УДК 004.052 DOI: 10.34759/trd-2021-117-12

Сложность алгоритма определения источника данных

Таныгин М.О.*, Алшаиа Х.Я., Митрофанов А.В.*****

Юго-Западный государственный университет, ЮЗГУ,

ул. 50 лет Октября, 94, Курск, 305040, Россия

**e-mail: tanygin@yandex.ru*

***e-mail: haideryhy7@gmail.com*

****e-mail: mitro3000@rambler.ru*

Статья поступила 12.02.2021

Аннотация

В статье рассмотрена проблема оценки трудоёмкости процедур определения источника поступающих информационных блоков. Определены зависимости между характеристиками информационных систем, размерами полей служебной информации и числом элементарных операций, выполняемых при идентификации источника, сформировавшего пакет данных. Показано, что в рабочих диапазонах сложность реализации рассматриваемого метода определения линейно зависит от числа идентифицируемых приёмником источников.

Ключевые слова: обработка данных, приёмник сообщений, сложность алгоритма, быстродействие, математическое моделирование.

Введение

Задача обеспечения безошибочного взаимодействия удалённых субъектов информационного обмена является типовой в современных средствах вычислительной техники, распределённых информационно-управляющих система, системах управления подвижными объектами [1–4]. Одним из подходов, направленных на её решение, является объединение на стороне приёмника поступающих пакетов в структурированные множества и проверка для этих множеств некоторых значений, высчитываемых исходя из содержимого пакетов и некоторых априорных данных, известных источнику и приёмнику. Для связи пакетов в множества или цепочки используются режимы блочного кодирования данных, при котором предыдущий блок данных связывается с текущим блоком по некоторым алгоритмам [4, 6]. Ещё одним способом группирования пакетов и принятия решения об их источнике может быть исчисление для группы блоков данных некоторой цифровой метрики, анализируя значение которой принимается решение, во-первых, о корректности формирования группы пакетов данных, а, во-вторых, об источнике пакетов [7]. Ещё одной группой методов определение источника сообщений является анализ маршрутов передачи информационных пакетов от источника к приёмнику [8, 9].

В то же время реализуемые связывания данных в цепочки имеют своей целью повышение достоверности анализа поступающих пакетов данных [6]. Тогда как проблемы их вычислительной сложности в реальных условиях эксплуатации остаются без внимания [10]. При этом вычислительная сложность реализуемых механизмов

влияет не только на скорость обработки поступающего информационного потока [11], но и, в случае взаимодействия автономных комплексов, из-за дополнительных энергетических затрат, на их автономность [12 – 13]. Сложность рассматриваемых методов определяется числом анализируемых вариантов группирования пакетов и, в наихудшем случае может быть вида $O(n!)$, где n – размер множества пакетов, для которого выполняются процедуры идентификации его источника. Это обуславливает актуальность задачи разработки методов идентификации источников данных, обладающих приемлемой сложность для реализации в составе автономных роботизированных комплексов. Целью работы является исследование алгоритмической сложности одного метода определения источника блочных данных, поступающих в приёмник, основанного на анализе небольшой по объёму служебной информации, передаваемой и обрабатываемой вместе с основными данными

Материалы и методы

В качестве предмета исследования мы выбрали метод определения источника пакетов данных на основе анализе позиции пакета в некотором структурированном множестве (сообщении) и хеше, формируемом из данных пакета, подробно описанный в [15]. Он основан на буферизации анализируемых пакетов во внутренней памяти приёмника, формировании на основе метода (цепочки связанных блоков) древовидной структуры, объединяющей все поступившие информационные пакеты (допускается вхождение одного пакета в несколько ветвей такой структуры) и применении

решающего правила к каждой сформированной ветви такой структуры. В качестве такого правила выступает равенство длины ветви некоторому заранее определённому числу n – максимальной длине фрагментированного на пакеты сообщения, среди блоков ветви встречается ровно один раз некий выделенный числовой идентификатор (индекс блока), порядок следования блоков, обладающих такими идентификаторами, строго определён алгоритмов взаимодействия источника и приёмника и хеш, формируемый из данных предыдущего блока повторяет содержимое специального поля последующего.

В основе алгоритма, реализующего вышеописанный метод, лежит разбиение множества пакетов данных U, поступивших в приёмник к определённому моменту времени на подмножества $w_1 - w_{n+1}$, содержащие пакеты с одинаковым индексом, где n – максимальный номер блока во множестве пакетов. Затем последовательно формируются подмножества $u_1 - u_v$, v - максимальное число ветвей формируемой приёмником древовидной структуры, которое в общем случае не ограничено сверху. Для каждого блока такого подмножества верно соотношение [16]:

$$\begin{aligned} f^{\text{ind}}\left(\tilde{u}^{\langle i\rangle}, S^{\text{key}}\right) &= i, \\ f^{sh}\left(u_i, S^{\text{key}}\right) &= F_{\text{hash}}\left(f^{si}\left(u_{i-1}, S^{\text{key}}\right)\right) \end{aligned} \qquad (1)$$

где: f^{si} – операция декодирования информационной части пакета,

f^{ind} – операция декодирования содержимого поля индекса пакета,

f^{sh} – операция декодирования содержимого поля хеша пакета.

Затем проверяется равенство длины всех подмножества $u_1 - u_v$, значению n. В случае отсутствия ошибок идентификации источника, этому условию должно удовлетворять только одно подмножество, пакеты которого опознаются как пакеты, сформированные целевым источником, а порядок их следования определяется их порядком в таком подмножестве. Блок-схема алгоритма определения источника пакетов приведена на рисунке 1.

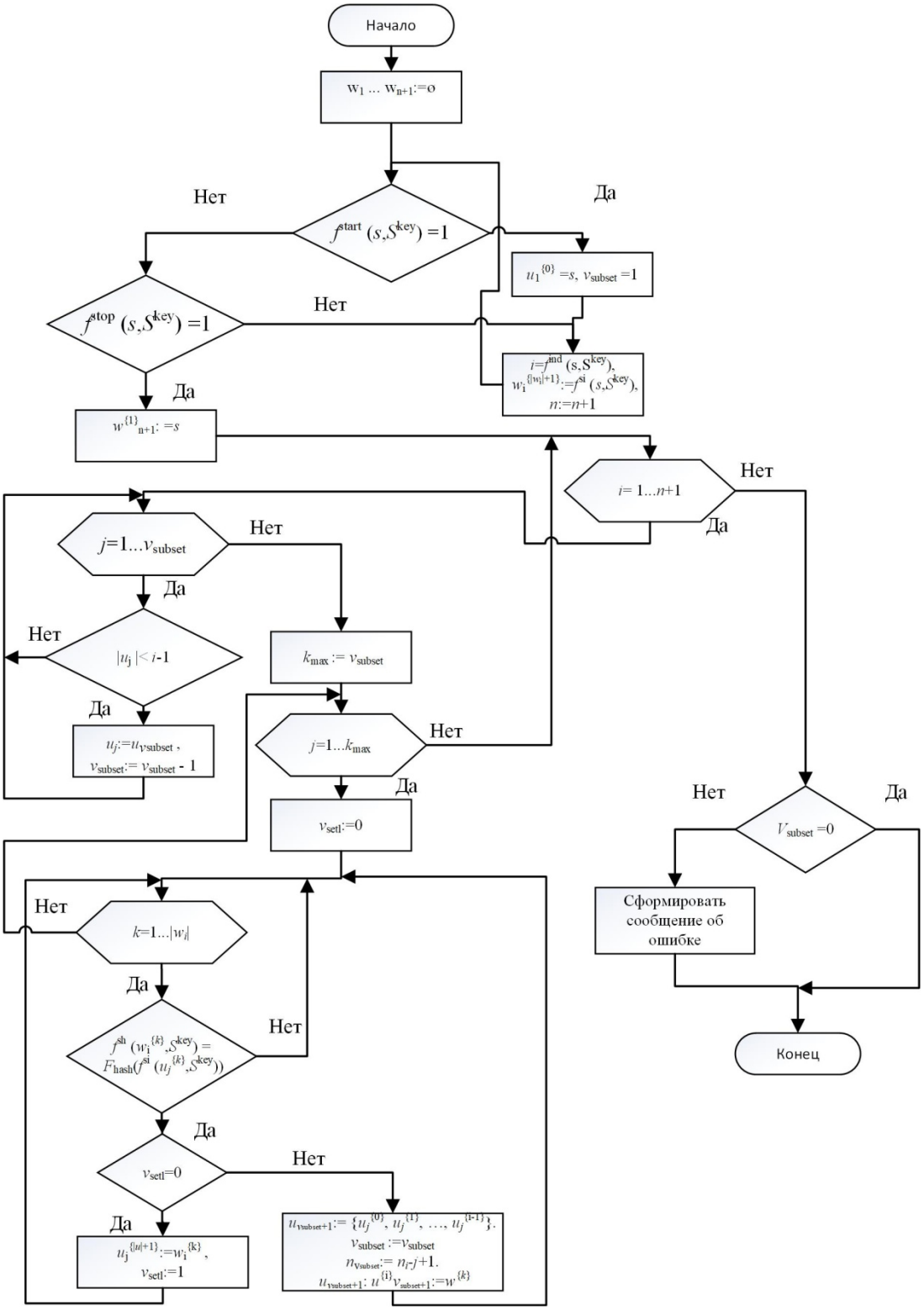

Рисунок 1 – Алгоритм определения источника пакетов данных.

Основные временные затраты при реализации алгоритма будут связаны с выполнением операций формирования хешей пакетов, составляющих подмножества w_1

– w_{n+1}, так как процесс формирования самих подмножеств может быть реализован достаточно просто – путём размещения буферизируемых пакетов в соответствующих областях памяти [17]. При этом количество операций формирования хешей в общем случае будет определяться необходимым для формирования подмножеств $u_1 - u_v$, операций сравнения хешей [18, 19]. Поэтому именно число операций сравнения мы выберем в качестве меры сложности реализации алгоритма определения.

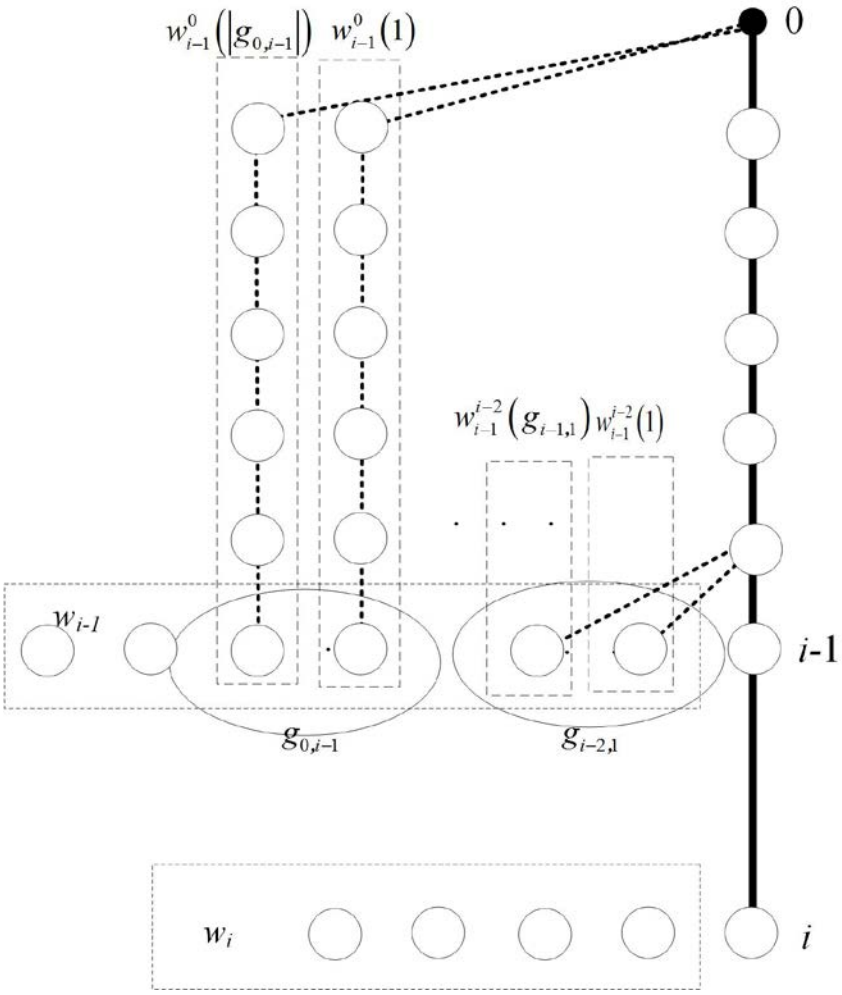

Рисунок 2 – Схема сравнения хешей пакетов.

Сравнения хешей пакетов данных проиллюстрировано на рисунке 2 . Видно, что хеши пакетов подмножества w_i, сравниваются с теми элементами подмножества w_{i-1},

которые включены в побочные ветви $\left\{w_{i-1}^{0}(1)\ldots w_{i-1}^{0}\left(k_{0}^{i-1}\right)\right\}$ – $\left\{w_{i-1}^{i-2}(1)\ldots w_{i-1}^{i-2}\left(k_{i-2}^{i-1}\right)\right\}$ древовидной структуры. Эти ветви отходят от элементов 0… (i–2) подмножества пакетов целевого источника (эта ветвь выделена на рисунке жирной линией) и имеют длину (i–1) … 1 соответственно. Их последние элементы, которые и сравниваются, образуют подмножества $g_{0,i-1}$ – $g_{i-1,1}$. Алгоритм формирования подмножеств подразумевает, что подмножества $\left\{w_{i-1}^{0}(1)\ldots w_{i-1}^{0}\left(k_{0}^{i-1}\right)\right\}$ – $\left\{w_{i-1}^{i-2}(1)\ldots w_{i-1}^{i-2}\left(k_{i-2}^{i-1}\right)\right\}$ могут пересекаться. Оценку числа сравнений будем вести через оценку мощностей подмножеств $g_{0,i-1}$ – $g_{i-1,1}$ или, иными словами, числа таких побочных ветвей. Мерой оценивания будет математическое ожидание данных случайных величин M[$|g_{0,i-1}|$] – M[$|g_{i-1,1}|$].

Пусть от некоторой позиции i = 1 … n цепочки целевого источника сформировалось $|g_{i,j}|$ посторонних ветвей длиной j. Тогда плотность распределения вероятностей случайного числа $h_{i,j}$ различных хешей, сформированных из данных $g_{i,j}$ последних пакетов этих ветвей определится формулой:

$$p^{h}\left(h_{i,j}\right)=\sum_{l=h_{i,j}}^{|U|-n}\left[p^{g}\left(\left|g_{i,j}\right|\right)\times\left(\left(2^{-H}\right)^{j-h_{i}}\prod_{k=1}^{h_{i,j}}\left(1-(k-1)2^{-H}\right)\right)\right]. \qquad (2)$$

где: $p^{g}(|g_{i,j}|)$ – плотность распределения вероятностей мощности множества $g_{i,j}$

H – длина хеша, определяющая вероятность выполнения условия (1)

$|U|$ – мощность множества анализируемых приёмником пакетов

К этим h_i различным хешам в следующую позицию цепочек будет добавлено $|g_{i,j+1}|$ пакетов множества w_{i+1}. Плотность распределения этого числа выводится из вероятности попарного совпадения значения хешей с учётом вырождения биномиального распределения в распределения Пуассона при достаточно большом значении произведения $|g_{i,j+1}| \times |w_{i+1}|$ [20]:

$$p^g\left(\left|g_{i,j+1}\right|\right) = \sum_{l=\left|g_{i,j+1}\right|}^{|U|-n}\left[p^w(l) \times \sum_{h_{i,j}=1}^{|U|-n} p^h\left(h_{i,j}\right) \frac{\left(h_{i,j} \cdot l \cdot 2^{-H}\right)^l \times e^{h_{i,j} \cdot l \cdot 2^{-H}}}{l!} \right], \qquad (3)$$

где $p^w(l)$ – плотность распределения случайного числа $|w_{i+1}|$ – мощности множества w_{i+1}.

С учётом того, что множество пакетов U формируется произвольным числом источников, то считаем, что случайные величины, которыми являются мощности подмножеств w_i, $i = 1 \ldots n$ подчинены распределению Пуассона с интенсивностью $(|U–n|)/n$ [16]:

$$p^w(l) = \frac{\left(\left(|U|-n\right)/n\right)^l \times e^{-\frac{\left(|U|-n\right)}{n}}}{l!} \qquad (4)$$

Рекуррентные выражения (2) и (3) позволяют получить плотность распределения вероятностей чисел $|g_{0,i-1}| - |g_{i-1,1}|$ образуют и выражение для их математических ожиданий:

$$M\left[\left|g_{i,j}\right|\right] = \sum_{k_j^i=0}^{\infty} r \cdot p^g\left(\left|g_{i,j}\right|\right), i = \overline{1 \ldots n}. \qquad (5)$$

Общее число сравнений определится как сумма произведений мощностей множеств w_i , $i = 1 \ldots n$ (с учётом того, что к каждому из них добавляется i–й пакет источника) и мощностей объединений множеств $g_{0,i-1} - g_{i-1,1}$, $i = 1 \ldots n$ (с учётом того, что к каждому результирующему множеству добавляется i–1–й пакет источника):

$$N = \sum_{i=1}^{n} \left[\left(\left| g_{i-1,1} \cap \ldots \cap g_{0,i-1} \right| + 1 \right) \left(\left| w_i \right| + 1 \right) \right]. \quad (6)$$

Математическое ожидание мощности объединения множеств исчисляются, исходя из выражения [21]:

$$M\left[\left| g_{i-1,1} \cap g_{i-2,2} \right| \right] = M\left[\left| g_{i-1,1} \right| \right] + M\left[\left| g_{i-2,2} \right| \right] - M\left[\left| g_{i-1,1} \cup g_{i-2,2} \right| \right]. \quad (7)$$

Так как подмножество $g_{i-1,1} \cup g_{i-2,2}$ образовано элементами, принадлежащими и $g_{i-1,1}$, и $g_{i-2,2}$, вероятность того, что произвольный элемент подмножества w_i принадлежит подмножеству $g_{i-1,1}$ равна отношению $M[|g_{i-1,1}|]/M[|w_i|]$, подмножеству $g_{i-2,2}$ – отношению $M[|g_{i-2,2}|]/M[|w_i|]$, обоим подмножествам – $M[|g_{i-1,1}|] \times M[|g_{i-2,2}|]/(M[|w_i|])^2$. Тогда:

$$M\left[\left| g_{i-1,1} \cap g_{i-2,2} \right| \right] = M\left[\left| g_{i-1,1} \right| \right] + M\left[\left| g_{i-2,2} \right| \right] - \frac{M\left[\left| g_{i-1,1} \right| \right] M\left[\left| g_{i-2,2} \right| \right]}{M\left[\left| w_i \right| \right]}. \quad (8)$$

Применяя формулу (8) последовательно ко всем элементам выражения (6) и исчисляя соответствующие значения мощностей подмножеств, получим итоговое выражение для числа сравнений хеша.

Результаты и их обсуждение

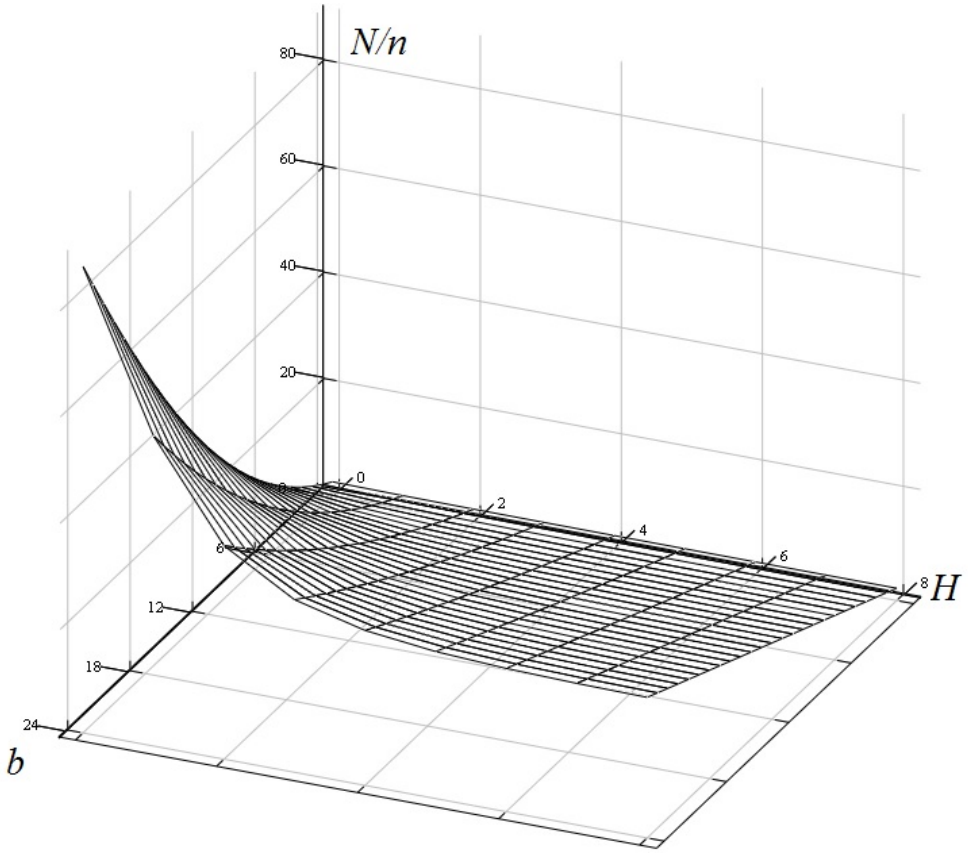

Рисунок 3 – Зависимость N/n от числа источников b и размера хеша H.

Так как количество сравнений хешей пропорционально числу n пакетов в цепочке источника, составляющих фрагментированное сообщение, то интерес представляет не само значение числа сравнений N, а отношение N к n, представленное на рисунке 3 Параметрами выступили длина хеша пакета H и числа источников b, которое определялось как отношение общего числа анализируемых пакетов $|U|$ к числу n пакетов одного источника. Анализ графика показывает, что в диапазоне $b<2^H$ отношение N/n практически линейно зависит от b с коэффициентом 1,5…2.0. Объясняется это тем, что при таком соотношении между параметрами модели мощность множества $g_{i-1,1} \cap \ldots \cap g_{0,i-1}$ незначительна, поэтому основной вклад в число

операций сравнения хешей вносит компонента, которая определяется числом сравнения хешей множества w_i , $i = 1 \ldots n$ с хешем из i–1 – го пакета целевого источника.

Выводы

1. Определены соотношения между числом b взаимодействующих устройств и размером полей служебной информации, при котором трудоёмкость выполнения процедур определения источника имеет сложность $O(b)$, что делает исследуемый метод более предпочтительным по сравнению с известными, имеющими степенную и факториальную сложность, особенно при использовании цепочек пакетов большой длины.

2. Установленная зависимость между трудоёмкостью, числом взаимодействующих устройств и размером полей служебной информации выбирать аппаратную сложность приёмников (количество вычислительных блоков, осуществляющих сравнение хешей) в зависимости от характеристик систем, в которых предполагается их эксплуатация.

3. Результаты исследования трудоёмкости алгоритма позволяют определить целесообразные значения длины цепочки блоков источника и размеры дополнительных служебных полей (индекса пакета в цепочке и хеша) при сформулированных требованиях по длительности полного цикла обработки пакетов данных.

Библиографический список

1. Предварительный национальный стандарт РФ. ПНСТ 354-2019. Информационные технологии. Интернет вещей. Протокол беспроводной передачи данных на основе узкополосной модуляции радиосигнала (NB-Fi). URL: http://docs.cntd.ru/document/1200162760

2. Лихтциндер Б.Я. Киричек Р.Ва., Федотов Е.Д. и др. Беспроводные сенсорные сети. - М.: Горячая линия–Телеком, 2020. – 236 с.

3. Предварительный национальный стандарт РФ. Информационные технологии. Интернет вещей. Протокол обмена для высокоемких сетей с большим радиусом действия и низким энергопотреблением. URL: https://drive.google.com/uc?id=12kPw5_ndO8zav7_BP_Kdytu7uEyy3x&export=download

4. 802.15.4-2015. IEEE Standard for Low-Rate Wireless Personal Area Networks, IEEE Computer Society, 2016. URL: https://standards.ieee.org/standard/802_15_4-2015.html

5. Domin K. et al. Security analysis of the drone communication protocol: Fuzzing the MAVLink protocol, Engineering Secure Software and Systems, 2016, pp. 198 - 204.

6. Спеваков А.Г., Калуцкий И.В. Устройство формирования уникальной последовательности, используемой при обезличивании персональных данных // Труды МАИ. 2020. № 115. URL: http://trudymai.ru/published.php?ID=119939. DOI: 10.34759/trd-2020-115-13

7. Panagiotis Papadimitratos, Zygmunt J. Haas Secure message transmission in mobile ad hoc networks // Ad Hoc Networks, 2003, no. 1, pp. 193 – 209. URL: https://doi.org/10.1016/S1570-8705(03)00018-0

8. Othman S.B., Alzaid H., Trad A., Youssef H. An efficient secure data aggregation scheme for wireless sensor networks // IEEE, Piraeus, Greece, 2013. DOI:10.1109/iisa.2013.6623701

9. 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: http://trudymai.ru/published.php?ID=118998. DOI: 10.34759/trd-2020-114-13

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

11. Васильков Ю.В., Тимошенко А.В., Советов В.А., Кирмель А.С. Методика оценки функциональных характеристик систем радиомониторинга при ограниченных данных о параметрах надежности // Труды МАИ. 2019. № 108. URL: http://trudymai.ru/published.php?ID=109557. DOI: 10.34759/trd-2019-108-16

12. Yağdereli E., Gemci C. A study on cyber-security of autonomous and unmanned vehicles // Journal of Defense Modeling and Simulation, 2015. DOI: https://doi.org/10.1177/1548512915575803

13. Беспилотные авиационные системы. Часть 3. Эксплуатационные процедуры Стандарт ISO 21384-3:2019 (E). URL: https://cdn.standards.iteh.ai/samples/70853/7ec34c8a22bf46958423b7e3a2e43693/ISO-21384-3-2019.pdf

14. Leccadito M. A Hierarchical Architectural Framework for Securing Unmanned Aerial Systems, Virginia Commonwealth University, 2016, URL: https://doi.org/10.25772/0DK3-E418

15. 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: http://trudymai.ru/published.php?ID=119007. DOI: 10.34759/trd-2020-114-15

16. Таныгин М.О. Теоретические основы идентификации источников информации, передаваемой блоками ограниченного размера: монография. - Курск: Изд-во Университетская книга, 2020. - 198 с.

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

18. Iwata T., Kurosawa K. OMAC: one-key CBC MAC // Conference Fast Software Encryption, 2003, pp. 129 – 153. DOI: 10.1007/978-3-540-39887-5_11

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

20. Корн Г., Корн Т. Справочник по математике для научных работников и инженеров. - М.: Наука, 1978. – 832 с.

21. Хаусдорф Ф. Теория множеств. – М.: Издательство ЛКИ, 2015. –304 с.

Complexity of algorithm for data source determining

Tanygin M.O.*, Alshaea H.Y., Mitrofanov A.V.*****

South-Western State University,

94, 50-let Oktyabrya str., Kursk, 305040, Russia

**e-mail: tanygin@yandex.ru*

***e-mail: haideryhy7@gmail.com*

****e-mail: mitro3000@rambler.ru*

Abstract

The article deals with the problem of complexity assessing of the procedures for determining the incoming information blocks source. The algorithm for processing the blocks analyzed by the receiver, implementing the data source identifying method, is described. The method is based on incoming blocks unification on the receiver side into the structured sets, and checking for these blocks certain logic values, being computed on the assumption of these blocks content and certain a priori information, known to both the source and receiver. The blocks, incoming to the receiver, are being buffered and then unified into the structured intersected sets. This sets form a tree-type structure in the receiver memory. Analyzing this structure, the receiver determines that structured set, which was formed by the target source.

The article shows how the number of these sets, being formed, affects the incoming blocks analyzing complexity. A mathematical model for assessing typical operations, executed by the receiver while the incoming blocks checking and their appending to the corresponding side branches of the tree structure, was developed based on the theory of probability.

Functional dependencies between the probability of the side branches of the tree structure forming and their length and parameters, used while organizing interaction between the source and the receive were determined.

Mathematical expectation of the number of operations executed by the receiver to analyze the contents of the information blocks service fields was estimated, based on the obtained probability estimates. The dependencies between the characteristics of the information systems, in which the considered identification method is implemented, the service information fields size and the number of elementary operations were determined. Based on the obtained results, the space of receiver operating parameters was partitioned into the ranges, in which the dependence of algorithmic complexity on the number of data sources can be approximated by various functions. The range where complexity increases linearly with the number of interacted elements of the information system growth was determined as operating range. This makes the studied method more preferable compared to the known ones with power and factorial complexity, especially when identifying the sets of large the data blocks.

Keywords: data processing, message receiver, algorithm complexity, performance, mathematical modeling.

References

1. *Predvaritel'nyi natsional'nyi standart RF. PNST 354-2019. Informatsionnye tekhnologii. Internet veshchei. Protokol besprovodnoi peredachi dannykh na osnove uzkopolosnoi*

modulyatsii radiosignala (NB-Fi) ((PNST 354-2019. Preliminary national standard of the Russian Federation. Information Technology. Internet of Things. Wireless data transmission protocol based on narrowband radio signal modulation (NB-Fi)). URL: http://docs.cntd.ru/document/1200162760

2. Likhttsinder B.Ya. Kirichek R.Va., Fedotov E.D. et al. *Besprovodnye sensornye seti* (Wireless sensor networks), Moscow, Goryachaya liniya–Telekom, 2020, 236 p.

3. *Predvaritel'nyi natsional'nyi standart RF. Informatsionnye tekhnologii. Internet veshchei. Protokol obmena dlya vysokoemkikh setei s bol'shim radiusom deistviya i nizkim energopotrebleniem* (Preliminary national standard of the Russian Federation. Information Technology. Internet of Things. An exchange protocol for high-capacity networks with a long range and low energy consumption). URL: https://drive.google.com/uc?id=12kPw5_ndO8zav7_BP_Kdytu7uEyy3x&export=download

4. 802.15.4-2015. IEEE Standard for Low-Rate Wireless Personal Area Networks, *IEEE Computer Society*, 2016. URL: https://standards.ieee.org/standard/802_15_4-2015.html

5. Domin K. et al. *Security analysis of the drone communication protocol: Fuzzing the MAVLink protocol*, Engineering Secure Software and Systems, 2016, pp. 198 – 204.

6. Spevakov A.G., Kalutskii I.V. *Trudy MAI*, 2020, no. 115. URL: http://trudymai.ru/eng/published.php?ID=119939. DOI: 10.34759/trd-2020-115-13

7. Panagiotis Papadimitratos, Zygmunt J. Haas Secure message transmission in mobile ad hoc networks, *Ad Hoc Networks*, 2003, no. 1, pp. 193 – 209. URL: https://doi.org/10.1016/S1570-8705(03)00018-0

8. Othman S.B., Alzaid H., Trad A., Youssef H. An efficient secure data aggregation scheme for wireless sensor networks, *IEEE*, Piraeus, Greece, 2013. DOI: 10.1109/iisa.2013.6623701

9. Borzov D.B., Dyubryuks S.A., Sokolova Yu.V. *Trudy MAI*, 2020, no. 114. URL: http://trudymai.ru/eng/published.php?ID=118998. DOI: 10.34759/trd-2020-114-13

10. Mytsko E.A., Mal'chukov A.N., Ivanov S.D. *Pribory i sistemy. Upravlenie, kontrol', diagnostika*, 2018, no. 6, pp. 22 - 29.

11. Vasil'kov Yu.V., Timoshenko A.V., Sovetov V.A., Kirmel' A.S. *Trudy MAI*, 2019, no. 108. URL: http://trudymai.ru/eng/published.php?ID=109557. DOI: 10.34759/trd-2019-108-16

12. Yağdereli E., Gemci C. A study on cyber-security of autonomous and unmanned vehicles, *Journal of Defense Modeling and Simulation*, 2015. DOI: https://doi.org/10.1177/1548512915575803

13. *Bespilotnye aviatsionnye sistemy. Chast' 3. Ekspluatatsionnye protsedury Standart ISO 21384-3:2019 (E)*. URL: https://cdn.standards.iteh.ai/samples/70853/7ec34c8a22bf46958423b7e3a2e43693/ISO-21384-3-2019.pdf

14. Leccadito M. *A Hierarchical Architectural Framework for Securing Unmanned Aerial Systems*, Virginia Commonwealth University, 2016, URL: https://doi.org/10.25772/0DK3-E418

15. Tanygin M.O., Alshaia Kh.Ya., Dobritsa V.P. *Trudy MAI*, 2020, no. 114. URL: http://trudymai.ru/eng/published.php?ID=119007. DOI: 10.34759/trd-2020-114-15

16. Tanygin M.O. *Teoreticheskie osnovy identifikatsii istochnikov informatsii, peredavaemoi blokami ogranichennogo razmera* (Theoretical foundations of sources identification of

information transmitted by blocks of limited size), Kursk, Izd-vo Universitetskaya kniga, 2020, 198 p.

17. Tanygin M.O., Alshaia Kh.Ya., Altukhova V.A., Marukhlenko A.L. *Izvestiya Yugo-Zapadnogo gosudarstvennogo universiteta. Seriya: Upravlenie, vychislitel'naya tekhnika, informatika. Meditsinskoe priborostroenie*, 2018, vol. 8, no. 4 (29), pp. 63 - 71.

18. Iwata T., Kurosawa K. OMAC: one-key CBC MAC, *Conference Fast Software Encryption*, 2003, pp. 129 - 153. DOI: 10.1007/978-3-540-39887-5_11

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

20. Korn G., Korn T. *Spravochnik po matematike dlya nauchnykh rabotnikov i inzhenerov* (Handbook of mathematics for scientists and engineers), Moscow, Nauka, 1978, 832 p.

21. Khausdorf F. *Teoriya mnozhestv* (Theory of sets), Moscow, Izdatel'stvo LKI, 2015, 304 p.