УДК 004.052 **DOI:** 10.34759/trd-2021-118-14

Метод ограничения множества обрабатываемых приёмником блоков данных для повышения достоверности операций определения их источника

Таныгин М.О.*, Добросердов О.Г., Власова А.О***.,**
Ахмад Али Айед Ахмад****
Юго-Западный государственный университет, ЮЗГУ,
ул. 50 лет Октября, 94, Курск, 305040, Россия
**e-mail: tanygin@yandex.ru*
***e-mail: serfingk@yandex.ru*
****e-mail: anononanav@gmail.com*
*****e-mail: aliayid2013@gmail.com*

Статья поступила 27.04.2021

Аннотация

Цель исследования состоит в разработке метода, алгоритма и моделей повышения достоверности идентификации источника информационных пакетов. Указанная цель достигается путём дополнительной проверки содержимого специального служебного слова, входящего в состав пакета данных, на попадание в динамически формируемый приёмником диапазон значений. В результате снижается число пакетов, которые анализируются приёмником при идентификации источника структурированного множества информационных пакетов. Показано, что уменьшение числа анализируемых пакетов ведёт к снижению вероятности возникновения ошибок идентификации. На основе аппарата цепей Маркова разработаны модели оценки

достоверности идентификации. Процесс получения приёмником информационных пакетов от различных источников представлен как случайный процесс, в котором часть состояний соответствуют возникновению ошибки обработки данных, а часть – возможности достоверной обработки пакетов. В качестве параметров модели выступили: ширина диапазона значений, используемых для проверки содержимого специального служебного слова пакета данных, вероятность включения одиночного блока данных в структурированное множество, длина структурированного множества пакетов данных от единичного источника, общее число обрабатываемых приёмником пакетов данных. Полученные в результате моделирования значения вероятности ошибки позволили сформировать целесообразные параметры алгоритмов обработки поступающих в приёмник информационных пакетов. Показано, что использование метода ограничения множества анализируемых пакетов позволяет повысить достоверность идентификации субъектов распределённых информационных систем, которые обмениваются пакетами данных ограниченного размера. При этом вероятность ошибочной идентификации источника, сформировавшего некоторое структурированное множество пакетов снижается в 2 – 3 раза. В практическом плане это позволяет снизить размер дополнительных служебных полей в каждом пакете данных, что позволит снизить информационную избыточность обрабатываемых данных, повысить скорость обработки данных приёмником, снизить размеры внутренней регистровой и оперативной памяти приёмника.

Ключевые слова: цепи Маркова, математическое моделирование, приёмник сообщений, информационные пакеты, идентификация.

Введение

Разделение информационных потоков от множества источников является обязательной задачей, выполняемой современными устройствами, функционирующими в составе распределённых информационных систем [1 – 5]. Если в рассматриваемых системах информационный поток представлен совокупностью отдельных блоков данных, то основным решением для указанного выше разделения является исчисление в приёмнике на основании данных каждого блока и некоторой дополнительной информации в нём числовой характеристики и сравнении её с некоторым набором значений, характеризующих соответствующий информационный поток [1 – 4]. Основным недостатком таких методов является недостаточная достоверность разделения информационных потоков при ограниченном размере полей дополнительной служебной информации в каждом таком блоке [5 - 6]. Для повышения достоверности является представление информационного потока не в виде совокупности отдельных информационных блоков, а в виде совокупности множеств таких блоков. При этом числовая характеристика, используемая для разделения информационных потоков, вычисляется для таких множеств [7 – 9]. В таком классе систем, обеспечивающих более высокую достоверность разделения при одинаковом размере дополнительных служебных полей, более актуальна проблема снижения

скорости выполнения операций проверки данных [10, 11]. Последнее обстоятельство чрезвычайно актуально для автономных систем с высокими требованиям по скорости отработки управляющих воздействий и жёсткими требованиями по энергопотреблению и массо-габаритным характеристикам вычислительного блока, например, в современных беспилотных летающих аппаратах [12, 14]. Так как достоверность выполнения процедур разделения информационного потока, а так же скорость их выполнения находятся в зависимости от числа обрабатываемых приёмником блоков данных, то очевидным решением, обеспечивающим повышение достоверности определения источника данных, является логическое ограничение числа таких блоков. Такое ограничение должно исходить из условия неизменности во времени некоторых характеристик информационного потока от конкретного источника в приёмник, которые можно считать априорными. Целью работы является повышение достоверности процедур определения источника блоков данных за счёт применения правила, ограничивающего мощность анализируемых приёмником блоков данных.

Формулировка задачи

Формальное описание решаемой задачи выглядит следующим образом. Приёмник осуществляет приём некоторого структурированного множества $X = \{x_1,\ldots x_n\}$ блоков данных от источника данных. В общем случае очерёдность доставки блоков при передаче не сохраняется. Под структурированным мы понимаем такое множество, в котором важен порядок элементов его составляющих. Иными

словами, приёмник получает фрагментированное на n частей сообщение от источника. В течение сеанса обмена данными в приёмник поступает некоторое множество блоков данных $O = \{o_1,\ldots o_{N-n}\}$, сформированных другими источниками, то есть являющимися посторонними относительно данной конкретной пары «источник – приёмник». Вместе оба этих множества образуют множества U обрабатываемых приёмником блоков данных, мощностью N:

$$U = X \cup O, X \cap O = \varnothing, |U| = N \qquad (1)$$

Каждый блок множества X кодирован таким образом, чтобы приёмник в результате выполнения декодирования и предобработки выделяет из множества U множество X. Существует большое число алгоритмов группового кодирования, так называемых CBC шифры [7, 14 – 17], которые, в случае ограниченного размера самих блоков данных, размера полей дополнительной атрибутивной информации в них обеспечивают требуемую достоверность выполнения такой операции. Формально это можно записать в виде:

$$\begin{aligned} &\exists ! X \subset U, |X| = n, \quad \boldsymbol{B}\left(X, S^{\text{key}}\right) = 1, \\ &\forall Y \subset U, Y \neq X, |Y| = n, \quad \boldsymbol{B}\left(Y, S^{\text{key}}\right) = 0, \end{aligned} \qquad (2)$$

где $\boldsymbol{B}$ – некоторое решающее правило, применяемое к различным подмножествам мощностью n множества U , принимающее значения истина для подмножества X, в качестве одного из параметров которого выступает некоторая идентификационная последовательность S^{key}.

В работе [18] подробно рассмотрена модели возникновения ошибок определения источника, в основе которых лежит формирование приёмником, помимо множества X ещё одного подмножества $Y \neq X$, для которого $\boldsymbol{B}(Y, S^{key}) = 1$. В таком случае установить, какое из двух множеств блоков сформировано источником, не представляется возможным. В той же работе показано, что в рамках той постановки задачи, которая описана выше, вероятность $P_e(U) = f(n,|U|,H)$ возникновения подобных ошибок есть функция числа анализируемых блоков N, некоторого параметра H, определяющего вероятность вхождения одного элемента множества U на конкретную позицию формируемого множества X . В качестве такого в алгоритмах [14, 17] выступал размер поля информационного блока, в котором размещалось значение хеша, сформированного из данных предыдущих блоков (предыдущего блока).

Функция P_e является монотонно возрастающей от 0 до 1 функция на всей области определения. Поэтому для повышения достоверности выполнения источника при формировании множества X можно формировать его не из всех блоков, поступивших в приёмник, а только из их части, образующей некоторое множество $U' \subset U$, $|U'|<|U|$. Для этого необходимо сформулировать некоторое ограничивающее правило.

Так как при практической реализации множество анализируемых блоков данных на этапе предобработки буферизируется во внутренней памяти приёмника, то можно выделить то, как предложено в [19], множество его можно разделить на n непересекающихся подмножеств $w_1 - w_n$, в состав каждого из которых входит лишь

один блок целевого источника и произвольное число посторонних блоков из множества $O = U/X$. Схематично их размещение в буфере можно представить в виде некоторой матрицы, строки которой образованы подмножествами $w_1 - w_n$, а число столбцов равно некоторой величине M, характеризующей буфер приёмника (рис 1).

w_1	x	o	o			
w_2	o	x	o			
w_3	x		x	o		
w_4	x	o		o		
			----			
w_n	x	o	x		o	

Рисунок 1 – Размещение блоков данных в буфере приёмника

Описание метода повышения достоверности обработки блоков

В качестве теоретической основы для синтеза правила, ограничивающего мощность множества U' буферизируемых приёмником блоков данных, выступает такая априорная характеристика информационного потока от источника к приёмнику, как порядок формирования и выдачи блоков данных, образующих фрагментированное сообщение длиной n. Так как они формируются и передаются последовательно от 1-го до n-го, то можно предположить невозможность некоторых вариантов очерёдности поступления блоков в приёмник. Например, первый блок может поступить после второго, но не может поступать после третьего.

Формализуем правило буферизации блоков данных в приёмнике, которое позволит сформировать меньшее по мощности множество анализируемых блоков данных U'. Для каждого блока определяется его принадлежность к одному из

подмножеств $w_1 - w_n$. В основе этой операции лежит операция декодирования содержимого блока данных [17] и выделения из него порядкового номера (индекса) i во фрагментированном сообщении: $f^{\text{ind}}\left(s, S^{\text{key}}\right) = i \Rightarrow s \in w_i$, где: f^{ind} – операция декодирования содержимого поля индекса блока,

Рассмотрим произвольный момент времени на этапе передачи фрагментированного сообщения в приник. Примем за W_{forw} – ширину окна опережения – максимальное число, на какое индекс поступающего информационного блока может превышать максимальный индекс блоков M_{max} , уже буферизированных к текущему моменту, чтобы быть записанным в буфер. Данный показатель может варьироваться в диапазоне от 1 до n. Если поступающий информационный блок имеет индекс, превышающий $M_{\text{max}} + W_{\text{forw}}$, то данный блок игнорируется и не записывается в буфер. При этом равенство параметра W_{forw} единице будет означать невозможность для легальных информационных блоков менять очерёдность поступления в приёмник, так как в этом случае разница между индексами легальных информационных блоков, поступающих подряд в приёмник, может иметь значение от 2 и более. Это увеличивает вероятность ошибки при передаче всей цепочки блоков и накладывает высокие требования к протоколу связи, обеспечивающую их транспортировки от источника в приёмник: он должен гарантировать доставку блоков в исходном порядке. Всё это потребует от системы связи буферизации, контроля очерёдности и выльется, в конечном счете, в снижение пропускной способности канала.

Ширина окна запаздывания W_{back} – параметр, определяющий, на какое максимальное число индекс поступающего информационного блока быть меньше максимального индекса блоков, уже буферизированных к текущему моменту, чтобы быть записанным в буфер. Так же как и предыдущий параметр, может принимать значения 1 до W_{chain} .

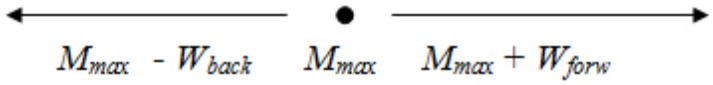


Рисунок 2 – Диапазон значений индексов, при которых запись блока в буфер возможна

Представим процесс получения информационных блоков в виде марковского процесса с непрерывным временем. За единицу условного времени выберем время получения множества X легальных блоков мощностью n. Тогда интенсивность получения приёмником легальных блоков будет $P_{legal} = n$

Вместе с легальными блоками в приёмник поступают и посторонние из множества O. В качестве параметра моделирования выберем число M_{false} – число посторонних блоков, поступающих в приёмник в единицу условного времени. Интенсивность записи постороннего блока на конкретный ярус определится как: $P_{false} = M_{false} / n$

Здесь мы исходили из предположения, что любой посторонний блок может быть записан в буфер на какой-либо ярус, из-за особенностей алгоритма формирования

содержимого информационных блоков вероятность генерации постороннего блока с определённым индексом крайне мала, соответственно, вероятность на любой ярус блок, поступивший в приёмник, запишется с одинаковой вероятностью $1/M_{\text{false}}$ [20].

Граф, описывающий марковский процесс получения информационных блоков приведён на рисунке 3. Так как моделируемая ситуация не предполагает изменения порядка следования легальных информационных блоков, то ширина окна опережения W_{forw} принята равной 1, а все информационные блоки с индексом большим $M_{\max}+1$ игнорируются приёмником. Состояние $S_{i,j}$ соответствует записи в буфер i легальных блоков (максимальный номер записанного легального блока будет равен i) и неопределённого числа нелегальных блоков, при котором максимальный индекс $M_{\max}$ записанных блоков равен j. Состояния $S_{i,j}$ когда $i < j$ недопустимы. Переход из состояния $S_{i,j}$ возможен только в состояния $S_{i,j+1}$ – запись в буфер постороннего блока с индексом $M_{\max}+1$, и в стояние $S_{i+1,\max(i+1,j+1)}$ – запись в буфер легального блока [21].

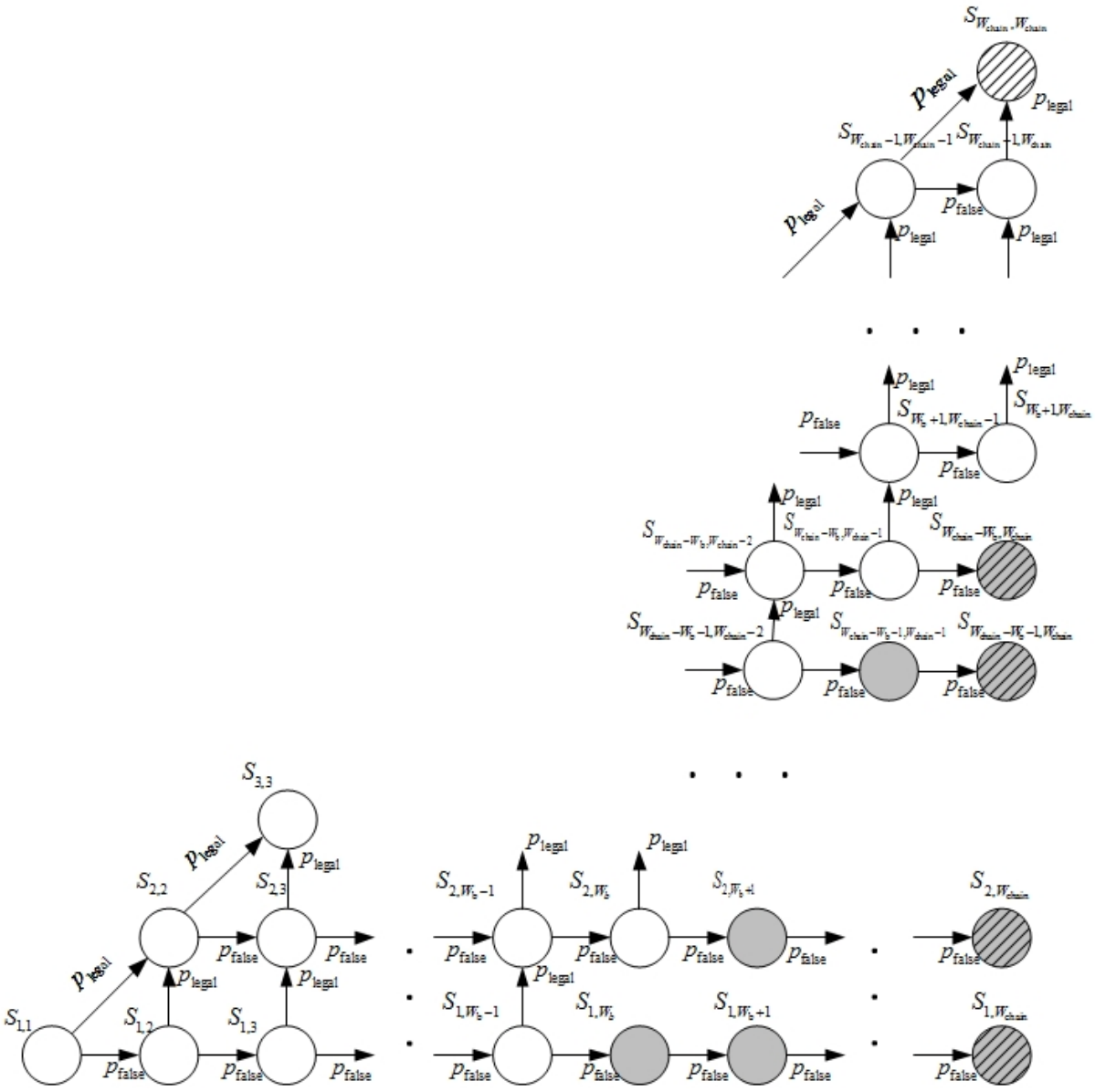


Рисунок 3 – Граф марковского процесса, моделирующего заполнение буфера

Состояния графа, выделенные серым цветом, соответствуют достижению разницы между максимальным индексом легального блока и максимальным индексом записанного в буфер постороннего блока значения W_{back}. После этого запись в буфер легальных блоков становится невозможна из-за непопадания их индексов в окно индексов, разрешённых для записи в буфер. Это соответствует отсутствию перехода

между состояниями $S_{i,j}$ и $S_{i+1,\max(i+1,j+1)}$ при $j-i \geq W_{\text{back}}$. В таком случае передача цепочки блоков считается завершённой с ошибкой. У цепи Маркова есть поглощающие состояния, выделенные штриховкой: $S_{W_{\text{chain}},W_{\text{chain}}}$ – передача блоков завершилась успешно, и $S_{1,W_{\text{chain}}} - S_{W_{\text{chain}}-W_{\text{back}},W_{\text{chain}}}$ – буфер был заполнен посторонними блоками. Система уравнений Колмогорова, описывающих данный граф выглядит следующим образом:

$$\begin{cases} \dfrac{dP_{S_{i,i}}(t)}{dt} = -\left(p_{\text{legal}} + p_{\text{falce}}\right)P_{S_{i,i}}(t) + p_{\text{legal}}\left(P_{S_{i-1,i-1}}(t) + P_{S_{i-1,i}}(t)\right), \quad i = \overline{2 \ldots W_{\text{chain}} - 1} \\ \dfrac{dP_{S_{1,1}}(t)}{dt} = -\left(p_{\text{legal}} + p_{\text{falce}}\right)P_{S_{1,1}}(t), \\ \dfrac{dP_{S_{W_{\text{chain}},W_{\text{chain}}}}(t)}{dt} = p_{\text{legal}}\left(P_{S_{W_{\text{chain}}-1,W_{\text{chain}}-1}}(t) + P_{S_{W_{\text{chain}}-1,W_{\text{chain}}}}(t)\right), \\ \dfrac{dP_{S_{i,j}}(t)}{dt} = -p_{\text{falce}}P_{S_{i,j}}(t) + p_{\text{false}}P_{S_{i,j-1}}(t), \quad i = \overline{2 \ldots W_{\text{chain}} - 1},\ j = \overline{i+1 \ldots W_{\text{chain}} - 1}, \\ \dfrac{dP_{S_{i,W_{\text{chain}}}}(t)}{dt} = p_{\text{false}}P_{S_{i,W_{\text{chain}}-1}}(t), \quad i = \overline{1 \ldots W_{\text{back}}}, \end{cases} \qquad 3)$$

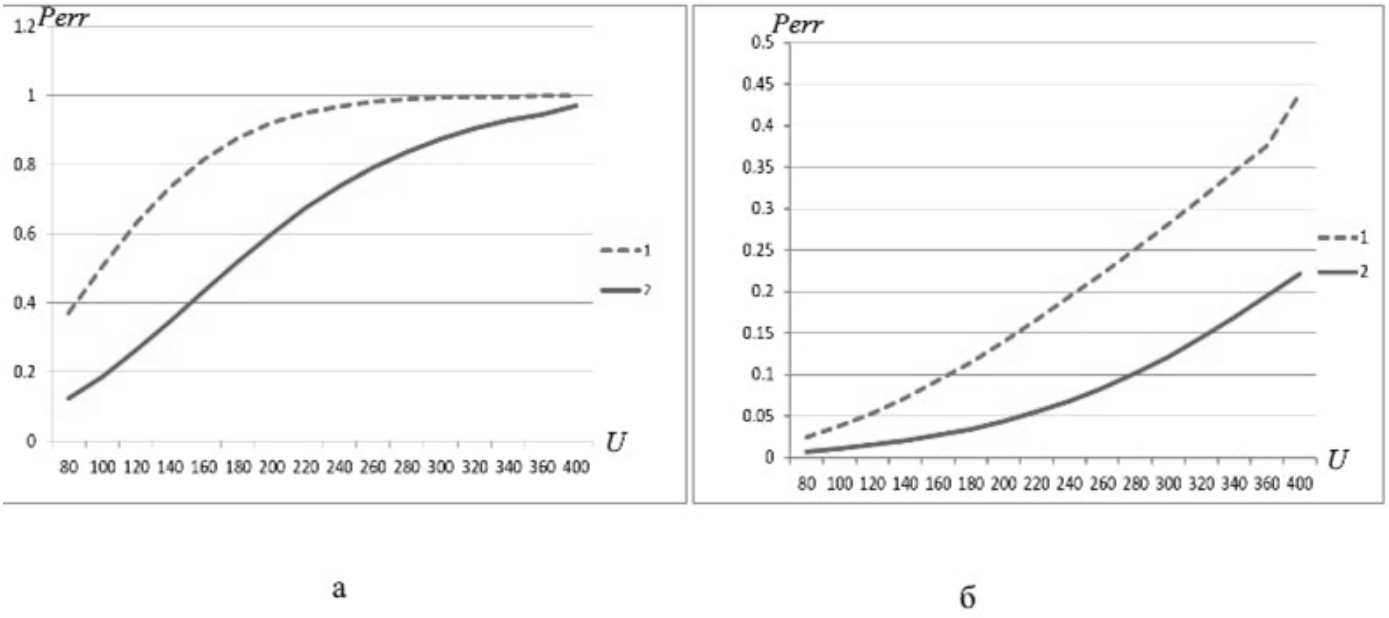
где $P_{S_{i,j}}(t)$ – вероятность нахождения моделируемой системы в состоянии $S_{i,j}$ от времени.

Решение данной системы уравнений позволяет определить вероятность попадания системы в стояние $S_{W_{\text{chain}},W_{\text{chain}}}$ через достаточно большой промежуток времени при различных значениях параметров модели: W_{back}, n, $|U'|$. Это является вероятностью $P_{\text{err1}} = f(n, |U'|, W_{\text{back}})$ возникновения ошибки буферизации блоков, при которой блоки от целевого источника были проигнорированы. Зная зависимость $P_{\text{e}}(U')$, с учётом того,

что $|U'| = |U| \cdot n / W_{back}$ можем получить общую вероятность ошибки определения источника информационных блоков:

$$P_{err} = 1 - (1 - P_{err1}(n, |U| \cdot n / W_{back}, W_{back}))(1 - P_e(|U| \cdot n / W_{back})) \quad (4)$$

Графики зависимости вероятности ошибочного разделения информационных потоков приёмником с применением метода ограничения числа анализируемых блоков и без него приведены на рисунке 3. Что вероятность ошибки в некоторых диапазонах значения $|U|$ снижается в 2 – 3 раза по сравнению с рассмотренными в [18] методами



а б

Рис 4 – Графики зависимости вероятности ошибки определения P_{err} источника от мощности множества U при а) n = 10, б) n=14,

1 – без применения метода ограничения числа блоков,

2 – с применением метода ограничения числа блоков

Выводы

Проведённое исследование метода ограничения числа анализируемых блоков данных показало, что использование неизменных во времени характеристик информационного потока между источником и приёмником, например, гарантированность очерёдности доставки блоков данных, позволяет существенно повысить достоверность процедур разделения информационных потоков от разных источников. В рабочих диапазонах параметров работы приёмника вероятность ошибки снижается с 0.4 – 0.7 до 0.15 – 0.25. В практическом плане это выражается в снижении количества информации, которую вынужден передать источник в результате переспросов после обнаружения ошибки, что повышает скорость отработки команд приёмником, повышает достоверность и оперативность реализуемых рассматриваемым классом информационных систем процедур управления. Кроме того, использование метода позволяет без увеличения вычислительных затрат, осуществлять обработку в приёмнике большего (до трёх раз) числа информационных блоков от большего числа источником при сохранении требуемой протоколом передачи достоверности обработки данных.

Библиографический список

1. Бухарин В.В., Дворядкин В.В., Пикалов Е.Д. и др. Способ и устройство управления потоками данных распределенной информационной системы. Патент RU 2547628 C2, 10.04.2015.

2. Бухарин В.В., Казачкин А.В., Карайчев С.Ю. и др. Способ и устройство управления потоками данных распределенной информационной системы с использованием идентификаторов. Патент RU 2710284 C1, 25.12.2019.

3. Горохов Алексей, Кхандекар Аамод, Борран Мохаммад Д., Пракаш Раджат. Способы и системы для сокращения непроизводительных затрат для обработки для пакетов канала управления. Патент RU 2419219 C2, 20.05.2011.

4. 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=11993. DOI: 10.34759/trd-2020-115-13.

5. Предварительный национальный стандарт РФ. Информационные технологии. Интернет вещей. Протокол обмена для высокоемких сетей с большим радиусом действия и низким энергопотреблением. URL: http://docs.cntd.ru/document/554596382

6. 802.15.4-2015. IEEE Standard for Low-Rate Wireless Personal Area Networks // IEEE Computer Society. DOI: 10.1109/ieeestd.2016.7460875.

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

8. Stallings W. NIST Block Cipher Modes of Operation for Confidentiality // Cryptologia, 2010, no. 34 (2), pp. 163 – 175. DOI:10.1080/01611190903185401

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. Xie J., Pan X. An improved rc4 stream cipher // International Conference on Computer Application and System Modeling, 2010. DOI: 10.1109/IC-CASM.2010.5620800

12. Allouch A., Cheikhrouhou O., Koubaa A. MAVSec: Securing the MAVLink Protocol for Ardupilot/PX4 Unmanned Aerial Systems // International Wireless Communications and Mobile Computing Conference (IWCMC), Morrocco, 2019. DOI: 10.1109/IWCMC.2019.8766667

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. Zhao J., Cheng D., Hao Ch. An Improved Ant Colony Algorithm for Solving the Path Planning Problem of the Omnidirectional Mobile Vehicle // Mathematical Problems in Engineering, 2016, no. 12. DOI: 10.1155/2016/7672839

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

16. Liu C., Ji J., Liu Z. Implementation of DES Encryption Arithmetic based on FPGA // AASRI Procedia, 2013, vol. 5, pp. 209 - 213. DOI: 10.1016/j.aasri.2013.10.080

17. Таныгин М.О., Алшаиа Х.Я Исследование свойств алгоритмов формирования защищенных сообщений // Телекоммуникации. 2020. № 1. С. 2 - 9.

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

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

20. Денисенко Т.И. Использование марковских цепей при решении различных прикладных задач // Фундаментальные исследования. 2009. № 1. С. 27 – 28.

21. Наумов В.А., Самуйлов К.Е., Гайдамака Ю.В. Мультипликативные решения конечных цепей Маркова: монография. – М.: РУДН, 2015. - 159 с.

A method for limiting data blocks set being processed by the receiver to increase their source detection operations reliability

Tanygin M.O., Dobroserdov O.G., Vlasova A.O., Ahmad Ali A.A.

South-Western State University, 94, 50-let Oktyabrya str., Kursk, 305040, Russia

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

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

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

*****e-mail: aliayid2013@gmail.com*

Abstract

The purpose of the study consists in developing a method, algorithm and models of authenticity enhancing of the information packets source identification. This goal is achieved by extra checking the content of a special service word that is a part of the data packet for falling into the value range dynamically generated by the receiver. As the result, the number of packets, being analyzed by the receiver while identifying the source of the structured set of information packets, reduces. The article demonstrates that reduction of the number of packets being analyzed leads to the probability of identification errors origin reduction. Models for identification authenticity evaluation were developed based Markov chains apparatus. The process of information packs acceptance by the receiver from various sources is presented as a random process, in which a part of the states corresponds to the data packets processing errors occurrence, while the other part corresponds to the possibility of the reliable packets processing. The model parameters are the values range width, used for checking the data packet special word; the probability of a single data block inclusion into the structured

set; the length of the structured set of data packets from the single source; the total number of data packets being processed by the receiver. The article shows that application of the method of limiting the analyzed packets set being analyzed allows enhancing identification reliability of the distributed information systems subjects, which exchange data packets of limited size. The probability of identification herewith of false source, which formed a certain structured set of packets, reduces by two or three times. In practical terms, it allows reducing the size of extra service margins in each data packet. This, in its turn, allows reducing information excessiveness of the processed data, increasing the data processing speed by the receiver, and reducing the size of both internal register memory and random-access memory of the receiver.

Keywords: Markov chain, mathematical modeling, messages receiver, network packet, identification.

References

1. Bukharin V.V., Dvoryadkin V.V., Pikalov E.D. et al. *Patent RU 2547628 S2*, 10.04.2015.

2. Bukharin V.V., Kazachkin A.V., Karaichev S.Yu. et al. *Patent RU 2710284 C1*, 25.12.2019.

3. Gorokhov Aleksei, Kkhandekar Aamod, Borran Mokhammad D., Prakash Radzhat. *Patent RU 2419219 S2*, 20.05.2011.

4. Spevakov A.G., Kalutskii I.V. *Trudy MAI*, 2020, no. 115. URL: http://trudymai.ru/eng/published.php?ID=11993. DOI: 10.34759/trd-2020-115-13

5. *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. Exchange protocol for high-capacity networks with a long range and low power consumption). URL: http://docs.cntd.ru/document/554596382

6. 802.15.4-2015. IEEE Standard for Low-Rate Wireless Personal Area Networks, *IEEE Computer Society*. DOI: 10.1109/ieeestd.2016.7460875

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

8. Stallings W. NIST Block Cipher Modes of Operation for Confidentiality, *Cryptologia*, 2010, no. 34 (2), pp. 163 – 175. DOI: 10.1080/01611190903185401

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. Xie J., Pan X. An improved rc4 stream cipher, *International Conference on Computer Application and System Modeling*, 2010. DOI: 10.1109/IC-CASM.2010.5620800

12. Allouch A., Cheikhrouhou O., Koubaa A. MAVSec: Securing the MAVLink Protocol for Ardupilot/PX4 Unmanned Aerial Systems, *International Wireless Communications and Mobile Computing Conference (IWCMC)*, Morrocco, 2019. DOI: 10.1109/IWCMC.2019.8766667

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. Zhao J., Cheng D., Hao Ch. An Improved Ant Colony Algorithm for Solving the Path Planning Problem of the Omnidirectional Mobile Vehicle, *Mathematical Problems in Engineering*, 2016, no. 12. DOI: 10.1155/2016/7672839

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

16. Liu C., Ji J., Liu Z. Implementation of DES Encryption Arithmetic based on FPGA, *AASRI Procedia*, 2013, vol. 5, pp. 209 - 213. DOI: 10.1016/j.aasri.2013.10.080

17. Tanygin M.O., Alshaia Kh.Ya *Telekommunikatsii*, 2020, no. 1, pp. 2 - 9.

18. Tanygin M.O. *Teoreticheskie osnovy identifikatsii istochnikov informatsii, peredavaemoi blokami ogranichennogo razmera* (Theoretical basics of sources identification of information transmitted by limited size blocks), Kursk, Izd-vo Universitetskaya kniga, 2020, 198 p.

19. 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-2020-114-155

20. Denisenko T.I. *Fundamental'nye issledovaniya*, 2009, no. 1, pp. 27 – 28.

21. Naumov V.A., Samuilov K.E., Gaidamaka Yu.V. *Mul'tiplikativnye resheniya konechnykh tsepei Markova* (Multiplicative solutions of finite Markov chains), Moscow, RUDN, 2015, 159 p.