)+$$
$$+p^{err}\left[\left(T^{rec}\frac{(M-J)(M+J+1)+2J}{2M}+T_2^{rec}\right)\right], \quad (3)$$

где второе слагаемое T_2^{rec} в квадратных скобках есть время, которое будет затрачено при переспросе группы из всех M сообщений в случае, если при первой попытке была обнаружена ошибка аутентификации. Оно, в свою очередь, может вырасти из-за возникновения ошибки аутентификации уже при переспросе. Таким образом, мы имеем рекурсивную формулу для средней длительности i-й попытки передачи последовательности сообщений:

$$T_i^{rec}=T^{rec}\cdot\left(1-p^{err}\right)+$$
$$+p^{err}\left[\left(T^{rec}\frac{(M-J)(M+J+1)+2JM}{2M^2}+T_{i+1}^{rec}\right)\right]. \quad (4)$$

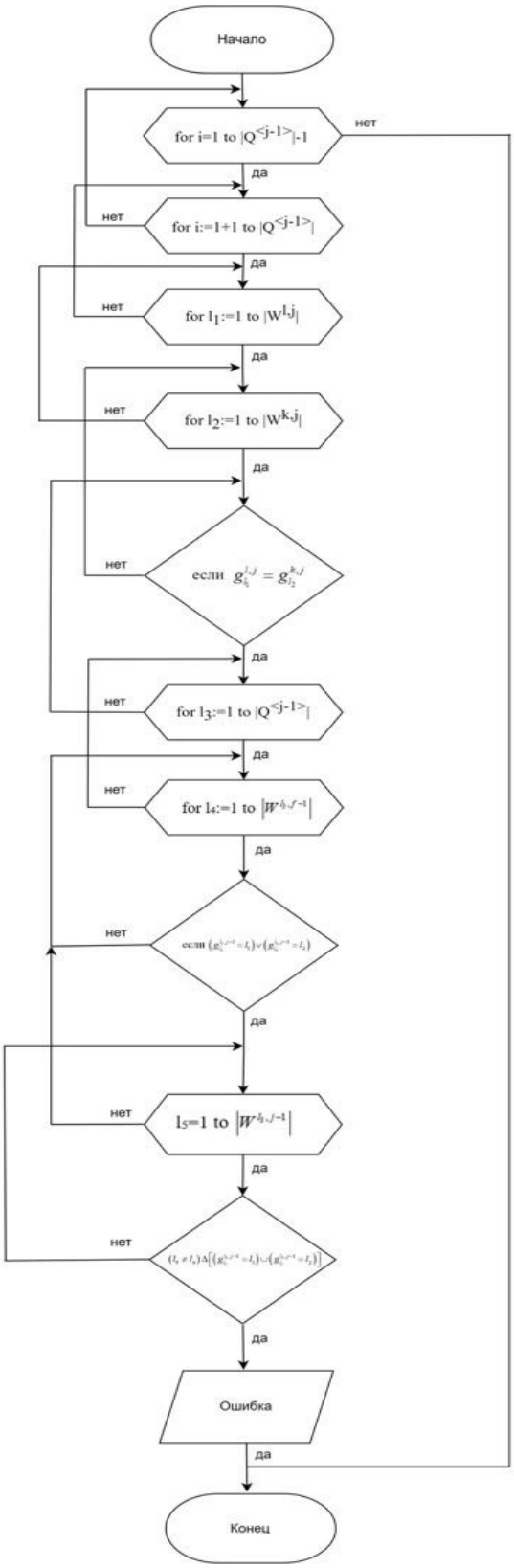

Рис. 4. Блок схема алгоритма обработки древовидной структуры для участка, соответствующего ошибке аутентификации

Fig. 4. Block diagram of the tree structure processing algorithm for the section corresponding to the authentication error

Математическое ожидание времени передачи группы сообщений без использования описанного выше алгоритма поиска ошибки аутентификации исчисляется по формуле

$$T^{\text{orig}} = T^{rec} \cdot \left(1 - p^{err}\right)^{-1}. \qquad (5)$$

Отношение K – математического ожидания времени передачи группы сообщений при использовании алгоритма обработки древовидных структуры T_1^{rec} к математическому ожиданию времени передачи группы сообщений без использования описанного выше алгоритма T^{orig} приведено на графиках на рис. 5.

При варьировании параметра обработки групп сообщений при фиксированной вероятности ошибки аутентификации p^{err} наблюдается следующая картина (рис. 6).

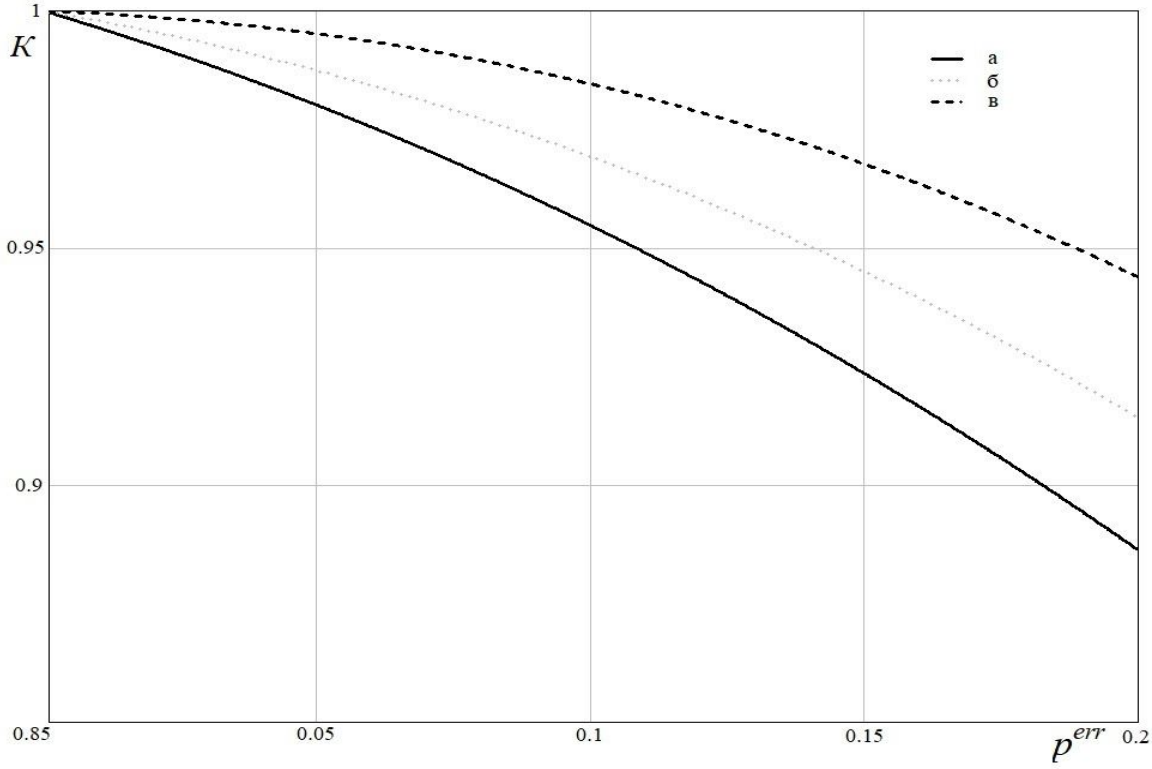

Рис. 5. Зависимость отношения K – математического ожидания времени передачи группы сообщений при параллельной работе алгоритма обработки и алгоритма формирования древовидных структур T_1^{rec} к математическому ожиданию времени передачи группы сообщений без последовательной работы алгоритмов T^{orig} от вероятности возникновения ошибки аутентификации p^{err} при передаче группы сообщений при длине группы M =15: **а** – J =2, **б** – J =5, **в** – J =10

Fig. 5. The dependence of the ratio of the K– mathematical expectation of the transmission time of a group of messages during the parallel operation of the processing algorithm and the algorithm for the formation of tree structures T_1^{rec} on the mathematical expectation of the transmission time of a group of messages without sequential operation of algorithms T^{orig} on the probability of an authentication error p^{err} when transmitting a group of messages with a group length M =15: **а** – J =2, **б** – J =5, **в** – J =10

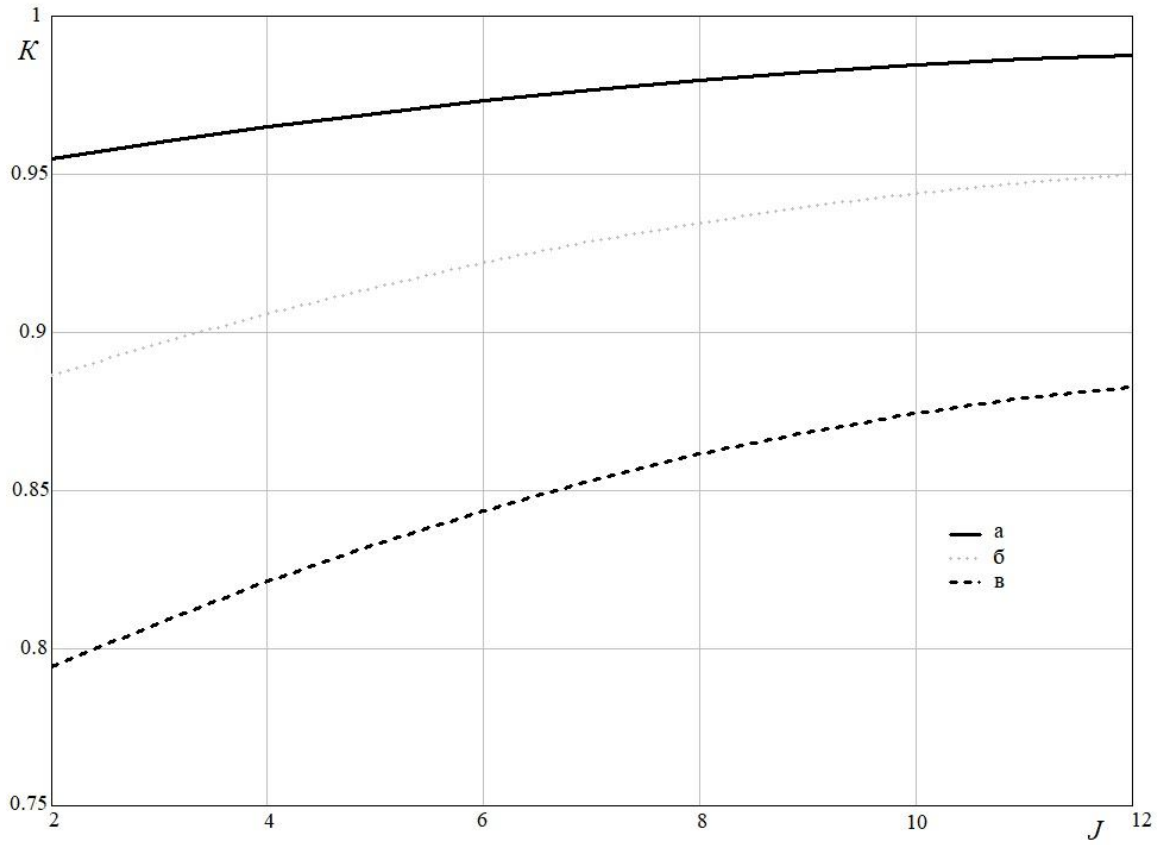

Рис. 6. Зависимость отношения K – математического ожидания времени передачи группы сообщений при параллельной работе алгоритма обработки и алгоритма формирования древовидных структур T_1^{rec} к математическому ожиданию времени передачи группы сообщений при последовательной работе алгоритмов T^{orig} от параметра обработки групп сообщений J при M =15. **а –** p^{err} =0,1, **б –** p^{err} =0,2, **в** – p^{err} =0,3

Fig. 6. The dependence of the ratio of K – he mathematical expectation of the transmission time of a group of messages during the parallel operation of the processing algorithm and the algorithm for the formation of tree structures T_1^{rec} on the mathematical expectation of the transmission time of a group of messages during the sequential operation of the algorithms T^{orig} on the processing parameter of message groups J at M =15. **а –** p^{err} =0,1, **б –** p^{err} =0,2, **в** – p^{err} =0,3

Анализ полученных результатов подтверждает эффективность применения параллельной работы алгоритмов формирования и анализа древовидного графа, выражающегося в снижении математического ожидания времени передачи группы сообщений относительно методов, в которых данные операции реализуются последовательно. При этом целевая характеристика K снижается с увеличением вероятности ошибки аутентификации. На рис. 6 приведены её значения для диапазона ошибок, допустимых протоколами передачи данных с низкой пропускной способностью и большим радиусом действия [25]. Увеличение же параметра J – величины, определяющей область модификации древовидной структуры, наоборот, повышает целевое соотношение, снижая результативность параллелизации работы двух алгоритмов.

Выводы

Рассмотренный в статье подход к обработке промежуточных результатов при выполнении процедуры аутентификации источника группы сообщений нацелен прежде всего на упреждающее определение ошибок до момента передачи всей групп. Так как в целевом классе информационных систем – систем, компоненты которых взаимодействуют по протоколам с низкой пропускной способностью, именно длительность передачи сообщений вносит основные задержки при организации информационного обмена. Прекращение передачи после обнаружения ошибки и до момента поступления последнего сообщения в группе позволяет снизить математическое ожидание времени передачи последовательности, которое определяется как длительностью передачи группы сообщений, так и длительностью переспроса в результате ошибки. Проведённые исследования показали, что в зависимости от вероятности ошибки аутентификации и параметра же параметра J – величины, определяющей область модификации древовидной структуры, математическое ожидания времени передачи групп сообщений снижается на 5 -12%..

Список литературы

1. Bellare M., Kilian J., Rogaway P. The security of the cipher block chaining message authentication code. M. // Journal of Computer and System Sciences. 2000 61(3): pp. 362-399 DOI: 10.1006/jcss.1999.1694

2. Iwata T., Kurosawa K. OMAC: one-key CBC MAC // Fast Software Encryption. 2003. P. 129 – 53.

3. Dworkin M. SP 800-38D: Recommendation for Block Cipher Modes of Operation: Galois/Counter Mode (GCM) and GMAC, 2007.

4. Dworkin M. Recommendatin for Block Cipher Modes of Operation: The CCM Mode for Authentication and Confidentiality // Nist Spec. Publ. 2004. Vol. 800. 38 p.

5. Stallings W. The advanced encryption standard // Cryptologia. 2002. Vol. 26. № 3. P. 165–188.

6. Black J. Authenticated Encryption // Encycl. Cryptogr. Secur. 2005. P. 11–21.

7. Black J., Rogaway P. CBC MACs for arbitrary-length messages: The three-key constructions // J. Cryptol. 2005. Vol. 18. № 2. P. 111–131.

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

9. Модель размещения данных во внутренней памяти вычислителя, реализующего схему кодирования данных в режиме сцепления блоков / М.О. Таныгин, А.А. Ахмад, О.В. Казакова, Д.А. Голубов // Известия Юго-Западного государственного университета. 2023; 27(1): 73-91. https://doi.org/10.21869/2223-1560-2023-27-1-73-91.

10. Пасечников К. А., Иванова Г. С. Синтез оптимальных структур данных для решения задач на графах // Вестник Московского государственного технического университета им. Н.Э. Баумана. Серия Приборостроение. 2008. № 4(73). С. 29-37.

11. 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. DOI 10.14529/cmse160301

12. Tasci S., Demirbas, M Employing in-memory data grids for distributed graph processing // IEEE 2015 IEEE International Conference on Big Data (Big Data), 2015, pp. 1856–1864. doi:10.1109/bigdata.2015.7363959

13. Волчихин В. И., Вашкевич Н. П., Бикташев Р. А. Модели событийных недетерминированных автоматов представления алгоритмов управления взаимодействующими процессами в многопроцессорных вычислительных системах на основе использования механизма монитора // Известия высших учебных заведений. Поволжский регион. Технические науки. 2013. № 2(26). С. 5-14.

14. Courtois P. J., Heymans F., Parnas D. L. Concurrent Control with "Readers" and "Writers" // Communications of the ACM. 14 (10), 1971. P. 667–668. doi:10.1145/362759.362813. S2CID 7540747.

15. Babionitakis K., Doumenis G.A., Georgakarakos G. et al. A real-time motion estimation FPGA architecture // J. Real-Time Image Proc. 2008. № 3. Pp. 3–20. https://doi.org/10.1007/s11554-007-0070-9

16. Дородных Н. О., Юрин А. Ю. Подход к автоматизированному наполнению графов знаний сущностями на основе анализа таблиц // Онтология проектирования. 2022. Т. 12. № 3(45). С. 336-352. DOI 10.18287/2223-9537-2022-12-3-336-352.

17. Путнин В. И. Автоматизация процесса построения расписания с применением топологической сортировки на графе // E-Scio. 2021. № 3(54). С. 584-588.

18. 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. 15 doi 10.34759/trd-2021-118-14.

19. Modinger D., Frohlich N., Hauck F.J. Pixy: A Privacy-Increasing Group Creation Scheme // Conference: ICNCC 2020: 2020 The 9th International Conference on Networks, Communication and Computing. December 2020 DOI: 10.1145/3447654.3447671.

20. Хабибулин Н. Ф., Шкердин А. Н., Щербенко А. Н. Повышение пропускной способности систем передачи с переспросом за счет введения дополнительной связи между процессами декодирования с исправлением и обнаружением ошибок // Науковедение. 2016. Т. 8, № 3(34). С. 143.

21. Тучкин А. В. Принципы функционирования протокола канального уровня для пакетной передачи разнородного трафика по низкоскоростным каналам // T-Comm: Телекоммуникации и транспорт. 2008. Т. 2, № 3. С. 31-33.

22. Мальцев Г. Н. Помехоустойчивость и скрытность передачи информации по радиоканалам на основе комбинированного случайного кодирования // Информационно-управляющие системы. 2015. № 2(75). С. 82-89. DOI 10.15217/issn1684-8853.2015.2.82

23. Таныгин М. О., Чеснокова А. 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.

24. 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. DOI 10.34759/trd-2022-125-20.

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

References

1. Bellare M., Kilian J., Rogaway P. The security of the cipher block chaining message authentication code. *Journal of Computer and System Sciences*, 2000. 61(3):pp. 362-399 DOI: 10.1006/jcss.1999.1694

2. Iwata T., Kurosawa K. OMAC: one-key CBC MAC. *Fast Software Encryption*, 2003, pp. 129 – 53.

3. Dworkin M. SP 800-38D: Recommendation for Block Cipher Modes of Operation: Galois/Counter Mode (GCM) and GMAC, 2007.

4. Dworkin M. Recommendatin for Block Cipher Modes of Operation: The CCM Mode for Authentication and Confidentiality. *Nist Spec*. Publ., 2004, vol. 800, 38 p.

5. Stallings W. The advanced encryption standard. *Cryptologia*, 2002, vol. 26, no. 3, pp. 165–188.

6. Black J. Authenticated Encryption. Encycl. Cryptogr. Secur., 2005, pp. 11–21.

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

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

9. Tanygin M. O., Ahmad A.A., Kazakova O. V., Golubov D. A. Recursive Algorithm for Forming Structured Sets of Information Blocks that Increase the Speed of Performing Procedures for Determining Their Source. *Izvestiya Yugo-Zapadnogo gosudarstvennogo universiteta = Proceedings of the Southwest State University*. 2023; 27(1): 73-91 (In Russ.). https://doi.org/10.21869/2223-1560-2023-27-1-73-91.

10. Pasechnikov K.A., Ivanova G.S. Sintez optimal'nykh struktur dannykh dlya resheniya zadach na grafakh [Synthesis of optimal data structures for solving problems on graphs]. *Vestnik Moskovskogo gosudarstvennogo tekhnicheskogo universiteta im. N.E. Baumana. Seriya Priborostroenie = Bulletin of the Bauman Moscow State Technical University*, 2008, no. 4(73), pp. 29-37.

11. Kolganov A.S. Parallel'naya realizatsiya algoritma poiska minimal'nykh ostovnykh derev'ev s ispol'zovaniem tsentral'nogo i graficheskogo protsessorov [Parallel implementation of minimum spanning tree algorithm on CPU and GPU]. *Vestnik Yuzhno-Ural'skogo*

gosudarstvennogo universiteta. Seriya: Vychislitel'-naya matematika i informatika = Bulletin of the South Ural State University, 2016, vol. 5, no. 3, pp. 5-19. DOI 10.14529/cmse160301

12. Tasci S., Demirbas M. Employing in-memory data grids for distributed graph processing. *IEEE 2015 IEEE International Conference on Big Data (Big Data)*, 2015, pp. 1856–1864. doi:10.1109/bigdata.2015.7363959

13. Volchikhin V. I., Vashkevich N. P., Biktashev R. A. Modeli sobytijnyh nedeterminirovannyh avtomatov predstavleniya algoritmov upravleniya vzaimodejstvuyushchimi processami v mnogoprocessornyh vychislitel'nyh sistemah na osnove ispol'zovaniya mekhanizma monitora [Models of event-driven nondeterministic automata representing algorithms for controlling interacting processes in multiprocessor computing systems based on the use of a monitor mechanism]. *Izvestiya vysshikh uchebnykh zavedenii. Povolzhskii region. Tekhnicheskie nauki = Izvestia of higher educational institutions. Volga region. Technical sciences*, 2013, no. 2(26), pp. 5-14.

14. Courtois P. J.; Heymans F.; Parnas D. L. Concurrent Control with "Readers" and "Writers". *Communications of the ACM*. 14 (10), 1971, pp. 667–668. doi:10.1145/362759.362813. S2CID 7540747.

15. Babionitakis K., Doumenis G.A., Georgakarakos G. et al. 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

16. Dorogikh N. O., Yurin A. Y. Podhod k avtomatizirovannomu napolneniyu grafov znanij sushchnostyami na osnove analiza tablic [An approach to automated filling of knowledge graphs with entities based on table analysis]. *Ontologiya proektirovaniy = Design Ontology*, 2022, vol. 12, no. 3(45), pp. 336-352. DOI 10.18287/2223-9537-2022-12-3-336-352.

17. Putnin V. I. Avtomatizaciya processa postroeniya raspisaniya s primeneniem topologicheskoj sortirovki na grafe [Automating the process of building a schedule using topological sorting on a graph]. *E-Scio = Aposematic*, 2021, no. 3(54), pp. 584-588.

18. 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, 15 doi 10.34759/trd-2021-118-14.

19. Modinger D., Frohlich N., Hauck F.J. Pixy: A Privacy-Increasing Group Creation Scheme. *Conference: ICNCC 2020: 2020 The 9th International Conference on Networks, Communication and Computing*. December 2020 DOI: 10.1145/3447654.3447671.

20. Khabibullin N. F., Shkerdin A. N., Shcherbenko A. N. Povyshenie propusknoj sposobnosti sistem peredachi s peresprosom za schet vvedeniya dopolnitel'noj svyazi mezhdu processami dekodirovaniya s ispravleniem i obnaruzheniem oshibok [Increasing the throughput of transmission systems with a replay by introducing additional communication between decoding processes with correction and error detection]. *Internet-zhurnal Naukovedenie = Online journal of Science Studies*, 2016, vol. 8, no. 3(34), pp. 143 (In Russ.)

21. Tuchkin A.V. Principy funkcionirovaniya protokola kanal'nogo urovnya dlya paketnoj peredachi raznorodnogo trafika po nizkoskorostnym kanalam [Principles of functioning of the channel layer protocol for packet transmission of heterogeneous traffic over low-speed channels]. *T-Comm: Telekommunikatsii i transport = T-Comm: Telecommunications and Transport*, 2008, vol. 2, no. 3, pp. 31-33.

22. Maltsev G. N. Pomekhoustojchivost' i skrytnost' peredachi informacii po radiokanalam na osnove kombinirovannogo sluchajnogo kodirovaniya [Noise immunity and secrecy of information transmission over radio channels based on combined random coding]. *Informatsionno-upravlyayushchie sistemy = Information and Control Systems*, 2015, no. 2(75), pp. 82-89. DOI 10.15217/issn1684-8853.2015.2.82.

23. 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]. *Prikaspiiskii zhurnal: upravlenie i vysokie tekhnologii = Caspian Journal: Management and High Technologies*, 2022, no. 4(60), pp. 22-29.

24. 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. DOI 10.34759/trd-2022-125-20.

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

Информация об авторах / Information about the Authors

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

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

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

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