Оригинальная статья / Original article

https://doi.org/10.21869/2223-1560-2020-24-1-175-188

Восстановление порядка следования информационных пакетов на основе анализа хеш-последовательностей

М.О. Таныгин [1] ✉

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

✉ e-mail: tanygin@yandex.com

Резюме

Цель исследования. *В настоящее время для контроля целостности и аутентичности данных, передаваемых по открытым каналам связи, используются различные технологии и методы. Одним из таковых является технология передачи последовательностей информационных пакетов, связанных друг с другом в цепочки по определённым криптографическим алгоритмам. Аналогичные подходы используются в широко известной технологии блокчейн и ориентированы на большие объёмы передаваемой и защищаемой информации и большие размеры дополнительных служебных полей данных. Целью настоящей статьи является исследование характеристик систем, передачи информационных пакетов небольшого, в сравнении с традиционными размерами кадров стека протоколов TCP/IP, размера, в которых нарушенный порядок следования пакетов восстанавливается с помощью метода цепочек, за счёт анализа хеш-последовательностей, имеющихся в составе каждого такого пакета.*

Методы. *В данной статье использовались имитационное моделирование, метод системного анализа, метод систематизации и ранжирования полученных результатов.*

Результаты. *Показано, что существенное влияние на снижение вероятности ошибочного восстановления порядка следования информационных пакетов оказывает повышение размера дополнительного поля с хешем предыдущего сообщения с 4 до 6 битов. Дальнейшее увеличение длины поля хеша снижает вероятность ошибки лишь на 2 – 5 % на каждый дополнительный бит поля хеша при любой длине восстанавливаемой цепочки. Показано, что коэффициент использование канала связи – отношение объёма полезной цепочки пакетов к объёму всей информации, переданной по каналу связи – максимален при длине поля хеша 6 во всём диапазоне размеров поля информационной части пакета данных.*

Заключение. *В работе показано, что метод цепочек применим для восстановления исходной последовательности передаваемых от источника в приёмник информационных пакетов в системах, где сохранение очерёдности следования пакетов не гарантируется. Полученные значения параметров работы системы передачи позволяют обеспечить приемлемую надёжность передачи данных при минимальном объёме дополнительной служебной информации и достичь информационной избыточности меньше, чем у аналогов на 10–15%.*

Ключевые слова: *передача информации; метод цепочек; хеш; имитационное моделирование; вероятность ошибки передачи данных.*

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

Для цитирования: Таныгин М.О. Восстановление порядка следования информационных пакетов на основе анализа хеш-последовательностей // Известия Юго-Западного государственного университета. 2020; 24(1): 175-188. https://doi.org/10.21869/2223-1560-2020-24-1-175-188.

Поступила в редакцию 28.11.2019 *Подписана в печать 14.01.2020* *Опубликована 21.02.2020*

Restoring the Order of Information Packets Based on Hash Sequence Analysis

Maxim O. Tanygin [1] ✉

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

✉ e-mail: tanygin@yandex.com

Abstract

Purpose of research. *Currently, various technologies and methods are used to control the integrity and authenticity of data transmitted through open communication channels. One of them is the technology for transmitting sequences of information packets connected to each other in chains using certain cryptographic algorithms. Similar approaches are used in the well-known blockchain technology and are focused on large volumes of transmitted and protected information and large sizes of additional service information fields. The purpose of this article is to study the characteristics of systems, transmission of small information packets in comparison with traditional size frames of TCP/IP stack, in which the broken packet sequence order is restored using the chain method, by analyzing hash sequences available in each of such packets.*

Methods. *In this article, simulation modeling, system analysis method, method of systematization and ranking of the obtained results are used.*

Results. *It is shown that increasing the size of the additional field with the hash of the previous message from 4 to 6 bits has a significant effect on reducing the probability of erroneous restore of the order of information packets. Further increasing the length of the hash field reduces the probability of error by only 2 to 5 % for each additional bit of the hash field for any length of the chain being restored. It is shown that the coefficient of the usage of the communication channel (the ratio of useful chain of packets to the volume of information transmitted through the communication channel) is maximum when the length of the hash field is 6 in the whole range of sizes of the field information part of the data packet.*

Conclusion. *The paper shows that the chain method is applicable for restoring the original sequence of information packets transmitted from the source to the receiver in systems where the preservation of the sequence of packets is not guaranteed. The obtained values of the transmission system parameters allow us to ensure acceptable reliability of data transmission with a minimum amount of additional service information, and achieve information redundancy less than that in similar ones by 10-15.*

Keywords: *information transmission; chain method; hash, simulation modelling, probability of data transferring error.*

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

For citation: Tanygin M. O. Restoring the Order of Information Packets Based on Hash Sequence Analysis. *Izvestiya Yugo-Zapadnogo gosudarstvennogo universiteta = Proceedings of the Southwest State University*. 2020, 24(1): 175-188 (In Russ.). https://doi.org/10.21869/2223-1560-2020-24-1-175-188.

Received 28.11.2019 *Accepted 14.01.2020* *Published 21.02.2020*

***

Введение

Технология блок-чейн, то есть объединение в структурированную последовательность информации, представленной в форме отдельных блоков за счёт использования функций криптографического хеширования, приобрела в последнее время широкую известность. С помощью децентрализованного и распределенного управления данными существует возможность определения доверия на основе встроенного механизма криптографии и консенсуса, обеспечивая тем самым безопасность, анонимность и целостность данных. В то же время, развитие данной технологии подтолкнуло исследования в смежных направлениях информатики и теории связи, обеспечивая решение ряда проблем информационной безопасности [1]. Например, подходы, используемые в технологии блок-чейн, схожи с подходами, используемыми для аутентификации удалённых субъектов информационного обмена.

Предметом настоящей статьи являются системы, состоящие из источника и приёмника информационных блоков небольшого, в сравнении с традиционными размерами кадров стека протоколов TCP/IP, размера. Примером такой системы может быть программно-аппаратная система, в которой основные функции выполняются в аппаратном средстве, а программное обеспечение осуществляет управление его работой и другие сервисные операции [2 – 4]. Согласно правилам, реализованным в протоколе PCI Express, упорядочивание поступающих в приёмник пакетов не гарантируется для сохранения высокой скорости передачи данных [5]. В результате, при взаимодействии двух конечных устройств или программного обеспечения и устройства между собой возникает потребность в потоковой высокоскоростной передаче данных при соблюдении последовательности передаваемых данных. Это, в свою очередь, требует при передачи пакетов произвольной длины по стандартному PCIe, использовать алгоритмы, позволяющие исключать изменения порядка следования пакетов, один из которых рассмотрен в [6]. В настоящей работе мы исследуем свойства подобных алгоритмов, снижающих вероятности ошибочной передачи данных за счёт подходов, аналогичных подходам, используемым в блок-чейн.

Материалы и методы

Для рассматриваемой системы были определены следующие принципы работы алгоритма опознания поступающих информационных пакетов.

В качестве таких условий выступают:

– на источнике генерируются информационные пакеты и передаются по каналу связи в приемник;

– при передаче по каналу пакеты могут быть перемешаны, в результате чего порядок их поступления в приёмник будет отличаться от порядка их выдачи источником;

– проблема сохранения целостности информационных пакетов в настоящей работе не рассматривается.

Исходный порядок следования пакетов в приёмнике восстанавливается с помощью метода цепочек [7 – 9], заключающегося в том, что в информационный пакет добавляется сформированная каким-либо образом идентификационная информация, в нашем случае хеш-последовательность, сформированная из данных предыдущего пакета (рис. 1). Эта информация позволяет в ходе проверки точно определить, во-первых, принадлежность конкретного пакета последовательности и, во-вторых, место пакета в последовательности [10, 11].

Хеш поступившего пакета сравнивается со всеми хешами, сформированными пакетов, полученных приёмником к настоящему моменту времени, и, в случае совпадения блок добавляется в последовательность на требуемую позицию (рис. 2).

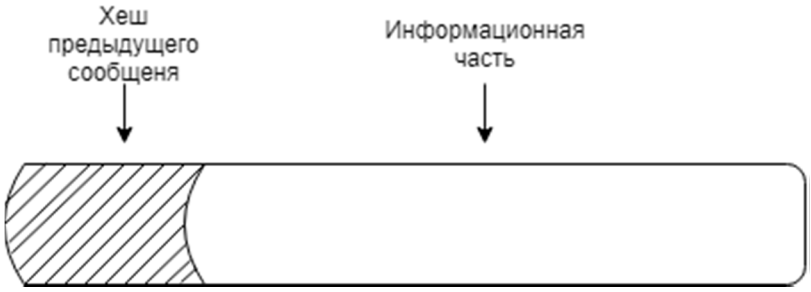

Рис. 1. Структура пакета

Fig. 1. The packet structure

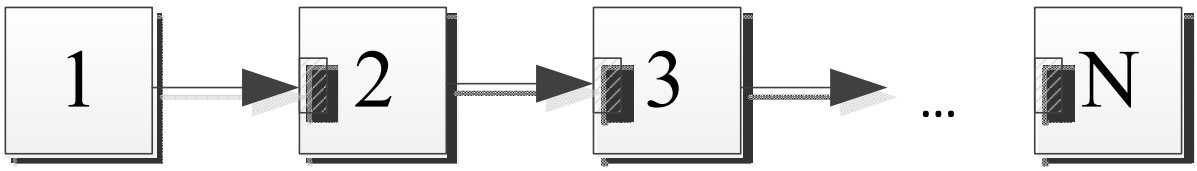

Рис. 2. Исходный порядок пакетов

Fig. 2. The original order of the packets

Условие записи пакета на позицию i в цепочке выглядит следующим образом

$$\begin{cases} S_{i+1}^{hash}=F_{hash}\left(S_i^{inf}\right). \\ S_i^{hash}=F_{hash}\left(S_{i-1}^{inf}\right),\ i=\overline{1\ldots N}, \end{cases} \quad (1)$$

где $S_i=\left\{S_i^{inf}\middle|S_i^{hash}\right\}$ – пакет, записываемый на позицию i, состоящий из информационной части S_i^{inf} и хеша S_i^{hash};

F_{hash} – хеш–функция;

S_{i-1}^{inf} – информационная часть пакета, которая будет записана на позицию i–1;

S_{i+1}^{hash} – хеш пакета, который будет записан на позицию i+1;

N – размер цепочки пакетов.

Как было сказано выше, при передаче пакетов порядок их следования может быть изменён. Поэтому проверка условия (1) должна происходить в приёмнике при каждом новом поступив-

шем пакете, и вся цепочка будет перестраиваться.

В процессе проверки хешей в приёмнике могут возникнуть коллизии. Коллизия – это ситуация, в которой, при правильном выполнении алгоритма хеширования, у двух или более различных пакетов получается один и тот же хеш [12]. Схематично данная ситуация представлена на рис. 3. В случае возникновения коллизии задача определения позиции пакета в цепочке не может быть разрешена исходя из имеющихся данных и требуется повторная передача всей цепочки.

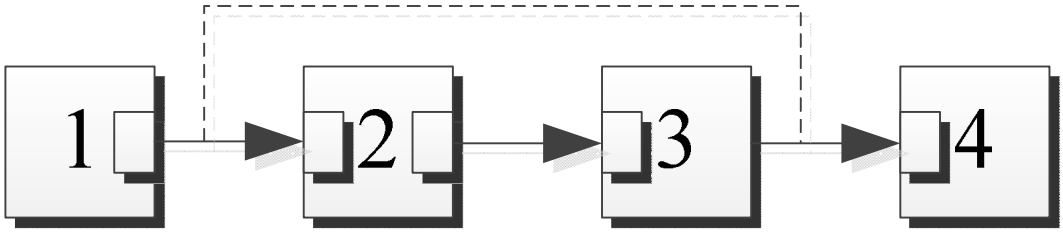

Рис. 3. Пример коллизии

Fig. 3. A collision example

Задача настоящего исследования состоит в определении вероятности возникновения подобных коллизий в системах, где на размер пакета накладываются серьезные ограничения. Причиной возникновения подобных ограничений является невысокая скорость передачи и требуемое высокое время отклика, что характерно, например, для протоколов, по которым работают устройства интернета вещей [13]. В подобных протоколах размер пакета может составлять несколько байтов [14]. Соответственно, размер поля хеша не должен превышать несколько битов.

В качестве основной характеристики, на которую влияет выбор метода восстановления порядка пакетов, является информационная избыточность – необходимый для организации сеанса связи объём информации, который анализируется приёмником для принятия решения о номере конкретного информационного пакета в последовательности. Это могут быть как передаваемые между источником и приёмником сеансовые параметры связи, криптографические ключи, идентификаторы, адреса, так и информация, содержащаяся в повторно посылаемых данных. Необходимость в таких повторных отправках возникает в результате ошибок и коллизий. Для нашего метода именно повторно пересылаемые данные будут вносить главный вклад в информационную избыточность, так как для описания процесса передачи: количества пакетов в цепочке, длины служебных полей и пр. достаточно буквально нескольких битов.

Исследования численных характеристик системы построения цепочек

пакетов на основе хешей представляет собой достаточно сложную задачу, при решении которой необходимо сделать множество допущений, снижающих достоверность полученного результата [15]. Поэтому было принято решение использовать имитационное моделирования процесса передачи и анализа поступающих пакетов [16]. Модель, реализованная в среде Mathcad, формировала случайным образом последовательность информационных пакетов, дополняла каждый пакет хешем требуемой длины, выполняла их перемешивание (изменение порядка поступления в приёмник) и последующее восстановление исходной последовательности [17]. В случае возникновения коллизии и невозможности выполнить задачу построения последовательности формировалось соответствующее сообщение. Для определения математического ожидания вероятности возникновения коллизии эксперимент для каждого тестового набора входных данных (длина хеша, тап хеш-функции) проводился 10^4 раз. При таком количестве опытов величина стандартной ошибки для полученного значения математического ожидания вероятности коллизии имеет порядок 10^{-3} [18].

Результаты и их обсуждение

В результате имитационного моделирования установлено, что на среднюю вероятность возникновения коллизии тип хеш–функции не влияет, влияет лишь длина поля хеша. Зависимость вероятности возникновения коллизии P_{coll} от длины поля хеша L_{hash} приведена на рис. 4.

Рис. 4. Зависимость вероятности возникновения коллизии P_{coll} от длины поля хеша L_{hash} при длине цепочки l_{cain} = 15

Fig. 4. Dependence of the probability of a collision P_{coll} on hash size L_{hash} with chain length l_{cain} = 15

График зависимости вероятности коллизий построен для значения длины цепочки информационных пакетов l_{cain} = = 15. График зависимости вероятности коллизии от длины поля хеша L_{hash} и длины цепочки l_{cain} показан на рис. 5. Для большей наглядности ось l_{cain} приведена в нелинейном масштабе. Анализ графиков на рис. 4 и 5 показывает, что длина поля хеша оказывает значительное влияние на вероятность коллизии лишь до значения 6. Дальнейший рост длины поля хеша снижает вероятность в пределах 1% на каждый дополнительный бит длины. Также незначительное влияние оказывает длина восстанавливаемой приёмником цепочки: рост на 10% при росте длины цепочки с 15 до 60 информационных пакетов. Следует отметить, что подобный рост вероятности коллизии наблюдается лишь при небольших длинах поля хеша L_{hash}. При больших значениях L_{hash} рост вероятности не превышает 5%. В связи с тем, что длина цепочки оказывает несущественное влияние на вероятность коллизии по сравнению с длиной поля хеша, дальнейшие данные экспериментов приведены для l_{cain} = 15.

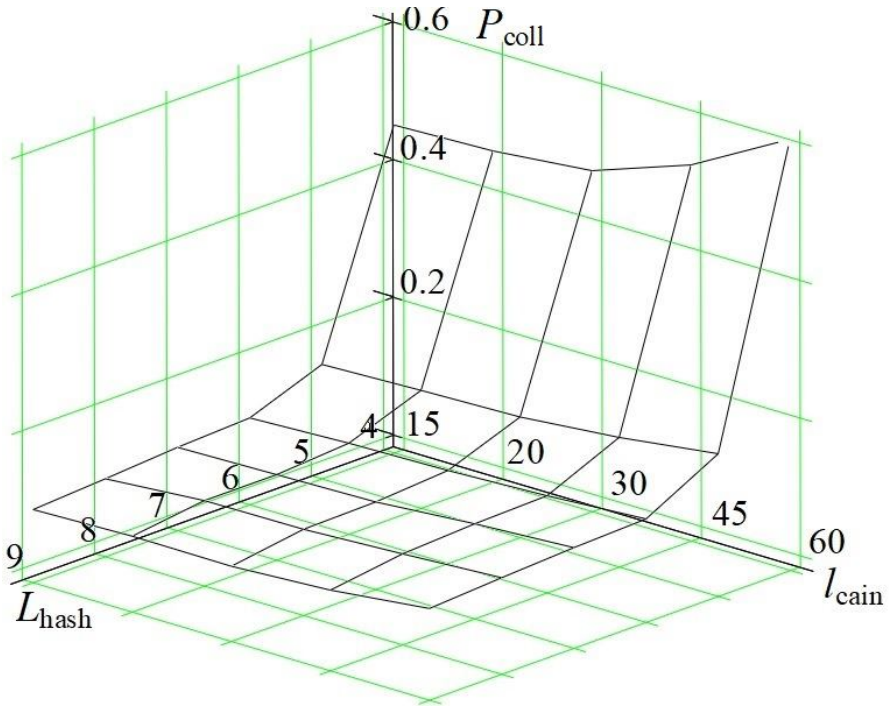

Рис. 5. Зависимость вероятности возникновения коллизии P_{coll} от длины поля хеша L_{hash} и длины цепочк l_{cain}

Fig. 5. Dependence of the probability of a collision P_{coll} on hash size L_{hash} and chain length l_{cain}

Переходя к анализу целевой характеристики эффективности – информационной избыточности, введём специальную меру – коэффициент использования канала K [16]. Данный коэффициент показывает отношение объёма полезной цепочки пакетов к объёму всей информации, переданной по каналу связи. При расчете данного параметра мы учитывали, что коллизия требует

повторной передачи данных, а следовательно, данный коэффициент должен находиться в прямой зависимости от вероятности успешной передачи всей цепочки пакетов [19]. Итоговая формула для коэффициента использования канала имеет вид:

$$K = \frac{L_{\text{inf}} \cdot \left(1 - P_{\text{coll}}\right)}{L_{\text{inf}} + L_{\text{hash}}}, \qquad (2)$$

где L_{hash} – длина поля хеша пакета (см. рис. 1),

L_{inf} – длина информационного поля пакета;

P_{coll} – вероятность коллизии при данной длине поля хеша пакета.

Анализ графика коэффициента использования канала (рис. 6) показывает очевидную тенденцию: с ростом длины информационной части коэффициент использования канала растёт при любом значении длины хеша. В то же время ярко выраженный максимум данного коэффициента наблюдается в районе $L_{\text{hash}} = 6$, где график образует своеобразный «гребень». Трактовать это можно следующим образом. При значениях длины поля хеша $L_{\text{hash}} < 6$, коэффициент использования канала уменьшается за счёт высокой вероятности коллизий, которые требует повторения сеанса передачи всей цепочки. При значениях длины поля хеша $L_{\text{hash}} > 6$, коэффициент использования канала снижается за счёт роста длины поля хеша при незначительном (см. рис. 4) снижении вероятности коллизии.

Если сравнивать описываемый в статье метод восстановления последовательностей сообщений с известными, то в качестве аналогичных можно упомянуть метод контроля целостности и аутентичности, описанный в работе [20]. Отсутствие ошибок передачи доставки для каждого пакета определяется по результатам операций в полях Галуа над двумя матрицами: одной, проверочной, хранящейся в приёмнике и задающей, на основе которой формируется вектор пакетов небольшого размера (сопоставимого с размерами пакетов, рассмотренных в настоящей работе). Сами матрицы дополняются псевдослучайными числами для повышения защищённости передаваемых данных. Для обеспечения секретности по структуре матрицы, полученной в результате операций над вышеуказанными двумя матрицами, принимается решение о правильности или неправильности доставки конкретного блока и о корректности его позиционирования в итоговом собранном из отдельных блоков сообщении. Метод позволяет безошибочно передавать фрагментированную на отдельные пакеты информацию за счёт универсальных характеристики, получаемых в результате матричных преобразований над проверочной матрицей и вектором поступающих слов. Преимуществом предлагаемого метода является отсутствие необходимости хранить в приёмнике большую по объёму матрицу чисел, необходимую для проверки поступающих пакетов.

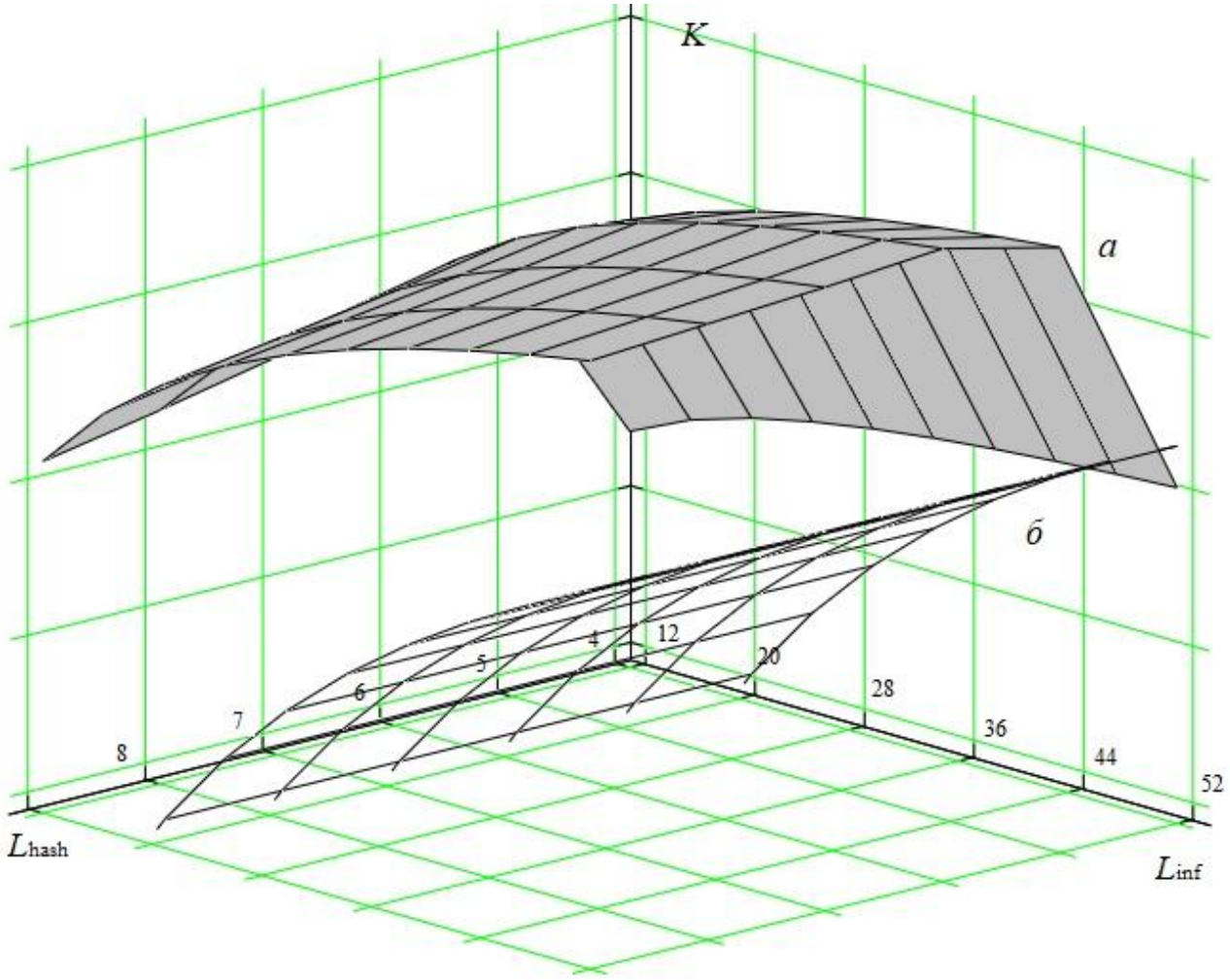

Рис. 6. Зависимость коэффициента *K* использования канала от длины дополнительных полей L_{hash} и длины информационного поля L_{inf}: **а** – метод на основе хешей; **б** – метод динамически конфигурируемых маршрутов доставки

Fig. 6. Dependence of the channel consumption coefficient *K* on additional field size L_{hash} and information field size L_{inf}: **а** – the hash-based method; **б** – the method for dynamically configured delivery routes

Сам размер такой матрицы, превышающий в несколько раз размер вектора данных, и необходимость её передачи из источника в приёмник позволяет достичь указанного в настоящей работе коэффициента использования канала в 80% лишь при использовании такой матрицы для контроля передачи пакетов в более чем ста последовательных сеансах передачи. Тогда как описанный метод позволяет использовать небольшой идентификатор источника для формирования хешей пакетов, размером, не превышающим один блок информации, что позволяет менять его практически каждый цикл передачи цепочки пакетов, что в целом делает подобную передачу более защищённой.

Другим методом, с которым можно сравнить описываемый, является метод контроля правильности поступления информационных пакетов в приёмник

за счёт контроля динамически конфигурируемых маршрутов доставки каждого из них [21]. Его особенностью является большой объём дополнительной служебной информации, доходящий до 30% от общего объёма передаваемой информации при размере контролируемых пакетов в несколько десятков байтов. На рис. 6 численные характеристики этого метода приведены для сравнения с характеристиками обсуждаемых. Обсуждаемый в настоящей статье метод, в сравнении с ним, обеспечивает меньшую информационную избыточность (до 15-25%) при сравнительно меньшем размере пакетов, формирующих цепочку.

Результат сравнения обсуждаемого в настоящей статье метода с аналогами можно представить в виде табл. 1.

Таблица 1. Сравнение методов восстановления последовательности сообщений

Table 1. Comparison of methods for restoring the messages sequence

Методы восстановления последовательности	Критерии		
	Отношение объёма параметров связи к объёму данных, передаваемых за один сеанс	Зависимость от условий канала связи	Информационная избыточность
Метод на основе хешей	<5%	отсутствует	15-25%
Метод на основе матричных преобразований	до 400%	отсутствует	-
Метод на основе динамически конфигурируемых маршрутов доставки	-	определяет объём дополнительных описателей маршрута	30%

Анализ таблицы позволяет сказать, что метод на основе хешей позволяет снизить объём дополнительных данных, передаваемых по каналам связи для обеспечения восстановления порядка следования информационных пакетов, при этом сохраняя возможность оперативного изменения отдельных сеансовых параметров передачи.

Выводы

Проведённые исследования позволяют сделать ряд выводов. Метод цепочек, заключающийся в формировании на основе криптографических преобразований цепочек связанных друг с другом в определённом порядке информационных пакетов, может быть применим для восстановления исходной последовательности пакетов, передаваемых от источника в приёмник, в системах, где сохранение очерёдности следования пакетов не гарантируется. Его использование целесообразно даже в системах, в которых размер передаваемого пакета может быть всего несколь-

ко байтов. Основным недостатком метода цепочек является возникновение коллизий – ситуаций совпадения значений в дополнительных полях информационных пакетов. Аналитический расчет вероятности возникновения подобных коллизий достаточно сложен и сопряжён с многочисленными упрощениями и пренебрежениями. Поэтому имитационное моделирование является целесообразным способом определения численных характеристик системы передачи пакетов с контролем очерёдности следования на основе метода цепочек.

Полученные в результате имитационного моделирования характеристики подобных систем позволяют определить целесообразные значения длины дополнительного поля хеша в информационном пакете, которое для систем с размером пакета в 4 – 7 байтов составляет 6 битов. При этом объём полезной информации достигает 80% от общего объёма данных, передаваемых по каналу связи, с учётом необходимости повторной передачи всей цепочки пакетов в случае возникновения ошибки, что больше, чем у известных аналогов. Данный метод позволяет использовать сеансовые параметры для формирования хеш–последовательностей, практически не повышая информационную избыточность, что делает его использование предпочтительным по сравнению с аналогами. Установлено, что путём ограничения длины цепочки пакетов, связанных с друг другом на основе хешей, можно незначительно, в пределах 10%, снизить вероятность возникновения ошибок восстановления исходной последовательности в приёмнике.

Список литературы

1. Kanter W., Kinzel E., Kanter Secure exchange of information by synchronization of neural networks // Europhysics Letters. 2002. Vol. 57. Is. 1, P. 141-147.

2. Глазков А. С., Типикин А. П. Метод и функциональная организация контроля обращений и закрытия доступа к секторам файлов при хищении накопителя информации // Информационные технологии. 2010. № 5. С. 25–30.

3. Типикин А.П., Глазков А.С., Муратов С.А. Организация пользовательской системы защиты информации, хранящейся на жестком магнитном диске // Телекоммуникации. 2009. №10. С.33 – 37.

4. Таныгин М. О., Типикин А. П. Архитектура системы аппаратного ограничения доступа к информации на жестком диске ЭВМ // Телекоммуникации. 2006. №3. С.44 – 46.

5. PCI Special Interest Group. PCI Express® Base Specification Revision 3.0. URL: http://citeseerx.ist.psu.edu/viewdoc/download?doi=10.1.1.694.7081&rep=rep1&type=pdf (дата обращения 15.10.2019)

6. Способ обмена данными между контроллерами защиты информации по протоколу PCI– Express / В.П. Добрица, Е.В. Непочатых, Р.С. Слободин, Е.В. Талдыкин, М. О. Таныгин, А. П. Типикин // Телекоммуникации. 2019. №8. С.21 – 26.

7. Stallings W. NIST Block Cipher Modes of Operation for Confidentiality // Cryptologia. 2010. № 34(2). P. 163 – 175.

8. Bellare M., Canetti R., Krawczyk H. Keying hash functions for message authentication // Advances in Cryptology. 1996. Vol. 1. 109 of Lecture Notes in Computer Science. P. 1 – 15.

9. Karri R., Rajendran J., Rosenfeld K. Trustworthy hardware: Identifying and classifying hardware Trojans. Moscow, Tehranipoor – Computer (Long. Beach. Calif). 2016. №10. C. 39 – 46.

10. Black J., Rogaway P. CBC MACs for arbitrary-length messages: The three-key constructions // J. Cryptol. 2015. Vol. 18. №2. P. 111–131.

11. Kruti S., Gambhava B. New Approach of Data Encryption Standard Algorithm // Int. J. Soft Comput. Eng. 2015. №1. 369 p.

12. Bellare M., Kilian J., Rogaway P. The security of the cipher block chaining message authentication code // JCSS. 1994. Vol. 3. № 3. P. 341–358.

13. Лоднева О.Н., Ромасевич Е.П. Анализ трафика устройств интернета вещей // Современные информационные технологии и ИТ-образование. 2018. Т. 14, № 1. С. 149 – 169.

14. Зайцев В., Соколов Н. Особенности мультисервисного трафика с учетом сообщений, создаваемых устройствами IoT // Первая миля. 2017. № 4. С. 44 – 47.

15. Установление доверительного канала обмена данными между источником и приёмником информации с помощью модифицированного метода одноразовых паролей / М.О. Таныгин, Х.Я. Алшаиа, В.А. Алтухова, А.Л. Марухленко // Известия Юго-Западного государственного университета. Серия: Управление, вычислительная техника, информатика. Медицинское приборостроение. 2018. Т. 8, № 4 (29). С. 63-71.

16. Каталевский Д. Ю. Основы имитационного моделирования и системного анализа в управлении. М., 2015. С. 62-98.

17. Hellerman H. Digital Computer System Principles // McGraw-Hill, 1967. P. 134-142.

18. Ткалич В.Л., Лабковская Р.Я. Обработка результатов технических измерений. СПб: СПбГУ ИТМО, 2011. 72 с.

19. Олифер В. Г., Олифер Н. А. Первые глобальные сети // Компьютерные сети. Принципы, технологии, протоколы. 5-е изд. СПб.: Питер, 2016.

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

21. 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

References

I. Kanter W., Kinzel E., Kanter Secure exchange of information by synchronization of neural networks. *Europhysics Letters*, 2002, vol. 57, is. 1, pp. 141-147.

2. Glazkov A. S., Tipikin A. P. Metod i funkcional'naya organizaciya kontrolya obrashchenij i zakrytiya dostupa k sektoram fajlov pri hishchenii nakopitelya informacii [Method and functional organization of access control and closing access to file sectors in case of theft of the information storage device]. *Informacionnye tekhnologii= Information technology*, 2010, no. 5, pp. 25–30 (In Russ.).

3. Tipikin A.P., Glazkov A.S., Muratov S.A. Opganizaciya pol'zovatel'skoj sistemy zashchity infopmacii, hpanyashchejsya na zhestkom magnitnom diske [Organization of user system for protecting information stored on a hard magnetic disk]. *Telekommunikacii = Telecommunications*, 2009, no.10, pp.33 – 37 (In Russ.).

4. Tanygin M. O., Tipikin A. P. Aphitektupa sistemy apparatnogo ogranicheniya dostupa k informacii na zhestkom diske [Architecture of the system of hardware restriction of access to information on the hard disk of a computer]. *Telekommunikacii = Telecommunications*, 2006, no.3, pp.44 – 46 (In Russ.).

5. PCI Special Interest Group. PCI Express® Base Specification Revision 3.0. Available at: http://citeseerx.ist.psu.edu/viewdoc/download?doi= 10.1.1.694.7081&rep= rep1&type=pdf (accessed 15.10.2019).

6. Dobrica V.P., Nepochatyh E.V., Slobodin R.S., Taldykin E.V., Tanygin M. O., Tipikin A. P. Sposob obmena dannymi mezhdu kontrollerami zashchity informacii po protokolu PCI– Express [Method of data exchange between controllers of information protection on proto-Cola PCI-Express]. *Telekommunikacii = Telecommunications*, 2019, no.8, pp.21 – 26 (In Russ.).

7. NIST Block Cipher Modes of Operation for Confidentiality. *Cryptologia*, 2010, no. 34(2), pp. 163 – 175.

8. M. Bellare, R. Canetti, H. Krawczyk Keying hash functions for message authentication. *Advances in Cryptology*, 1996, vol. 1109 of Lecture Notes in Computer Science, pp. 1 – 15.

9. Karri R., Rajendran J., Rosenfeld K. Trustworthy hardware: Identifying and classifying hardware Trojans. Moscow, Tehranipoor – Computer (Long. Beach. Calif), 2016, no.10, pp. 39 – 46.

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

11. Kruti S., Gambhava B. New Approach of Data Encryption Standard Algorithm. *Int. J. Soft Comput. Eng*, 2015, no.1, 369 p.

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

13. Lodneva O.N., Romasevich E.P. Analiz trafika ustrojstv interneta veshchej [Analysis of traffic devices in the Internet of things]. *Sovremennye informacionnye tekhnologii i IT-*

obrazovanie = Modern information technologies and it education, 2018, vol. 14, no. 1, pp. 149 – 169 (In Russ.).

14. Zajcev V., Sokolov N. Osobennosti mul'tiservisnogo trafika s uchetom soobshchenij, sozdavaemyh ustrojstvami IoT [Features of multiservice traffic taking into account the messages generated by IoT devices]. *Pervaya milya = First mile*, 2017, no. 4, pp. 44 – 47 (In Russ.).

15. Tanygin M.O., Alshaia H.YA., Altuhova V.A., Maruhlenko A.L. Ustanovlenie doveritel'nogo kanala obmena dannymi mezhdu istochnikom i priyomnikom informacii s pomoshch'yu modificirovannogo metoda odnorazovyh parolej [Establishing a trusted data exchange channel between the source and receiver of information using a modified method of disposable pairs]. *Izvestiya Yugo-Zapadnogo gosudarstvennogo universiteta. Seriya: Upravlenie, vychislitel'naya tekhnika, informatika. Meditsinskoe priborostroenie = Proceedings of the Southwest State University. Series: Control, Computing Engineering, Information Science. Medical Instruments Engineering,* 2018, vol. 8, no. 4 (29), pp. 63-71 (In Russ.).

16. Katalevskij D. Yu. *Osnovy imitacionnogo modelirovaniya i sistemnogo analiza v upravlenii* [Fundamentals of simulation modeling and system analysis in management]. Mocow, 2015, pp. 62-98 (In Russ.).

17. Hellerman H. Digital Computer System Principles. McGraw-Hill, 1967, pp.134-142

18. Tkalich V.L., Labkovskaya R.Ya. *Obrabotka rezul'tatov tekhnicheskih izmerenij* [Processing of technical measurement results]. Saint Petersburg, 2011, 72 p. (In Russ.).

19. Olifer V. G. Olifer N. A. Pervye global'nye seti [First global networks]. *Komp'yuternye seti. Principy, tekhnologii, protokoly* [Computer networks. Principles, technologies, protocols]. Saint Petersburg, Piter Publ., 2016 (In Russ.).

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

21. 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

Информация об авторе / Information about the Author

Максим Олегович Таныгин, кандидат технических наук, заведующий кафедрой «Информационная безопасность», ФГБОУ ВО «Юго-Западный государственный университет», г. Курск, Российская Федерация, e-mail: tanygin@yandex.ru

Maxim O. Tanygin, Cand. of Sci. (Engineering), Head of the Information Security Department, Southwest State University, Kursk, Russian Federation, e-mail: tanygin@yandex.ru