Труды МАИ. 2026. № 149.

Trudy MAI. 2026. No. 149. (In Russ.)

Научная статья
УДК 004.052
URL: https://trudymai.ru/published.php?ID=189165
EDN: https://www.elibrary.ru/YLHTHP

ИСПОЛЬЗОВАНИЕ ДВУНАПРАВЛЕННЫХ СПИСОЧНЫХ СТРУКТУР ДЛЯ ОБНАРУЖЕНИЯ ОШИБОК ОБРАБОТКИ ПРИ КОДИРОВАНИИ ДАННЫХ В РЕЖИМЕ СЦЕПЛЕНИЯ БЛОКОВ

М. Наджаджра[1], **М.О. Таныгин**[2], **А.А. Чеснокова**[2]✉

[1]Университет Аль-Истикляль, г. Иерихон, Палестина

[2]Федеральное государственное бюджетное образовательное учреждение высшего образования "Юго-Западный государственный университет", г. Курск, Россия

✉ chesnokova.50@yandex.ru

Цитирование: Наджаджра М., Таныгин М.О., Чеснокова А.А. Использование двунаправленных списочных структур для обнаружения ошибок обработки при кодировании данных в режиме сцепления блоков // Труды МАИ: электрон. журнал. № 149.
URL: https://trudymai.ru/published.php?ID=189165

Аннотация. В статье исследуется проблема обнаружения ошибок идентификации источника сообщений в системах с аутентификацией данных, использующих режим сцепления блоков для задач сокращения объёма служебных данных, передаваемых с борта беспилотного летательного аппарата. В таком режиме аутентификационный тег каждого сообщения зависит от содержимого предыдущего, формируя цепочку. Хотя это повышает общую достоверность, при снижении объёма передаваемой информации (и пропорциональному сокращению энергозатрат радиопередающего модуля на трансляцию таких данных в эфир), коллизии аутентификационных тегов между сообщениями целевого и посторонних источников могут приводить к неоднозначностям и ошибкам в определении, какое сообщение является подлинным. Традиционные методы, требующие буферизации и последующего анализа всей последовательности сообщений, оказываются ресурсоемкими и создают дополнительные задержки в контуре управления беспилотного летательного аппарата.

Предложен подход, основанный на использовании двунаправленных списочных структур (графов) для организации хранения и обработки поступающих сообщений в реальном времени. В предлагаемой модели каждое сообщение представляется вершиной графа, а связи (дуги) между вершинами устанавливаются при выполнении условия соответствия аутентификационных тегов. Ключевая идея метода заключается в активном обнаружении конфликтных ситуаций (коллизий) непосредственно в момент добавления нового сообщения в граф, путем анализа формируемых связей. Алгоритм выявляет характерные подструктуры (подграфы из четырех вершин), возникновение которых сигнализирует о невозможности однозначной идентификации источника.

Проведено математическое моделирование для оценки вероятности возникновения таких конфликтных структур и связанных с ними дополнительных вычислительных затрат. Показано, что при соблюдении условия, связывающего разрядность тега аутентификации и количество источников в системе, вероятность необходимости дополнительного анализа остается незначительной.

Ключевые слова: двунаправленные списочные структуры; кодирование; режим сцепления блоков; энергоэффективность; аутентификация.

USING BIDIRECTIONAL LIST STRUCTURES TO DETECT PROCESSING ERRORS WHEN ENCODING DATA IN BLOCK CHAINING MODE

M. Najajra[1], M.O. Tanygin[2], A.A. Chesnokova[2]✉

[1]Al-Istiqlal University, Jericho, Palestine

[2]Southwest State University, Kursk, Russia

✉ chesnokova.50@yandex.ru

Citation: Najajra M., Tanygin M.O., Chesnokova A.A. Using bidirectional list structures to detect processing errors when encoding data in block chaining mode // Trudy MAI. 2026. No. 149. (In Russ.). URL: https://trudymai.ru/published.php?ID=189165

Abstract. The article examines the problem of detecting errors in identifying the source of messages in data authentication systems that use the cipher block chaining mode to reduce the volume of overhead data transmitted from UAVs. In this mode, the

authentication tag of each message depends on the content of the previous one, forming a chain. Although this increases overall reliability, when the volume of transmitted information is reduced (and correspondingly the energy consumption of the UAV's radio transmitting module for broadcasting such data over the air is lowered), collisions of authentication tags between messages from the target and unintended sources can lead to ambiguities and errors in determining which message is authentic. Traditional methods that require buffering and subsequent analysis of the entire sequence of messages prove to be resource-intensive and create additional delays in the UAV control loop.

An approach is proposed based on the use of bidirectional list structures (graphs) for organizing the storage and processing of incoming messages in real time. In the proposed model, each message is represented as a vertex of the graph, and connections (edges) between vertices are established when the condition of matching authentication tags is met. The key idea of the method is the active detection of conflict situations (collisions) at the moment a new message is added to the graph, through the analysis of the formed connections. The algorithm identifies characteristic substructures (subgraphs of four vertices), the occurrence of which signals the impossibility of unambiguously identifying the source.

Mathematical modeling was conducted to assess the likelihood of the occurrence of such conflict structures and the associated additional computational costs. It was shown that if the condition linking the authentication tag length and the number of sources in the system is met, the probability of requiring additional analysis remains insignificant.

Keywords: bidirectional list structures; coding; block coupling mode; energy efficiency; authentication.

Введение

Безопасная коммуникация является одним из основных требований, предъявляемых к системам управления беспилотными летательными аппаратами (БПЛА). Традиционные криптографические решения для её обеспечения требуют слишком много вычислительных ресурсов, а

вычислительные блоки, используемые в БПЛА, имеют ограниченные размеры оперативной памяти и производительность RAM. Особенно же критическим является потребляемая мощность. Основными путями снижения энергопотребления оконечным вычислительным оборудованием БПЛА является снижение сложности используемых криптоалгоритмов [1], алгоритмов предлагается применять алгоритмы так называемой «легковесной криптографии» для снижения нагрузки на устройства с ограниченными ресурсами [2-6]. Снижение же энергозатрат на трансляцию в эфир данных с борта БПЛА достигается использованием коммуникационных протоколов с низким энергопотреблением и большим радиусом действия (в части передачи управляющих и служебных воздействий, а не передаче видеосигнала с борта БПЛА). Указанные протоколы предусматривают ограничение объёма передаваемых данных [2], что вызывает невозможность передачи больших объёмов аутентифицируемой информации, что вступает в противоречие с обозначенным требованием по безопасной коммуникации узла управления и БПЛА.

Для протоколов с низким энергопотреблением и большим радиусом действия характерно то, что до 70% [7-11] энергозатрат оконечного оборудования приходится на передачу данных, объем которой при использовании пакетов данных ограниченной, составляет до 40% в каждом пакете [12]. Это делает задачу минимизации служебной и аутентификационной данных критически важной для автономных беспилотных мобильных платформ с жесткими ограничениями по питанию и вычислительным ресурсам [13, 14].

Несмотря на большое количество исследований в области алгоритмов кодирования [15 – 19], их практическая реализация осложнена вычислительной сложностью [20], что как было сказано выше, вступает в противоречие с характеристиками аппартной платформы IoT-устройтсв. Актуальной становится разработка специализированных аппаратных моделей предобработки сообщений, способных за счет оптимизированной структурно-функциональной организации повысить скорость и надежность аутентификации в низкоэнергетических беспроводных каналах.

Стандартный механизм кодирование в режиме сцепления блоков CBC повышает вероятность обнаружения факта ошибки, но определить источник ошибки становится затруднительно. Коллизия аутентификационной информации в сообщении источника и постороннем сообщении "компрометирует" следующие за ним блоки данных. Это делает рассмотренные в [15] подходы неэффективным для локализации сообщения, в котором произошла ошибка определения источника.

Формулировка задачи

В механизме аутентификации на основе цепи, где аутентификационный тег (код целостности) каждого последующего сообщения зависит не ттолько от его собственного содержимого, но и от тега предыдущего сообщения, создается связанная последовательность (цепочка), разрыв или несоответствие в которой указывает на потерю или подмену данных. В сравнении с методами поблокового кодирования, метод CBC обладает более высокой достоверностью из-за уменьшения вероятности коллизий таких тегов.

В поблочном кодировании вероятность коллизии для одного сообщения S:

$P_{col} \approx 2^{-H}$, где H - разрядность тега

Для успешной подмены сообщения S в режиме сцепления блоков атакующему нужно подобрать не один, а два тега так, чтобы выполнялись условия:

$$F\left\{s_{i-1}^{\text{inf}}, \Omega\right\} = s_i^{\text{aut}} \quad (1)$$

где: i - порядковый номер сообщения в последовательности аутентичных сообщений целевого источника;

s_{i-1}^{inf} – часть, содержащая полезную информация i-1-го сообщения последовательности;

s_{i+1}^{aut} – часть, содержащая тег аутентификации i-го сообщения последовательности.

Таким образом, если исключить из рассмотрения первое и последнее сообщение последовательности, для которых можно предусмотреть особый

протокол определения источника, вероятность коллизии для некоторого сообщения s определится вероятностью одновременного выполнения условий:

$$\begin{aligned} F\left\{s_{i-1}^{\inf}, \Omega\right\} &= s^{\text{aut}}, \\ F\left\{s^{\inf}, \Omega\right\} &= s_{i+1}^{\text{aut}}, \end{aligned} \qquad (2)$$

которая в общем случае равна 2^{-2H}, где H – разрядность тега аутентификации.

При реализация такого кодирования возникает необходимость буферизации данных. Приемник вынужден хранить все полученные сообщения (или их хеши) в буфере, так как неизвестно, какое из них окажется частью правильной цепочки, когда придет следующее. Необходимо постоянно перепроверять связи между всеми полученными сообщениями при поступлении нового, что требует вычислительных ресурсов.

Целесообразным представляется выделение отдельной оперативной памяти для хранения полезной нагрузки сообщений и регистровой – для хранения описателей сообщений, информации о связи сообщениями друг с другом и прочих данных в виде динамической списочной структуры или графа.

Если представить, как это сделано в [20] множество поступающих сообщений в виде графа, то вершинами его будут сообщения $s \in U$, поступившие в приёмник, а ориентированная дуга $e^{\langle s_i, s_j \rangle}{}_j$ между вершинами $s_i, s_j \in U$ дугами существует, если выполнено условие $F\left\{s_i^{\inf}, \Omega\right\} = s_j^{\text{aut}}$.

Соответственно, можно сформулировать критерии аутентичности сообщения или последовательности сообщений, то есть критерии отнесения сообщений к некоторому подмножеству сообщений $U^{\text{A}} \subset U$, сформированных целевым источником. Для одного сообщения его можно сформулировать следующим образом. Сообщение U^{A} принадлежит множеству U^{A} в случае, если одновременно выполняются следующие условия: существует сообщение, для которого определено, что оно сформировано целевым источником: $s' \in U^{\text{A}}$, существует единственное сообщение множества U $s \in U$, такое, что существует

ветвь $e^{\langle s',s\rangle}$, а также существует подмножество сообщений мощностью N $\{s_i, s_{i+1},\ldots,s_{i+N}\}\subset U$, такое, что существует ветвь $e^{\langle s,s_i\rangle}$, а также ветви $e^{\langle s_{i+j},s_{i+j+1}\rangle}$, $j=0\ldots N-1$.

Для последовательности сообщений условие аутентичности формулируется следующим образом. Подмножество сообщений мощностью N $\{s_i, s_{i+1},\ldots,s_{i+N}\}\subset U$ сформировано целевым источником $\{s_i, s_{i+1},\ldots,s_{i+N}\}\subset U^{\mathrm{A}}$ в случае, если для сообщения $s'\in U^{\mathrm{A}}$, сформированного целевым источником, существует ветвь $e^{\langle s',s_i\rangle}$, а также ветви $e^{\langle s_{i+j},s_{i+j+1}\rangle}$, $j=0\ldots N-1$. При этом не должно существовать никакого другого подмножества такой же мощности, отличного от указанного, для которого вышеназванные условия также выполняются.

Ошибки аутентификации возможны, когда указанные условия выполняются не только для одного сообщения или последовательности сообщений, то есть когда возникает коллизия кодов аутентификации у минимум двух сообщений, которую формально можно описать следующим образом. Для трёх последовательных сообщений целевого источника $s_{i-1}, s_i, s_{i+1}\in U^{\mathrm{A}}$, где i–1,i,i+1 – ранг элемента в динамической структуре или расстояние от соответствующих элементов до корня дерева – первого сообщения источника, в рассматриваемом графе существуют две дуги $e^{\langle s_{i-1},s_i\rangle}$ и $e^{\langle s_i,s_{i+1}\rangle}$. При этом существует сообщение $s'\in U, s'\notin U^{\mathrm{A}}$, для которого в графе также существуют дуги $e^{\langle s_{i-1},s'\rangle}$ и $e^{\langle s',s_{i+1}\rangle}$. В таком случае, не имея дополнительной информации, определить на основании выполнения условия (1) и условий формирования последовательностей, какое из двух сообщений s' или s сформировано целевым источником, невозможно.

Описание подхода к обнаружению ошибки определения источника сообщений

Одним из решений для ускорения обработки и экономии оперативной памяти является использование косвенной адресации через буферизацию блоков данных. В этом случае сами данные хранятся в ОЗУ в произвольном порядке, а их

описатели (например, адреса) размещаются в отдельной регистровой памяти, формируя древовидную структуру через систему ссылок [21]. Однако алгоритмы работы со списками часто требуют рекурсивного обхода всех ветвей графа, что в условиях отсутствия критериев для выбора пути (как в невзвешенных графах) приводит к необходимости полного перебора. В среднем, количество операций для поиска элемента составляет половину от общего числа элементов в структуре [22–24]. Попытки парализации процесса [22, 23] не устраняют фундаментальную проблему случайности количества операций. Альтернативой являются более простые в аппаратной реализации итерационные алгоритмы, которые работают с данными как с совокупностью векторов [25–26]. В этом случае регистровая память организуется в виде матрицы описателей. Такой подход обеспечивает предсказуемую производительность: среднее число операций поиска равно половине длины цепочки, что выгоднее полного перебора графа. Недостатком является необходимость резервирования памяти под вектор максимально возможной длины для каждой ветви, что ведет к неэффективному использованию ресурсов.

Проведенный анализ позволяет заключить, что ключевой задачей при обработке цепочек сообщений становится оптимизация объема памяти, требуемого для хранения служебных структур адресации. Что касается вычислительной сложности поиска, то она, в случае невзвешенных графов, жестко определяется размером структуры и не может быть кардинально снижена рассмотренными схемотехническими методами. Таким образом, основной фокус должен быть смещен в сторону минимизации затрат памяти при приемлемой производительности.

В известных решениях [27] определение источника сообщений происходило после формирования всей анализируемой последовательности и определялось способом временного хранения поступающих сообщений и представления описанного выше графа, его вершин и дуг. Повышение скорости достигалось за счёт варьирования размера анализируемой выборки N, исключения из обработки части сообщений при их формировании из множества всех сообщений отдельных последовательностей.

В то же время перспективным представляется поход к обнаружению коллизий на этапе добавления сообщения в граф путём анализа структуры такого графа и обнаружения в нём подграфов, состоящих из 4-х вершин (придерживаясь принятых ранее обозначений): $\{s_{i-1}, s_i, s_{i+1}, s'\}$, $s_{i-1}, s_i, s_{i+1} \in U^{\mathrm{A}}$, $s' \in U, s' \notin U^{\mathrm{A}}$), и 4-х дуг: $e^{\langle s_{i-1}, s_i \rangle}$, $e^{\langle s_i, s_{i+1} \rangle}$, $e^{\langle s_{i-1}, s' \rangle}$ и $e^{\langle s', s_{i+1} \rangle}$.

Соответственно, существует три способа формирования такого подграфа, показанные на рисунке 1, где элемент A соответствует сообщению s_{i-1}, элемент C – сообщению s_{i+1} а элементы B и B' – сообщениям s_i, s' (конкретное соответствие в данном случае не имеет значения). Штриховкой показано текущее обрабатываемое сообщение, которое добавляется в граф, а также дуги, формируемые при добавлении текущего сообщения в случае выполнения условия следования сообщений друг за другом. Пунктиром – дуги, связывающие рассматриваемый подграф с другими элементами графа.

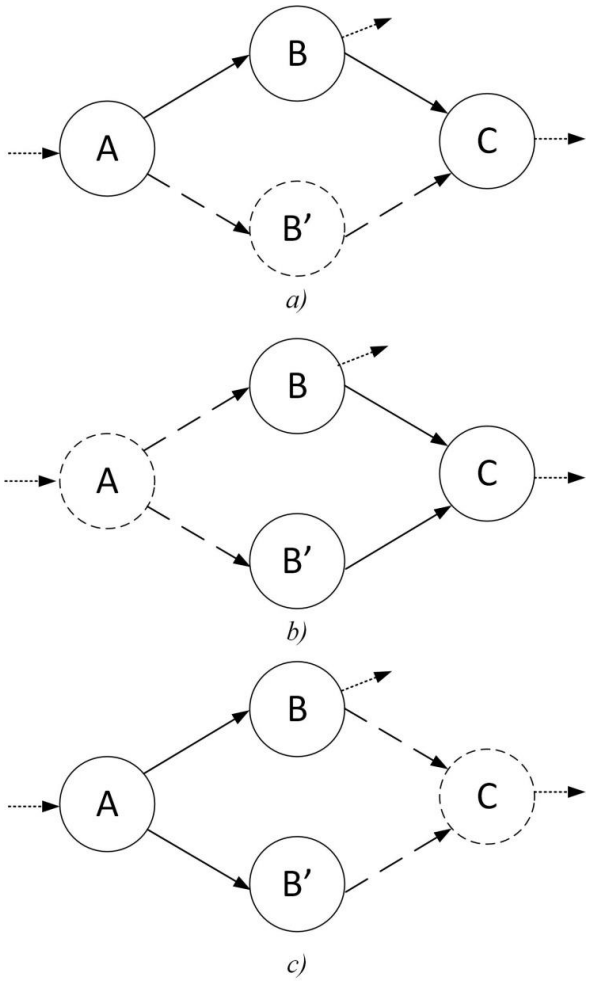

Рисунок 1 – Варианты формирования подструктуры, при которой невозможно определение источника сообщений

Очевидно, зафиксировать образование указанной структуры можно при добавлении соответствующего сообщения в граф. Для этого необходимо анализировать, сколько формируется связей с последующими и предшествующими сообщениями, и если общее число формируемых связей превышает два, то необходимо анализировать уже сформированные связи сообщений (обозначенные сплошной линией), которые соединяются с вновь добавляемым сообщением.

Результаты и их обсуждение

Для обнаружения конфликтных ситуаций и ошибок идентификации в процессе построения дерева требуется, по сравнению с описанным в [28] подходе, дополнительная память для хранения указателей на предыдущие элементы дерева и дополнительные вычислительные операции для анализа каждого нового элемента и его связей.

Проверка будет производиться для любого сообщения, для которого при добавлении в древовидную структуру были сформированы две и более дуги (указатели на элементы с рангом, отличающимся на единицу). Если у таких элементов, в свою очередь, будут обнаружены указатели на один и тот же элемент дерева (дуги, входящие или исходящие из одной вершины), можно утверждать о некорректном образовании структуры.

Оценим вероятность возникновения ситуации, при которой необходимы дополнительные вычислительные затраты. Используя модель распределения количества сообщений по рангам [28], можно оценить вероятность наличия k посторонних сообщений ранга i–1 в графе в зависимости от K – числа взаимодействующих источников в системе (или отношения общей интенсивности поступающих в приёмник сообщений к интенсивности сообщений, сформированных целевым источником) и H – разрядности тега аутентификации. Для упрощения модели принято допущение, что сообщения могут добавляться на любую позицию в дереве, хотя в реальности сообщения от источников с высоким рангом поступают позднее. Согласно [29], это допущение

справедливо, когда ранг текущего сообщения *i* значительно меньше общей длины дерева.

Процесс образования k дуг между новыми сообщениями и j посторонними сообщениями ранга i-1 моделируется биномиальным распределением. Вероятность этого события задаётся формулой $C_j^k\left(2^{-H}\right)^k\left(1-2^{-H}\right)^{j-k}$, где H – разрядность идентификатора в сообщении.

Вероятность образования k связей между новыми сообщениями и всеми элементами ранга i-1 (включая целевой источник) определится как произведение вероятностей:

$$p_k^{\langle i-1,i\rangle}=\sum_{j=0}^{k}\left\{\left(p_j^*\right)\sum_{l=k-j}^{\infty}\left(p_l^{i-1}C_l^{k-j}\left(2^{-H}\right)^{k-j}\left(1-2^{-H}\right)^{l-l+j}\right)\right\}, \quad (3)$$

$$p_0^*=1-2^{-H},\ p_1^*=2^{-H},\ p_j^*=0,\ j>1,$$

где p_j^* – вероятность образования *j* дуг между добавляемым сообщением и (*i*-1)-м сообщением целевого источника.

Дополнительная проверка дуг, исходящих от соседей добавляемого сообщения, потребуется, если произойдёт хотя бы одно из трех событий:

1. Сформировано две или более дуги с сообщениями ранга *i-1.*

2. Сформировано две или более дуги с сообщениями ранга *i*+1.

3. Сформировано 1 или более дуг с сообщениями ранга *i*-1 и 1 или более дуг с сообщениями ранга *i*+1.

Итоговая вероятность вычисляется по формуле объединения этих событий:

$$p^{\langle s_i\rangle}=1-\left\{1-\left(1-p_0^{\langle i-1,i\rangle}\right)^2\right\}\left(1-\sum_{k=2}^{\infty}p_k^{\langle i-1,i\rangle}\right)^2. \quad (4)$$

где p_j^* – вероятность образования.

Ниже на рисунке 2 приведен график зависимости вероятности формирования структуры, соответствующей ошибке идентификации источника, при поступлении одиночного сообщения в приёмник от числа источников K и разрядности тега аутентификации *H*.

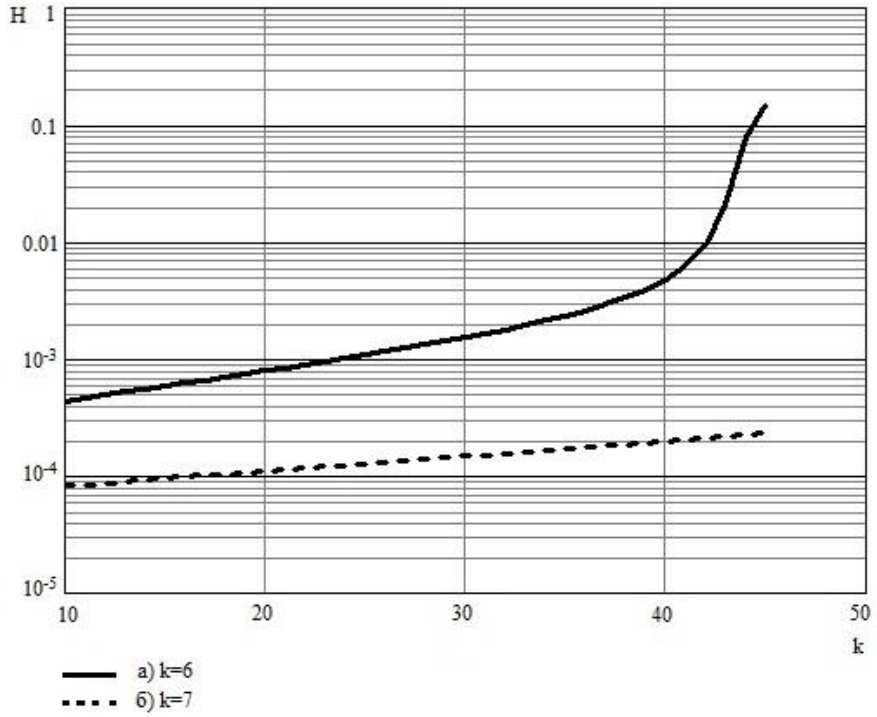

Рисунок 2- График зависимости вероятности *p* вероятности формирования структуры, соответствующей ошибке идентификации источника, при поступлении одиночного сообщения от числа источников *K* и разрядности тега аутентификации *H*

Видно, что при выполнении определённого в [29] минимальном условия $H>\log_2 K+1$ вероятность возникновения дополнительных вычислительных затрат для определения ошибки идентификации незначительна (менее 10^{-2}), тогда как при невыполнении указанного неравенства происходит значительный рост указанной вероятности до значений, при которых практическая реализация передачи данных невозможна. То есть реализация подхода к поиску ошибок идентификации за счёт анализа двунаправленных списков не приводит к росту дополнительных вычислительных затрат, но позволяет обнаруживать ошибки непосредственно при формировании соответствующей структуры, не дожидаясь приёма и последующей обработки всех сообщений последовательности. Кроме того, плавный рост вероятности возникновения обсуждаемых структур (рис. 1) с увеличением числа источников позволяет использовать предложенный подход для систем, в которых интенсивность сообщений может претерпевать значительные кратковременные скачки.

Заключение

В статье рассмотрен подход к обработке данных, кодированных в режиме сцепления блоков для задач сокращения объёма служебных данных, передаваемых с борта БПЛА. Подход подразумевает, что ошибки идентификации источников возникают в результате коллизий тегов аутентификации, ассоциированных с каждым передаваемым в системе сообщении. Показано, что реализация динамической структуры, хранящей промежуточные результаты обработки как сообщений целевого источника, так и иных сообщений, поступающих в приёмник, в виде двунаправленной списочной структуры позволяет обнаруживать ошибки идентификации источника группы сообщений непосредственно в момент коллизии тегов аутентификации сообщений, а не после обработки всей последовательности и всей структуры.

Создана математическая модель оценки возникновения потребности в дополнительных вычислительных затратах, необходимых для анализа двунаправленного списка, что критически важно для оценки энергопотребления вычислительного модуля, выполняющего реализацию рассматриваемого подхода. Показано, что для определённых в предшествующих исследованиях соотношениях между числом источников сообщений и разрядностью тега аутентификации, вероятность возникновения дополнительных вычислительных затрат, связанных с обработкой и поиском характерных структур в графе промежуточных результатов, не превышает 10^{-2}, что позволяет использовать кодирование в режиме сцепления для систем, использующих ограниченные размеры тега аутентификации, но требующих высокой скорости выполнения процедур идентификации источников информации, которая входит в противоречие с временными задержками, требуемыми для передачи всей последовательности сообщений.

Конфликт интересов

Авторы заявляют об отсутствии конфликта интересов.

Conflict of interest

The authors declare no conflict of interest.

Список источников

1. Roy, K. S., Sujith, M., Bhanu, B., Preethi, & Hazarika, R. A. (2024). FPGA-based dual-layer authentication scheme utilizing AES and ECC for unmanned aerial vehicles. Eurasip Journal on Wireless Communications and Networking, 2024(1), Article 91.
2. IEEE P2510 – Standard for Establishing Quality of Data Sensor Parameters in the Internet of Things Environment, February 10, 2020
3. Zhou, L., Li, X., Yeh, K., & Chiu, W. Lightweight IoT-based authentication scheme in cloud computing circumstance. Future Gener // Comput. Syst., 2019, 91, 244-251.
4. Abed, A., Abdelhafeez, A., & Fouad, M. Authentication in Cloud Computing Environments. Multicriteria Algorithms with Applications. 2024.
5. Arafin, T., & Qu, G. Hardware-Based Authentication Applications. 2021, 145-181.
6. Al-Shareeda, S. Data authentication algorithms. Authentication Technologies for Cloud Computing, IoT and Big Data. 2019
7. 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
8. Петров, Д. Стандарты беспроводной связи диапазона ISM // Электронные компоненты. - 2010. - № 10. - С. 28-32
9. Перри Л. Архитектура интернета вещей. – М.: ДМК Пресс, 2018. – 454 с. ISBN– 978-5-97060-672-8.
10. Киреев, А. О., Светлов, А. В. Распределенная система энергетического мониторинга беспроводных сенсорных сетей // Известия ЮФУ. Технические науки. 2011. № 5 (118). С. 60–65.
11. Галкин, П. В. Анализ энергопотребления узлов беспроводных сенсорных сетей // ScienceRise. 2014. № 2 (2). С.55–61.
12. Levchenko, P.; Bankov, D.; Khorov, E.; Lyakhov, A. Performance Comparison of NB-Fi, Sigfox, andLoRaWAN. Sensors 2022, 22, 9633.https://doi.org/10.3390/s22249633
13. Беспилотные авиационные системы. Часть 3. Эксплуатационные процедуры [Электронный ресурс] // Стандарт ISO 21384-3:2019(E). URL:

https://cdn.standards.iteh.ai/samples/70853/7ec34c8a22bf46958423b7e3a2e43693/ISO-21384-3-2019.pdf (дата обращения 08.11.2025)

14. 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 (12). doi: 10.1155/2016/7672839

15. D. Shant P. Premkumar, «Block Level Data Integrity Assurance Using Matrix Dialing Method towards High Performance Data Security on Cloud Storage,» Scientific Research Publishing, т. 7, № 11, pp. 3626-3644, 2016

16. Black, J. CBC MACs for arbitrary-length messages: The three-key constructions [Текст] / J. Black, P. Rogaway – J. Cryptol, 2015. – vol. 18 – №2 – P. 111–131

17. Ben Othman, S., Alzaid, H., Trad, A., & Youssef, H. An efficient secure data aggregation scheme for wireless sensor networks. // IISA 2013, doi:10.1109/iisa.2013.6623701

18. M. Bellare, J. Kilian, P. Rogaway, “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.

19. W. Stallings “NIST block cipher modes of operation for authentication and combined confidentiality and authentication,” Cryptologia, 2010, № 34, pp. 225- 235, doi: 10.1080/01611191003598295

20. Таныгин, М. О. Организация хранения результатов промежуточных вычислений в задачах аутентификации источников сообщений ограниченной длины / М. О. Таныгин, А. А. Чеснокова, В. П. Добрица // Труды МАИ. – 2023. – № 133.

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

22. 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

23. Paradies M, Lehner W, Bornhövd C GRAPHITE: an extensible graph traversal framework for relational database management systems. In: DBM. ACM, 2015pp 29:1–29:12. DOI : 10.1145/2791347.2791383

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

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

26. 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, http://mai.ru//upload/iblock/22f/Tanygin_Alshaia_Dobritsa_full.pdf. DOI: 10.34759/trd-2020-114-155

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

28. Модель размещения данных во внутренней памяти вычислителя, реализующего схему кодирования данных в режиме сцепления блоков / М. О. Таныгин, А. А. А. Ахмад, О. В. Казакова, Д. Голубов // Известия Юго-Западного государственного университета. – 2023. – Т. 27, № 1. – С. 73-91. – DOI 10.21869/2223-1560-2023-27-1-73-91.

29. Таныгин, М. О. Теоретические основы идентификации источников информации, передаваемой блоками ограниченного размера / М. О. Таныгин. – Курск : Закрытое акционерное общество "Университетская книга", 2020. – 198 с. – ISBN 978-5-907311-85-5.

References

1. Roy, K. S., Sujith, M., Bhanu, B., Preethi, & Hazarika, R. A. (2024). FPGA-based dual-layer authentication scheme utilizing AES and ECC for unmanned aerial vehicles. Eurasip Journal on Wireless Communications and Networking, 2024(1), Article 91.
2. IEEE P2510 – Standard for Establishing Quality of Data Sensor Parameters in the Internet of Things Environment, February 10, 2020
3. Zhou, L., Li, X., Yeh, K., & Chiu, W. Lightweight IoT-based authentication scheme in cloud computing circumstance. Future Gener // Comput. Syst., 2019, 91, 244-251.
4. Abed, A., Abdelhafeez, A., & Fouad, M. Authentication in Cloud Computing Environments. Multicriteria Algorithms with Applications. 2024.
5. Arafin, T., & Qu, G. Hardware-Based Authentication Applications. 2021, 145-181.
6. Al-Shareeda, S. Data authentication algorithms. Authentication Technologies for Cloud Computing, IoT and Big Data. 2019
7. 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
8. Petrov, D. ISM band wireless communication standards // Electronic components. - 2010. - No. 10. - pp. 28-32
9. Perry L. Architecture of the Internet of Things. – Moscow: DMK Press, 2018. – 454 p. ISBN– 978-5-97060-672-8.
10. Kireev, A. O., Svetlov, A.V. Distributed energy monitoring system for wireless sensor networks // Izvestiya SFU. Technical sciences. 2011. No. 5 (118). pp. 60-65.
11. Galkin, P. V. Analysis of energy consumption of wireless sensor network nodes // ScienceRise. 2014. No. 2 (2). pp.55-61.
12. Levchenko, P.; Bankov, D.; Khorov, E.; Lyakhov, A. Performance Comparison of NB-Fi, Sigfox, andLoRaWAN. Sensors 2022, 22, 9633.https://doi.org/10.3390/s22249633
13. Unmanned aircraft systems. Part 3. Operational procedures [Electronic resource] // ISO 21384-3:2019 standard(E). URL:

https://cdn.standards.iteh.ai/samples/70853/7ec34c8a22bf46958423b7e3a2e43693/ISO-21384-3-2019.pdf (accessed 08.11.2025).

14. 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 (12). doi: 10.1155/2016/7672839

15. D. Shant P. Premkumar, «Block Level Data Integrity Assurance Using Matrix Dialing Method towards High Performance Data Security on Cloud Storage,» Scientific Research Publishing, т. 7, № 11, pp. 3626-3644, 2016

16. Black, J. CBC MACs for arbitrary-length messages: The three-key constructions [Текст] / J. Black, P. Rogaway – J. Cryptol, 2015. – vol. 18 – №2 – P. 111–131

17. Ben Othman, S., Alzaid, H., Trad, A., & Youssef, H. An efficient secure data aggregation scheme for wireless sensor networks. // IISA 2013, doi:10.1109/iisa.2013.6623701

18. M. Bellare, J. Kilian, P. Rogaway, “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.

19. W. Stallings “NIST block cipher modes of operation for authentication and combined confidentiality and authentication,” Cryptologia, 2010, № 34, pp. 225- 235, doi: 10.1080/01611191003598295

20. Tanygin M. O., Chesnokova A. A., Dobritsa V. P. Organization of storage of results of intermediate calculations in authentication tasks of message sources of limited length // Proceedings of MAI. – 2023. – № 133.

21. Kolganov, A. S. Parallel implementation of the minimum spanning tree search algorithm using central and graphics processors / A. S. Kolganov // Bulletin of the South Ural State University. Series: Computational Mathematics and Computer Science. – 2016. – Vol. 5. – No. 3. – pp. 5-19. – DOI 10.14529/cmse160301

22. 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

23. Paradies M, Lehner W, Bornhövd C GRAPHITE: an extensible graph traversal framework for relational database management systems. In: DBM. ACM, 2015pp 29:1–29:12. DOI : 10.1145/2791347.2791383

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

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

26. Tanygin M. O., Alshaia H. Ya., Dobritsa V. P. Evaluation of the influence of buffer memory organization on the speed of execution of procedures for determining the source of messages // Proceedings of MAI, 2020, No. 114, http://mai.ru//upload/iblock/22f/Tanygin_Alshaia_Dobritsa_full.pdf . DOI: 10.34759/trd-2020-114-155

27. Plugatarev, A.V. A model for determining the source of messages based on statistical analysis of metadata in an open communication channel / A.V. Plugatarev // Caspian Journal: management and high technologies. – 2022. – № 4(60). – Pp. 30-37. – DOI 10.54398/20741707_2022_4_30.

28. A model of data placement in the internal memory of a computer implementing a data encoding scheme in the block coupling mode / M. O. Tanygin, A. A. A. Akhmad, O. V. Kazakova, D. Golubov // Izvestiya Yugo-Zapadnogo gosudarstvennogo universiteta. – 2023. – Vol. 27, No. 1. – pp. 73-91. – DOI 10.21869/2223-1560-2023-27-1-73-91.

29. Tanygin, M. O. Theoretical foundations of identification of information sources transmitted by blocks of limited size / M. O. Tanygin. – Kursk : Closed Joint Stock Company "University Book", 2020. – 198 p. – ISBN 978-5-907311-85-5.

Информация об авторах

Мухаммед Наджаджра – канд. техн. наук, доцент кафедры информационных систем управления университета Аль-Истикляль, Палестина, Иерихон; ORCID: https://orcid.org/0009-0004-0712-306X; e-mail: mnajajra@pass.ps

Максим Олегович Таныгин, доктор технических наук, заведующий кафедры «Информационная безопасность», ФГБОУ ВО «Юго-Западный государственный университет», г. Курск, Россия; ORCID: https://orcid.org/0000-0002-4099-1414; e-mail: tanygin@yandex.ru

Чеснокова Алина Андреевна, аспирант кафедры «Информационная безопасность», ФГБОУ ВО «Юго-Западный государственный университет», г. Курск, Россия; ORCID: https://orcid.org/0000-0003-1183-4572; e-mail: chesnokova.50@yandex.ru

Information about the authors

Mohammed Najajra, Candidate of Technical Sciences, Associate Professor of the Department of Management Information Systems at Al-Istiqlal University, Jericho, Palestine; ORCID: https://orcid.org/0009-0004-0712-306X; e-mail: mnajajra@pass.ps

Maxim Olegovich Tanygin, Doctor of Technical Sciences, Head of the Department of Information Security, Southwest State University, Kursk, Russia; ORCID: https://orcid.org/0000-0002-4099-1414; e-mail: tanygin@yandex.ru

Alina Andreevna Chesnokova, Postgraduate Student of the Department of Information Security, Southwest State University, Kursk, Russia; ORCID: https://orcid.org/0000-0003-1183-4572; e-mail: chesnokova.50@yandex.ru

Получено 17 февраля 2026 ● Принято к публикации 20 мая 2026 ● Опубликовано 31 августа 2026
Received 17 February 2026 ● Accepted 20 May 2026 ● Published 31 August 2026