Труды МАИ. 2023. № 133
Trudy MAI, 2023, no. 133

Научная статья
УДК 004.052
URL: https://trudymai.ru/published.php?ID=177830

ОРГАНИЗАЦИЯ ХРАНЕНИЯ РЕЗУЛЬТАТОВ ПРОМЕЖУТОЧНЫХ ВЫЧИСЛЕНИЙ В ЗАДАЧАХ АУТЕНТИФИКАЦИИ ИСТОЧНИКОВ СООБЩЕНИЙ ОГРАНИЧЕННОЙ ДЛИНЫ

Максим Олегович Таныгин[1], Алина Андреевна Чеснокова[2]✉,
Вячеслав Порфирьевич Добрица[3]

[1,2,3]Юго-Западный государственный университет, (ЮЗГУ)

Курск, Россия

[1]tanygin@yandex.ru

[2]chesnokova.50@yandex.ru✉

[3]dobritsa@yandex.ru

Аннотация. В данной работе было проведено исследование практической реализации подхода к аутентификации источников сообщений ограниченной длины. Этот подход основан на использовании кодирования в режиме сцепления блоков. Описана организация адресного пространства для хранения результатов промежуточных вычислений, которые представлены в виде ориентированного древовидного графа. Показано, что для каждого такого графа можно выделить участки, в которых происходит его модификация, и участки, которые оказываются немодифицируемыми на определённых этапах выполнения процедуры

аутентификации. Подобное различие в режимах доступа является предпосылкой для организации системы параллельной обработки указанных графовых структур.

Также было показано, что использование данной организации памяти позволяет разделить весь процесс обработки сообщения ограниченной длины на 5 этапов. Из этих этапов, три могут быть реализованы специализированными модулями, которые работают параллельно и обращаются к непересекающимся областям матрицы регистров. Реализация асинхронной параллельной работы модулей, выполняющих операции декодирования поступающих пакетов данных, размещения их в непересекающихся областях регистровой памяти и анализа результатов промежуточных вычислений позволяет повысить скорость выполнения процедуры аутентификации.

Также была произведена оценка теоретически достижимого уровня параллелизации процедуры обработки сообщений. Оценка показала, что разрядность кода аутентификации определяет характер зависимости максимального уровня параллелизации от числа взаимодействующих источников. В случае, если разрядность кода превышает теоретическую границу применимости подхода на основании кодирования в режиме сцепления блоков, целесообразно использовать для параллельной работы не более 5 блоков декодирования и обработки древовидной системе, разделяя при этом пространство памяти для хранения промежуточных результатов на соответствующее число областей.

Ключевые слова: источник сообщений, внутренняя память блока, промежуточные вычисления, аутентификация, матрица регистров

Для цитирования: Таныгин М.О., Чеснокова А.А., Добрица В.П. Организация хранения результатов промежуточных вычислений в задачах аутентификации источников сообщений ограниченной длины // Труды МАИ. 2023. № 133. URL: https://trudymai.ru/published.php?ID=177830

Original article

ORGANIZATION OF STORAGE OF RESULTS OF INTERMEDIATE CALCULATIONS IN TASKS OF AUTHENTICATION OF MESSAGE SOURCES OF LIMITED LENGTH

Maxim O. Tanygin[1], Alina A. Chesnokova[2]✉, Vyacheslav P. Dobritsa[3],

[1,2,3]Southwest State University

Kursk, Russia

[1]tanygin@yandex.ru

[2]chesnokova.50@yandex.ru✉

[3]dobritsa@yandex.ru

Abstract. The authors conducted a study on the practical implementation of the approach to the message sources of limited length authentication. This approach is based on the coding application in the blocks chaining mode. Organization of the address space for the intermediate calculations results storing, which are presented in the form of an oriented tree graph, is described. The article demonstrates the possibility of identifying sections for each such graph where its modification occurs, and the sections, which turned out to be unmodified at certain stages of the authentication procedure execution. Such a difference

in access modes is a prerequisite for organizing a system of parallel processing of these graph structures.

The article demonstrates as well that application of this memory organization allows dividing the entire procedure of processing a message of limited length into five stages. Of these stages, the three can be implemented by specialized modules that operate in parallel and access the disjoint areas of the register matrix. Implementation of asynchronous parallel operation of modules, executing decoding operations of the incoming data packets, their placing in the disjoint areas of register memory and analyzing the results of intermediate calculations allows to increasing the authentication procedure speed.

An assessment of the theoretically achievable level of parallelization of the message processing procedure was performed as well. The assessment revealed that the bit depth of the authentication code determines the nature of the maximum level of parallelization dependence on the number of interacting sources. In case of the code bit depth exceeds the theoretical applicability limit of the approach based on coding in the block coupling mode, it is advisable to employ no more than five decoding and processing blocks in a tree-like system for parallel operation, while dividing the memory space for storing intermediate results into an appropriate number of areas.

Keywords*:* message source, block internal memory, intermediate calculations, authentication, register matrix

For citation: Tanygin M.O., Chesnokova A.A., Dobritsa V.P. Organization of storage of results of intermediate calculations in tasks of authentication of message sources of limited length. *Trudy MAI*, 2023, no. 133. URL: https://trudymai.ru/eng/published.php?ID=177830

Введение

Протоколы связи с большим радиусом действия и низким энергопотреблением (Long Range Wide Area Network – LoRaWAN) становятся широко востребованными при проектировании распределённых систем сбора информации, в том числе и тех, в состав которых входят мобильные агенты (датчики, размещённые на транспортных средствах, беспилотных летательных аппаратах, носимые сенсоры) [1 – 3]. Их преимущества, обозначенные в названии, позволяют реализовывать сенсоры в виде высокоавтономных устройств небольшого веса и размера. В их задачи входят сбор информации (по расписанию или по фиксации изменения наблюдаемого параметра), предварительная обработка информации и её передача с помощью интегрированного радиомодуля [4, 5]. Более сложные системы обладают функцией дистанционного управления режимами сбора информации, режимами трансляции данных и т.д. [6 - 8]. Как показывают исследования, основное энергопотребление таких устройств происходит в режиме передачи данных, доходя до 70% от общего потребления энергии в течение всего жизненного цикла [9, 10]. Так как энергопотребление в режиме передачи данных находится в прямой зависимости от объёма передаваемых данных, а объём передаваемых служебных данных в каждом сетевом пакете достигает 40%, [11] то для мобильных платформ, объединённых технологией LoRaWAN, актуальной является задача минимизации объёма служебной и метаинформации, передаваемой с каждой единицей сетевого взаимодействия. Особенно актуальна такая минимизация для систем и комплексов с жёсткими ограничениями, накладываемыми на ёмкость автономных источников питания, энергопотребление и аппаратную сложность вычислительного блока, таких

как беспилотные летающие платформы [12, 12]. Теоретическими исследованиями свойств алгоритмов кодирования в режиме сцепления блоков посвящено большое количество исследований [14 – 17]. В тоже время на пути практической реализации описанного в работах подходы является высокая вычислительная сложность алгоритмов и сложность хранения промежуточных результатов [19]. В этой связи актуальным направление исследований является разработка методов и технических средств повышения скорости выполнения и достоверности процедур аутентификации за счёт специальной структурно-функциональной организации аппаратных моделей предобработки сообщений, поступающих в приёмник по беспроводному каналу связи с низким энергопотреблением и большим радиусом действия

Формулировка задачи

Особенности реализации алгоритмов аутентификации сообщений, кодированных в режиме сцепления блоков, подразумевают формирование последовательностей сообщений виде древовидной структуры $G=\{V, E\}$, в которой вершины множества V есть сообщения, а дуги множества E соответствуют совпадению кода аутентификации второго сообщения пары вершин коду, полученному из данных первого сообщения пары [20]:

$$e \in E, e = \{v_i, v_j\} \neq \{v_j, v_i\} \Leftrightarrow \mathrm{F}^{\mathrm{HASH}}(v_i) = \mathrm{F}^{\mathrm{MAC}}(v_j), v_j \in V, v_i \in V. \quad (1)$$

где $\mathrm{F}^{\mathrm{HASH}}(v)$ – операция вычисления кода аутентификации из данных сообщения для его последующего анализа;

$\mathrm{F}^{\mathrm{MAC}}(v)$ – операция выделения кода аутентификации из данных сообщения.

В рассмотренных методах для снижения вычислительной сложности алгоритма формирования древовидной структуры G код аутентификации сообщения дополняется порядковым номером сообщения в группе (если передача сообщений ведётся множествами фиксированного размера) [21]. При передаче потока сообщений, где число передаваемых сообщений за сеанс связи не фиксировано, порядковый номер можно заменить его остатком от деления на некоторое число, которое определит количество битов сообщения, занимаемое данным параметром. В таком случае ветвь e между двумя сообщениями v_i и v_j формируется в случае выполнения следующего условия:

$$\begin{aligned} &e \in E, e = \{v_i, v_j\} \neq \{v_j, v_i\} \Leftrightarrow \\ &\Leftrightarrow \left[\mathrm{F}^{\mathrm{HASH}}(v_i) = \mathrm{F}^{\mathrm{MAC}}(v_j)\right] \vee \left[\mathrm{F}^{\mathrm{IND}}(v_i) + 1 = \mathrm{F}^{\mathrm{IND}}(v_j)\right], v_j \in V, v_i \in V. \end{aligned} \quad (2)$$

где $\mathrm{F}^{\mathrm{IND}}(v)$ – операция выделения порядкового номера или его остатка от деления на некоторое число из кода сообщения.

Особенную актуальность последний подход приобретает при интеграции механизма аутентификации сообщений, кодированных в режиме сцепления блоков, на беспилотные и мобильные платформы, где остро встаёт вопрос вычислительной мощности бортового оборудования и его энергопотребления. Именно последний фактор и приводит к необходимости использования кодирования в режиме сцепления блоков, так как обеспечивает снижение объёма транслируемой в эфир служебной информации с мобильной или беспилотной летающей платформы, что обеспечивает снижение энергозатрат на передачу данных по используемым протоколам беспроводной связи [10]

Таким образом, комплексная задача снижения количества передаваемой с эфир информации, в том числе аутентифицирующей, включает в себя как подзадачу синтез схемотехнически экономной вычислительной системы, обеспечивающей формирование древовидной структуры сообщений, её хранение и обработку с целью выделения из входящего потока сообщений подпотока сообщений от целевого источника, прошедшего процедуру аутентификации с требуемой достоверностью.

Описание системы управления внутренней памятью блока аутентификации

С учётом того, что особенностью древовидных структур памяти является невозможность осуществления прямой адресации требуемого элемента, а плоская модель памяти, характерная для большинства современных запоминающих устройств, не позволяет определять связи между элементами, характеризующие формируемую древовидную структуру, целесообразно использовать для хранения промежуточных результатов комбинированную организацию памяти, при которой все элементы множества $v \in V$, обладающие одинаковым значением $\mathrm{F}^{\mathrm{IND}}(v)$, размещаются в одном столбце матрицы памяти, а элемент множества $e \in E, e = \{v_i, v_j\}$ представляет собой номер строки столбца $\mathrm{F}^{\mathrm{IND}}(v_j)$, в которой хранится элемент v_j [22].

Особенности индексации элементов последовательности, поступающей из источника в приёмник, обусловливают, как было сказано выше, использовать вместо порядкового номера остаток от деления [23]. Это позволяет снизить

вероятность формирования в дереве G структур, соответствующих возникновению ошибки аутентификации [20]. Это позволяет реализовывать в схеме хранения промежуточных результатов (деревьев, соответствующих разным источникам) возможность параллельного обращения к областям памяти, хранящим содержимое разных деревьев (см. рис 1).

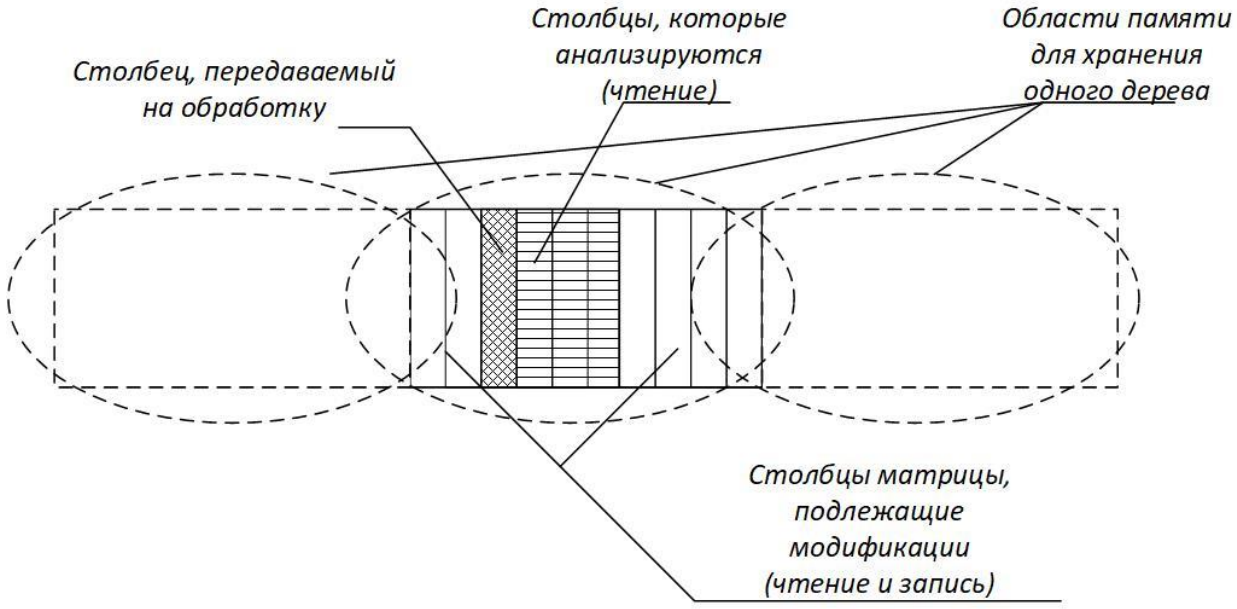

Рис. 1 – Карта оперативной памяти, хранящей результаты промежуточных вычислений при выполнении процедуры аутентификации нескольких источников

Всё адресное пространство памяти разделено на отдельные непересекающиеся области фиксированного, но необязательно равного размера, как это реализовано, например, в [24]. Каждая область O_i хранит древовидную структуру G_i, формируемую при выполнении процедуры аутентификации сообщений от i-го источника, и представляет собой совокупность M_i столбцов матрицы памяти, где M_i – мощность алфавита результата операции $\mathrm{F}^{\mathrm{IND}}(v)$. Известные решения

предполагают разные режимы обработки элементов дерева $v \in G_i$ в зависимости от значения их индекса $\mathrm{F}^{\mathrm{IND}}(v)$ [25]: в каждый момент существует набор индексов, к элементам, обладающим которым, возможно добавление вновь поступившего в приёмник сообщения (на рис. 1 такие столбца показаны без штриховки), к части элементов добавление новых невозможно и они анализируются на предмет структур, соответствующих ошибке аутентификации (на рис. 1 такие выделены горизонтальной штриховкой), и один индекс соответствует элементу, который принят как сообщение *i*-го источника и передаётся на обработку (штриховка клеткой). При этом номер столбца, используемого для хранения сообщения определяется по формуле

$$m' = \mathrm{F}^{\mathrm{IND}}(v) \bmod M_i + M_i^{\mathrm{BASE}} \qquad (3)$$

где m – порядковый номер сообщения в последовательности;

m' – реальный физический номер столбца регистровой памяти, используемого хранения элементов с индексом $\mathrm{F}^{\mathrm{IND}}(v)$;

M_i^{BASE} – номер первого столбца области O_i;

На рисунке 2 приведена структурная схема модуля хранения результатов промежуточных вычислений, осуществляющего обработку сообщений, ограниченной длины кодирования в режиме сцепления блоков. Блок хранения идентификаторов хранит кодовые последовательности, ассоциированные со источниками сообщений, на основании которых происходит декодирование сообщений. При этом каждое сообщение должно быть декодировано количество раз,

равное количеству источников, с которыми ведёт информационный обмен приёмник.

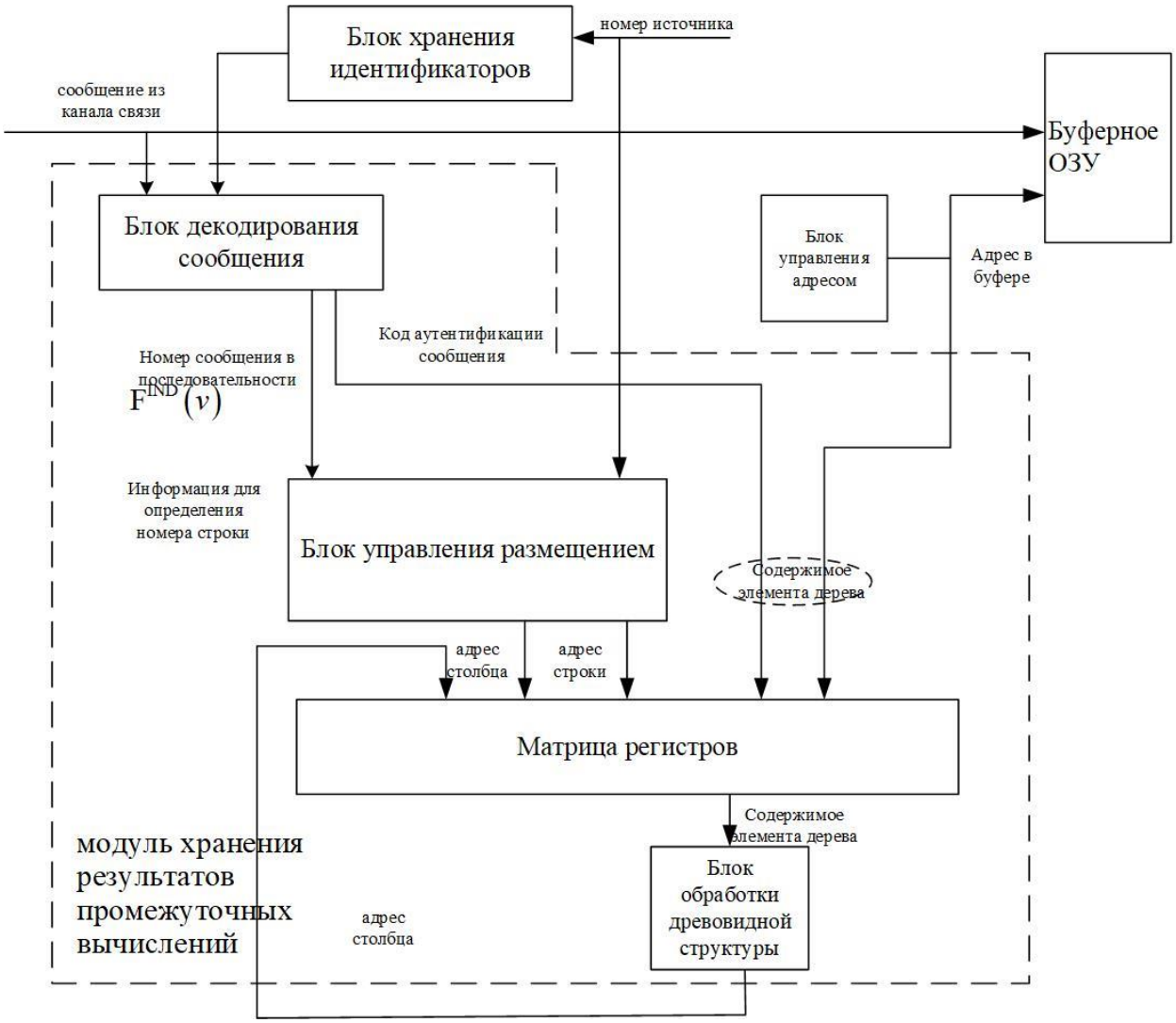

Рис. 2 – Структурная схема модуля хранения результатов промежуточных вычислений для задач аутентификации источников сообщений ограниченной длины

В буферном ОЗУ сообщение хранится в том же самом виде, в котором оно поступило из канала связи. Это требует повторного декодирования сообщения после извлечения из буфера, так как априори неизвестно, каким источником оно было сформировано и какой идентификатор требуется для его декодирования. Это добавляет в цикл обработки сообщения этап повторного декодирования сообщения после отнесения его к определенному источнику. В то же время это дает экономию

требуемой емкости буфера так, как если бы сообщение хранилось в декодированном виде, то хранить пришлось бы все варианты декодированного сообщения на всем множестве идентификаторов источников.

Блок управления размещением результатов промежуточных вычислений на основе формулы (3) производит трансляцию адресов записываемых данных. При этом добавление элемента в соответствующий столбец матрицы регистров требует анализа его содержимого, а так же содержимого соседних столбцов.

Элемент дерева, который хранится в одном регистре матрицы регистров, представляет собой выделенный из сообщения код аутентификации и адрес, сформированный блоком управления адресом, по которому код сообщения записан в буферном ОЗУ.

Элементы древовидных структур, после того, как к ним перестанут добавляться новые сообщения, передаются блок обработки древовидной структуры, где выполняется их анализ и выделения в каждом столбце матрицы регистров того элемента, который, в случае отсутствия ошибок, передаётся как сообщение соответствующего источника на обработку.

Результаты и их обсуждения

Описанная выше организация модуля хранения результатов промежуточных вычислений для задач аутентификации позволяет использовать для проведения процедур аутентификации нескольких источников как одного модуля (рис. 2), так и нескольких параллельно работающих модулей [26]. При этом общим ресурсом у них будет только буферное ОЗУ, хранящее данные поступающих сообщений, так как

матрица регистров представляет из себя непересекающиеся области памяти, доступ к которым можно осуществлять независимо различным блоками управления размещением. Цикл обработки сообщений при этом состоит из следующих этапов:

1. Запись сообщения в буфер

2. Декодирование сообщения

3. Размещение описателя сообщения в матрице регистров

4. Анализ столбца матрицы

5 Чтение из буферного ОЗУ сообщения и передача его на обработку.

При этом этапы 2 – 5 могут выполняться независимо параллельно работающими модулями хранения результатов промежуточных вычислений. С точки зрения схемотехники и синхронизации работы отдельных модулей, можно представить, что длительность этапов 1,2 и 5 равна одному такту машинного времени. Длительность этапа 3 определяется числом сравнений кода аутентификации сообщения с элементами древовидной структуры, хранящимися в произвольном столбце. Аналогично – длительность этапа 4, в котором последовательно перебираются элементы одного столбца и проверяется наличие структур, соответствующих ошибке аутентификации, определяется числом занятых элементов в столбце матрицы регистров.

В работе [22] получены оценки плотности вероятности для числа элементов, размещённых в каждом столбце. Это позволило получить оценки длительности цикла работы модуля хранения результатов промежуточных вычислений и длительности этапов, которые могут реализовываться в параллельно работающих

модулях. Согласно [22] число r элементов в каждом столбце является дискретной случайной величиной с функцией плотности вероятности:

$$p\ (r) = \sum_{i=r}^{U} \left(\frac{K^i \times e^{-K}}{i!} \left(\sum_{k=r}^{i} \frac{K^k \times e^{-K}}{k!} C_k^r \left(2^{-h}\right)^r \left(1-2^{-h}\right)^{U-r} \right) \right), \qquad (5)$$

где: H – разрядность кода аутентификации,

K –число источников сообщений,

U – число блоков данных, хранящихся в буферном ОЗУ, принятое равным $U = K \cdot M$

Тогда длительность цикла обработки сообщения будет равна сумме длительности отдельных его этапов:

$$N = N_1 + N_2 + N_3 + N_4 + N_5 =$$

$$= 1+1+2\times\left(1+\sum_{i=0}^{\infty}\left(r\times p\ (r)\right)\right)+2\times\left(1+\sum_{i=0}^{\infty}\left(r\times p\ (r)\right)\right)+1. \qquad (6)$$

где значения длительности 3 и 4 этапов получены, исходя из особенностей алгоритма формирования и анализа древовидных структур [25].

Показатель, равный отношению длительности цикла N к суммарной длительности этапов 1 и 2 $L = N/(N_1 + N_5)$ можно интерпретировать как теоретический максимум числа параллельно работающих модулей, при котором ни один модуль не будет простаивать в ожидании освобождения общего ресурса (буферного ОЗУ) другим. Дальнейшее увеличение числа блоков не обеспечит прироста производительности, так как лишь будет лишь создавать очереди из простаивающих в ожидании памяти блоков.

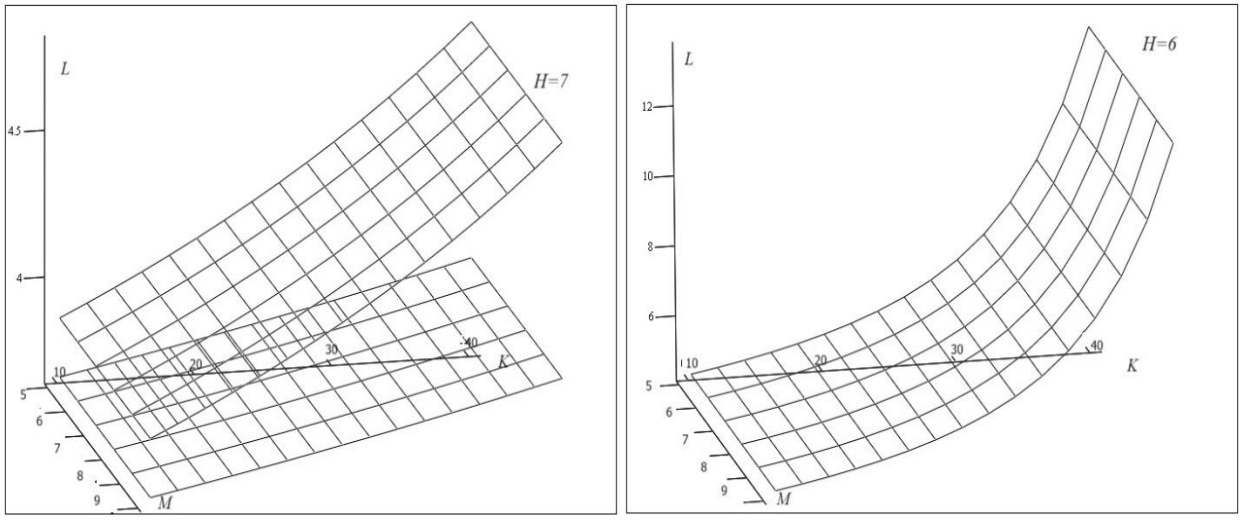

Рис. 3 – График зависимости *L* теоретического максимума числа параллельно работающих модулей хранения результатов промежуточных вычислений от числа источников сообщений

а) при достаточной разрядности кода аутентификации сообщения

б) при недостаточной разрядности кода аутентификации сообщения

Из анализа графиков на рисунке 3 видно, что если разрядность кода аутентификации сообщения удовлетворяет требованию по прогнозируемому уровню ошибки [27], то число параллельно работающих модулей не должно превышать 4 – 5. В противном случае, из-за роста числа операций при размещении описателя сообщения в матрице регистров и анализе столбца матрицы, теоретический максимум растёт с ростом числа источников сообщений

Заключение

В работе проведено исследование практической реализации подхода к аутентификации источников сообщений ограниченной длина, заключающегося в

использовании кодирования в режиме сцепления блоков. Определена организация памяти для хранения результатов промежуточных вычислений, представленных в виде ориентированного древовидного графа. Показано, что используемая организация позволяет разделить весь процесс обработки поступающего сообщения ограниченной длины на 5 этапов, три из которых могут быть реализованы специализированными модулями, работающими параллельно и обращающимися к непересекающимся областям матрицы регистров, служащей для хранения промежуточных результатов. На основе полученных ранее зависимостей была произведена оценка теоретически достижимого уровня параллелизации процедуры обработки сообщений, которая показала, что разрядность кода аутентификации определяет характер зависимости такого максимума от числа взаимодействующих источников. Если размер кода аутентификации превышает теоретически определённую для методов аутентификации на основе кодирования в режиме сцепления блоков границу [21], то достаточно 4 – 5 параллельно работающих моделей хранения, чтобы не создавать очередей к разделяемым ресурсам. Если же длина кода аутентификации меньше обозначенной границы, то число требуемых модулей растёт нелинейно, выходя за определённые условиями эксплуатации границами аппаратной сложности и энергопотребления приёмников сообщений, передаваемых по протоколам связи с большим радиусом действия и низким энергопотреблением.

В качестве направления дальнейших исследований можно определить моделирование работы модулей хранения результатов промежуточных вычислений

в асинхронном и синхронном режимах с помощью инструментария исследования систем массового обслуживания.

Список источников

1. IEEE Std 802.15.4-2020. IEEE Standard for Low-Rate Wireless Networks, pp.1-800, 23 July 2020. DOI: 10.1109/IEEESTD.2020.9144691
2. Петров Д. Стандарты беспроводной связи диапазона ISM // Электронные компоненты. 2010. № 10. С. 28-32.
3. Перри Л. Архитектура интернета вещей. – М.: ДМК Пресс, 2018. – 454 с.
4. Котов В.Н., Мельник Э.В., Щербинин И.П., Коровин Я.С. Распределенная информационно-управляющая система на основе интеллектуальных датчиков // Полезная модель 89257 G06F 15/00, опубл. 2009.11.27
5. Акимов А.А., Богатырев В.Е., Финогеев А.Г. Системы поддержки принятия решений на базе беспроводных сенсорных сетей с использованием интеллектуального анализа данных // Труды международного симпозиума "Надежность и качество". 2010. Т. 1. С. 225-229.
6. Кучерявый А.Е., Аль-Кадами Н.А. Адаптивный алгоритм кластеризации для беспроводных сенсорных сетей с мобильными узлами // Электросвязь. 2015. № 3. С. 22–26.
7. 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

8. Молчанов Д.А. Самоорганизующиеся сети и проблемы их построения // Электросвязь. 2006. № 6. С. 24–28.

9. Киреев А.О., Светлов А.В. Распределенная система энергетического мониторинга беспроводных сенсорных сетей // Известия ЮФУ. Технические науки. 2011. № 5 (118). С. 60–65.

10. Галкин П.В. Анализ энергопотребления узлов беспроводных сенсорных сетей // ScienceRise. 2014. № 2 (2). С. 55–61.

11. Levchenko P., Bankov D., Khorov E., Lyakhov A. Performance Comparison of NB-Fi, Sigfox, and LoRaWAN // Sensors, 2022, vol. 22 (24), pp. 9633. DOI: 10.3390/s22249633

12. Стандарт ISO 21384-3:2019(E). Беспилотные авиационные системы. Часть 3. Эксплуатационные процедуры. URL: https://www.gostinfo.ru/catalog/Details/?id=6479351

13. J. Zhao, D. Cheng, Ch. Hao. An Improved Ant Colony Algorithm for Solving the Path Planning Problem of the Omnidirectional Mobile Vehicle // Mathematical Problems in Engineering, 2016, vol. 12. DOI: 10.1155/2016/7672839

14. D. Shanti, P. Premkumar. Block Level Data Integrity Assurance Using Matrix Dialing Method towards High Performance Data Security on Cloud Storage // Scientific Research Publishing, 2016, vol. 7, no. 11, pp. 3626-3644. DOI:10.4236/CS.2016.711307

15. Black J., Rogaway P., Cryptol J. CBC MACs for arbitrary-length messages: The three-key constructions, 2015, vol. 18, no. 2, pp. 111–131.

16. Ben Othman S., Alzaid H., Trad A., Youssef H. An efficient secure data aggregation scheme for wireless sensor networks // Information, Intelligence, Systems and

Applications (IISA), 2013 Fourth International Conference, 2013. DOI: 10.1109/ii.sa.2013.6623701

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

18. Stallings W. NIST block cipher modes of operation for authentication and combined confidentiality and authentication // Cryptologia, 2010, no. 34, pp. 225- 235. DOI: 10.1080/01611191003598295

19. Таныгин М.О., Алшаиа Х.Я., Добрица В.П. Оценка влияния организации буферной памяти на скорость выполнения процедур определения источника сообщений // Труды МАИ. 2020. № 114. URL: https://trudymai.ru/published.php?ID=119007. DOI: 10.34759/trd-2020-114-155

20. Плугатарев А.В. Модель определения источника сообщений на основе статистического анализа метаданных в открытом канале связи // Прикаспийский журнал: управление и высокие технологии. 2022. № 4 (60). С. 30-37. DOI: 10.54398/20741707_2022_4_30

21. 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.

22. Таныгин М.О., Ахмад А.А.А., Казакова О.В., Голубов Д. Модель размещения данных во внутренней памяти вычислителя, реализующего схему кодирования

данных в режиме сцепления блоков // Известия Юго-Западного государственного университета. 2023. Т. 27. № 1. С. 73-91. DOI: 10.21869/2223-1560-2023-27-1-73-91

23. 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

24. Масюков И.И., Борзов Д.Б., Титов Д.В., Соколова Ю.В. Математическая модель и аппаратно-ориентированный алгоритм планирования размещения программ в системах на кристалле // Труды МАИ. 2021. № 119. URL: https://trudymai.ru/published.php?ID=159791. DOI: 10.34759/trd-2021-119-13

25. Таныгин М.О., Добросердов О.Г., Власова А.О., Ахмад А.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

26. Нестуев Д.С., Борзов Д.Б. Модель реорганизации беспроводного вычислительного кластера с орбитальным расположением элементов // Труды МАИ. 2023. № 128. URL: https://trudymai.ru/published.php?ID=171407. DOI: 10.34759/trd-2023-128-19

27. Алшаиа Хайдер Я.А. Метод и алгоритм обработки данных на основе идентификаторов в специализированном вычислительном устройстве: Дисс. канд. техн. наук. – Курск, 2021. – 138 с.

References

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

2. Petrov D. *Elektronnye komponenty*, 2010, no. 10, pp. 28-32.

3. Perri L. *Arkhitektura interneta veshchei* (Architecture of the Internet of Things), Moscow, DMK Press, 2018, 454 p.

4. Kotov V.N., Mel'nik E.V., Shcherbinin I.P., Korovin Ya.S. *Poleznaya model' 89257 G06F 15/00*, 2009.11.27

5. Akimov A.A., Bogatyrev V.E., Finogeev A.G. *Trudy mezhdunarodnogo simpoziuma "Nadezhnost' i kachestvo"*, 2010, vol. 1, pp. 225-229.

6. Kucheryavyi A.E., Al'-Kadami N.A. *Elektrosvyaz'*, 2015, no. 3, pp. 22–26.

7. 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

8. Molchanov D.A. *Elektrosvyaz*, 2006, no. 6, pp. 24–28.

9. Kireev A.O., Svetlov A.V. *Izvestiya YuFU. Tekhnicheskie nauki*, 2011, no. 5 (118), pp. 60–65.

10. Galkin P.V. *ScienceRise*, 2014, no. 2 (2), S. 55–61.

11. Levchenko P., Bankov D., Khorov E., Lyakhov A. Performance Comparison of NB-Fi, Sigfox, and LoRaWAN, *Sensors*, 2022, vol. 22 (24), pp. 9633. DOI: 10.3390/s22249633

12. *Standart ISO 21384-3:2019(E). Bespilotnye aviatsionnye sistemy. Chast' 3. Ekspluatatsionnye protsedury* (ISO 21384-3:2019 standard(E).13. Unmanned aircraft systems. Part 3. Operational procedures). URL: https://www.gostinfo.ru/catalog/Details/?id=6479351

13. J. Zhao, D. Cheng, Ch. Hao. An Improved Ant Colony Algorithm for Solving the Path Planning Problem of the Omnidirectional Mobile Vehicle, *Mathematical Problems in Engineering*, 2016, vol. 12. DOI: 10.1155/2016/7672839

14. D. Shanti, P. Premkumar. Block Level Data Integrity Assurance Using Matrix Dialing Method towards High Performance Data Security on Cloud Storage, *Scientific Research Publishing*, 2016, vol. 7, no. 11, pp. 3626-3644. DOI: 10.4236/CS.2016.711307

15. Black J., Rogaway P., Cryptol J. *CBC MACs for arbitrary-length messages: The three-key constructions*, 2015, vol. 18, no. 2. pp. 111–131.

16. Ben Othman S., Alzaid H., Trad A., Youssef H. An efficient secure data aggregation scheme for wireless sensor networks, *Information, Intelligence, Systems and Applications (IISA), 2013 Fourth International Conference*, 2013. DOI: 10.1109/ii.sa.2013.6623701

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

18. Stallings W. NIST block cipher modes of operation for authentication and combined confidentiality and authentication, *Cryptologia*, 2010, no. 34, pp. 225- 235. DOI: 10.1080/01611191003598295

19. Tanygin M.O., Alshaia Kh.Ya., Dobritsa V.P. *Trudy MAI*, 2020, no. 114. URL: https://trudymai.ru/eng/published.php?ID=119007. DOI: 10.34759/trd-2020-114-155

20. Plugatarev A.V. *Prikaspiiskii zhurnal: upravlenie i vysokie tekhnologii*, 2022, no. 4 (60), pp. 30-37. DOI: 10.54398/20741707_2022_4_30

21. Tanygin M.O., Chesnokova A.A., Akhmad A.A.A. *Prikaspiiskii zhurnal: upravlenie i vysokie tekhnologii*, 2022, no. 4 (60), pp. 22-29.

22. Tanygin M.O., Akhmad A.A.A., Kazakova O.V., Golubov D. *Izvestiya Yugo-Zapadnogo gosudarstvennogo universiteta*, 2023, vol. 27, no. 1, pp. 73-91. DOI: 10.21869/2223-1560-2023-27-1-73-91

23. 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

24. Masyukov I.I., Borzov D.B., Titov D.V., Sokolova Yu.V. *Trudy MAI*, 2021, no. 119. URL: https://trudymai.ru/eng/published.php?ID=159791. DOI: 10.34759/trd-2021-119-13

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

26. Nestruev D.S., Borzov D.B. *Trudy MAI*, 2023, no. 128. URL: https://trudymai.ru/eng/published.php?ID=171407. DOI: 10.34759/trd-2023-128-19

27. Alshaia Khaider Ya.A. *Metod i algoritm obrabotki dannykh na osnove identifikatorov v spetsializirovannom vychislitel'nom ustroistve* (Method and algorithm of data processing based on identifiers in a specialized computing device): Doctor's thesis, Kursk, 2021, 138 p.

Статья поступила в редакцию 15.11.2023
Одобрена после рецензирования 19.11.2023
Принята к публикации 25.12.2023
The article was submitted on 15.11.2023; approved after reviewing on 19.11.2023; accepted for publication on 25.12.2023