УДК 004.056.55 ISSN 1995-5499
DOI: https://doi.org/10.17308/sait/1995-5499/2022/2/38-49
Поступила в редакцию 05.11.2021
Подписана в печать 29.06.2022

МЕТОД ПОВЫШЕНИЯ ДОСТОВЕРНОСТИ ОБМЕНА ДАННЫМИ МЕЖДУ УДАЛЁННЫМИ УЗЛАМИ В УСЛОВИЯХ ОГРАНИЧЕННОГО РАЗМЕРА ИДЕНТИФИКАЦИОННЫХ ПОЛЕЙ СООБЩЕНИЙ

© 2022 А. А. Ахмад, А. Л. Марухленко, В. П. Добрица, М. О. Таныгин✉

Юго-Западный государственный университет
ул. 50 лет Октября, 94, 305040 Курск, Российская Федерация

Аннотация. Широкое распространение распределённых информационных систем для управления технологическими процессами и сложными техническими объектами привело к созданию особого класса протоколов связи, чьей характерной чертой является высокая энергоэффективность и низкая пропускная способность. Это, в свою очередь, приводит к жёстким ограничениям на размер передаваемого кадра информации, и снижает размер полей служебной и идентификационной информации, по которой компоненты распредёлённой системы определяют источник, сформировавший передаваемое управляющее или информационное сообщение. Для повышения достоверности идентификации созданы методы, основанные на определении источника для групп сообщений. Их недостатком является высокая вычислительная сложность, определяемая числом возможных вариантов формирования таких групп из всего множества сообщений, обрабатываемых приёмником. В статье рассматривается метод ограничения множества обрабатываемых блоков для повышения достоверности идентификации и снижения вычислительной сложности реализуемых при этом алгоритмов в условиях ограниченного несколькими битами размера поля идентификационной информации. Описаны математические модели формирования и обработки множеств сообщений приёмниками. На основе полученных результатов показано, что использование неизменности характеристик потока сообщений от источника позволяет в разы повысить достоверность методов, основанных на определении источника для групп сообщений. Определены условия применения метода ограничения множества обрабатываемых слов, при которых наблюдается наибольшее снижение вероятности ошибки идентификации. Практическим результатом проведённых исследований является снижение размеров полей идентификационной информации в пакетах данных, передаваемых между устройствами распределённых информационных систем по каналам связи с ограниченной пропускной способностью, и снижение числа переспросов, вызванных ошибками. Всё это обеспечивает снижение информационной избыточности передаваемых данных и повышение скорости их обработки оконечным оборудованием.

Ключевые слова: обработка потоков сообщений, информационная безопасность, идентификация, математическое моделирование, ошибка идентификации.

✉ Таныгин Максим Олегович
e-mail: tanygin@yandex.ru

ВВЕДЕНИЕ

Основой обеспечения качественных параметров функционирования современных распределённых информационных систем является достоверность обработки информации, передаваемой между отдельными её компонентами. Обеспечить указанную достоверность может лишь идентификация источника каждого передаваемого в такой системе пакета данных.

В общем случае проблема идентификации удалённого субъекта может быть сформулирована следующим образом. Имеется приёмник, в который через канал связи поступает некоторое множество сообщений U. Приемник взаимодействует с несколькими источниками Ω_{I}, Ω_{II}, Ω_{III}, … Из входящего множества сообщений U необходимо выделить непересекающиеся подмножества U_{I}, U_{II}, U_{III}, …, которые были сформированы и переданы в приёмник соответствующими источниками.

Существует большое количество методов определения источника сообщений, но в основе всех их лежит шифрование некоторого цифрового отпечатка из полезных данных сообщения u^{inf} с помощью секретного ключа Ω. [1–6] При этом результат шифрования $F(u^{\text{inf}},\Omega)$ вводится в состав сообщения u и передаётся вместе с полезными данными: $u=\{u^{\text{inf}},F(u^{\text{inf}},\Omega)\}$. В приёмнике происходит проверка содержимого сообщения и отнесение его к одному из множеств $U_{\text{I}},U_{\text{II}},U_{\text{III}},\ldots$

$$\begin{gathered}\mathrm{G}\left(u,\Omega_{\text{I}}\right)=1\Rightarrow u\in U_{\text{I}},\\ \mathrm{G}\left(u,\Omega_{\text{I}}\right)=0\Rightarrow u\notin U_{\text{I}};\\ \mathrm{G}\left(u,\Omega_{\text{II}}\right)=1\Rightarrow u\in U_{\text{II}},\\ \mathrm{G}\left(u,\Omega_{\text{II}}\right)=0\Rightarrow u\notin U_{\text{II}};\\ \ldots\end{gathered}\qquad(1)$$

где G — решающее правило, применяемое к сообщению $u\in U$ и идентификатору Ω_{I} источника, которое позволяет выделить из множества U подмножество U_{I}.

Так как приёмник не обладает априорной информацией о содержимом поля u^{inf}, то принятие решение осуществляется только на основании анализа слова $F(u^{\text{inf}},\Omega)$. Условие возникновения ошибки можно записать в виде:

$$\begin{gathered}u\notin U_A\wedge\mathrm{G}\left(u,\Omega_A\right)=1,\\ u=\left\{u^{\text{inf}},\mathrm{F}\left(u^{\text{inf}},\Omega\right)\right\}.\end{gathered}\qquad(2)$$

где U_A — множество сообщений источника A.

Соответственно, достоверность идентификации определяется соотношением между двумя числами: мощностью множества U и количеством кодовых комбинаций слова $F(u^{\text{inf}},\Omega)$, определяемым разрядностью H поля идентификатора (результата шифрования) в обрабатываемом слове [7]. Вероятность успешной идентификации источника сообщений определится как вероятность невыполнения условия (2) для всех слов множества U, не принадлежащих источнику A:

$$p_{\text{tr}}^{1}=\left(1-2^{-H}\right)^{|U|}.\qquad(3)$$

Для методов идентификации, применяемых в протоколах для каналов связи с низкой пропускной способностью, размер передаваемого сообщения может быть ограничен несколькими десятками и даже несколькими байтами [8]. Соответственно, размер поля идентификатора не позволяет проводить достоверную идентификацию компонентов распределённых систем. Кроме этого, ограничение размеров слов в формуле (2) делает бессмысленным использования широко известных алгоритмов криптографических преобразований. Поэтому в качестве функции необратимого преобразования $F(u^{\text{inf}},\Omega)$ целесообразно использовать алгоритмы, основанные на комбинации побитового исключающего ИЛИ (для уменьшения размера выходного слова) и конъюнкции (для обеспечения зависимости выходного слова от идентификатора источника) [9]. Для повышения достоверности идентификации применяются методы, в основе которых лежит применение решающего правила не к отдельному сообщению, а к группе [10–17]:

$$\begin{gathered}\mathrm{G}\left(\left\{u_1,\ldots u_M\right\},\Omega_{\text{I}}\right)=1\Rightarrow\\ \Rightarrow u_1\in U_{\text{I}},\ldots,u_M\in U,\\ \mathrm{G}\left(\left\{u_1,\ldots u_M\right\},\Omega_{\text{I}}\right)=0\Rightarrow\\ \Rightarrow u\notin U_{\text{I}},\ldots,u_M\notin U,\end{gathered}\qquad(4)$$

где M — размер группы сообщений, для которой принимается решение о принадлежности множеству

Подобные методы дают большую достоверность, так как вероятность случайного выполнения условия (2) для одного сообщения больше, чем для группы из M сообщений. Итоговая вероятность успешной идентификации источника группы из M сообщений определится как:

$$p_{\text{tr}}^{M} = \left(1-2^{-H\cdot M}\right)^{A_{|U|}^{M}} > \left(p_{\text{tr}}^{1}\right)^{M}. \qquad (5)$$

где $A_{|U|}^{M}$ — число сочетаний M по $|U|$, соответствующее числу вариантов формирования группы M сообщений из множества U (считаем, что порядок следования сообщений в условии (4) важен для результата применения правила G).

Недостатком методов идентификации для групп сообщений является высокая вычислительная сложность алгоритмов формирования и проверки таких групп. Для применения решающего правила требуется, в общем случае, сформировать $A_{|U|}^{M}$ проверяемых множеств. Поэтому для возможности их практической реализации используют методы не произвольного формирования группы проверяемых сообщений, а методы направленного поиска вариантов размещения сообщений в группе. В работе [18] рассматривался метод формирования сообщений $u = \{u^{\text{inf}}, F(u^{\text{inf}}, \Omega)\}$, который при определённых условиях давал квадратичную и даже линейную сложность реализации в зависимости от размера множества U, обеспечивая при этом достоверность выше, чем p_{tr}^{1} в формуле (3).

Исходя из сказанного выше, основным методом повышения достоверности идентификации источника сообщения, а также снижения трудоёмкости реализации данной процедуры, является уменьшение размеров множества U обрабатываемых приёмником сообщений.

1. ПОСТАНОВКА ЗАДАЧИ

Основываясь на описанных в литературе методах определения источника информации, был разработан метод, заключающийся в формировании источником группы U_A из M сообщений. В составе каждого сообщения, помимо идентификатора $F(u^{\text{inf}}, \Omega)$, вводится ещё и индекс J сообщения в группе, принимающий значения от 1 до M [19, 20]. Каждое сообщение в группе проверяется не только по значению идентификатора, но и по значению индекса. Это позволяет добиться значительно меньшей вычислительной сложности по сравнению с известными методами [19]. В то же время при длине поля идентификатора $H < \log_2(|U|M^{-1})$ вероятность ошибки резко возрастала, делая метод непригодным для практического использования

Для повышения вероятности правильной идентификации источника необходимо сформулировать правило формирования из множества U всех сообщений, поступивших в приёмник в течение времени передачи множества U_A, меньшего по мощности множества анализируемых сообщений U':

$$\left(1-2^{-H\cdot M}\right)^{A_{|U|}^{M}} > \left(1-2^{-H\cdot M}\right)^{A_{|U'|}^{M}}, \quad \text{при } |U| > |U'|. \qquad (6)$$

В качестве теоретической основы для синтеза правила, ограничивающего мощность множества U', выступает порядок формирования и выдачи блоков данных, образующих множество U_A. Так как его сообщения формируются и передаются последовательно от 1-го до M-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.

2. МАТЕРИАЛЫ И МЕТОДЫ

Рассмотрим произвольный момент времени передачи группы сообщений U_A. Пусть $M_{\max}$ — максимальный индекс всех поступивших сообщений. Тогда при поступлении очередного сообщения u в приёмник, оно будет отнесено ко множеству U' при выполнении условия:

$$M_{\max} + W_{\text{back}} \le J^{u} \le M_{\max} + W_{\text{forw}}, \qquad (7)$$

где J^{u} — индекс поступившего сообщения u,

W_{forw} — ширина окна опережения, максимальное число, на которое индекс поступаю-

щего информационного блока может превышать максимальный индекс сообщений $M_{\max}$, $1 \le W_{\text{forw}} \le M$.

W_{back} — ширина окна запаздывания, параметр, определяющий число, на которое индекс поступающего сообщения может быть меньше $M_{\max}$, $1 \le W_{\text{back}} \le M$.

Таким образом, мощность множества анализируемых сообщений $|U'|$ окажется в $M / \min\left(M, W_{\text{back}} + W_{\text{forw}}\right)$ раз меньше мощности множества U, что позволяет, зная зависимость вероятности p_{tr}^{M} успешной идентификации от параметров H, U' и M (5), оценить эффективность метода.

2.1. Математическая модель оценки достоверности идентификации для исходного метода

Для оценки вероятности корректной идентификации $p_{\text{tr}}^{M} = \text{f}\left(H, |U|, M\right)$ предложена следующая математическая модель процесса обработки данных. На основании значения индекса J, имеющегося в каждом сообщении множества U, последнее можно разделить на M непересекающихся подмножеств $w_1 - w_M$, в состав каждого из которых входит лишь одно сообщение из множества U_A и произвольное число сообщений из множества U / U_A. В соответствии с методом определения источника [19, 21] анализируемые группы формируются исходя из результата проверки первой строки условия (2) для каждого сообщения подмножеств $w_1 - w_M$. Считаем, что сообщения множества U / U_A формируются случайным образом, что верно в случае, если сообщения проходят предварительное декодирование [20]. Тогда случайные величины, которыми являются мощности подмножеств w_i, $i = 1 \ldots M$ подчинены распределению Пуассона с интенсивностью $\left(|U| - M\right) / M$:

$$p^{w}\left(|w_i|\right) = \frac{\left(\left(|U| - M\right) / M\right)^{|w_i|} \times e^{-\frac{\left(|U| - M\right)}{M}}}{|w_i|!}. \quad (8)$$

Вероятность выполнения первой строки условия (2) ровно для k_1 сообщения с учётом вероятности совпадения идентификаторов [18]:

$$p_1\left(k_1\right) = \sum_{l=k_1}^{|U|-M} \left[p^{w}\left(l\right) \times \times \left(C_l^{k_1} \left(2^{-H}\right)^{k_1} \left(1 - 2^{-H}\right)^{l-k_1} \right) \right]. \quad (10)$$

Плотность вероятности числа k_1^h различных вариантов слова $F(u^{\text{inf}}, \Omega)$ для этих k_1 сообщений:

$$p_1^h\left(k_1^h\right) = \sum_{l=k_1^h}^{|U|-n} \left[p_1\left(l\right) \times \times \left(\left(2^{-H}\right)^{j-k_1^h} \prod_{k=1}^{k_1^h} \left(1 - \left(k-1\right)2^{-H}\right) \right) \right]. \quad (11)$$

Для второй позиции в группе имеем k_1^h вариантов слова $F(u^{\text{inf}}, \Omega)$ и $|w_2|$ сообщения, которые образуют $k_1^h |w_2|$ испытаний, в каждом из которых вероятность совпадения идентификаторов для отнесения сообщения к группе равна 2^{-H}. Считая $k_1^h |w_2|$ достаточно большим, получаем вырождение биномиального распределения в распределение Пуассона с интенсивностью $k_1^h |w_2| 2^{-H}$ [19]. С учётом плотности вероятности для $|w_2|$:

$$p_2\left(k_2\right) = \sum_{l=k_2}^{|U|-n} \left[p^{w}\left(l\right) \times \times \sum_{k_1^h=1}^{|U|-n} p_1^h\left(k_1^h\right) \frac{\left(k_1^h \cdot l \cdot 2^{-H}\right)^{l} \times e^{-k_1^h \cdot l \cdot 2^{-H}}}{l!} \right]. \quad (12)$$

На основании (10)–(12) получаем рекуррентные формулы для вероятности формирования k_r, $r = 1 \ldots M$ различных групп сообщений:

$$p_r\left(k_r\right) = \sum_{l=k_r}^{|U|-M} \left[p^{w}\left(l\right) \times \times \sum_{k_{r-1}=1}^{|U|-M} p_{r-1}^h\left(k_{r-1}^h\right) \frac{\left(k_{r-1}^h l 2^{-H}\right)^{l} \times e^{-k_{r-1}^h l 2^{-H}}}{l!} \right], \quad p_r^h\left(k_r^h\right) = \sum_{l=k_r^h}^{|U|-M} \left[p_r\left(l\right) \times \times \left(\left(2^{-H}\right)^{j-k_r^h} \prod_{k=1}^{k_r^h} \left(1 - \left(k-1\right)2^{-H}\right) \right) \right]. \quad (13)$$

Вероятность формирования двух различных групп сообщений длиной j, для каждого

сообщения которых u_i, $i = 1 \ldots j$ верно равенство $\mathrm{G}(u_i, \Omega_A) = 1$:

$$p_{\mathrm{col}}(j) = \sum_{l=1}^{|U|-n} \left[p_j(l) \left(1 - \left(1 - 2^{-H} \right)^l \right) \right], \quad (14)$$

Вероятность формирования двух групп сообщений длиной M, отличающихся одним или несколькими сообщениями, начиная с i-го, для которых верна первая часть условия (4):

$$P_i^{sc} = 1 - \prod_{j=1}^{M-i} \left(1 - p_{\mathrm{col}}(j) \right). \quad (15)$$

Вероятность формирования более чем одной группы сообщений, для каждой из которых выполнится условие (4):

$$P^{col} = 1 - p_{\mathrm{tr}}^M = 1 - \prod_{i=1}^{M-1} \left(1 - P_i^{sc} \right) = \\ = 1 - \prod_{i=1}^{M-1} \left(1 - p_{\mathrm{col}}(i) \right)^{M-i}. \quad (16)$$

Полученные формулы позволяют получить зависимости между вероятностью ошибки идентификации, длиной группы сообщений M, размером поля идентификатора H и мощностью множества анализируемых сообщений $|U|$ (рис. 1). Из результатов проведённых исследований установлено, что функция $p_{\mathrm{tr}}^M = \mathrm{f}(H, |U|, M) = 1 - P^{\mathrm{col}}$. является монотонно убывающей на всём диапазоне изменения значений аргумента $|U|$ от M до ∞. При этом, как видно на графиках (рис. 1), кратное уменьшение мощности множества анализируемых сообщений, особенно в области высоких значений вероятности ошибки, позволит добиться кратного же снижения вероятности ошибки.

2.2. Математическая модель оценки вероятности ошибки формирования множества анализируемых блоков

Описанный выше принцип формирования множества анализируемых сообщений допускает ситуации, при которых сообщения множества U_A не попадут в множество анализируемых сообщений U'. Для оценки вероятности этого события сознана математическая модель получения сообщений приёмником, основанная на представлении процесса поступления сообщений в виде марковского процесса с непрерывным временем. За единицу модельного времени выбрано время передачи множества сообщений U_A. Модель опи-

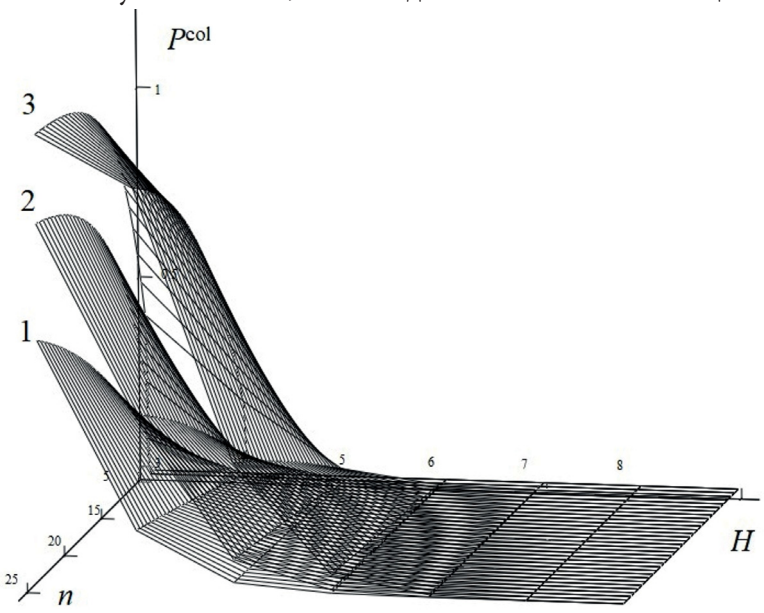

Рис. 1. Зависимость вероятности P^{col} возникновения ошибки определения источника от длины группы сообщений M и длины поля идентификатора H.
1) $|U|/M = 5$, 2) $|U|/M = 10$, 3) $|U|/M = 20$

[Fig. 1. The dependence of the probability P^{col} of the source determining error on the length of the message group M and the length of the identifier field H.
1) $|U|/M = 5$, 2) $|U|/M = 10$, 3) $|U|/M = 20$]

сывается набором состояний $S_{i,j}$, где $i=1\ldots M$ — число поступивших в приёмник сообщений целевого источника, j — максимальный индекс сообщений всех источников, $j \geq i$. Переход из состояния $S_{i,j}$ возможен только в состояния $S_{i,j+1}$ — получение постороннего сообщения источника с индексом, превышающим j, и в стояние $S_{i+1,\max(i+1,j+1)}$ — получение сообщения целевого источника из множества U_A. Существует нескольких поглощающих состояний: $S_{M,M}$ — соответствует попаданию всех сообщений из U_A в U' ($U_A \cap U' = U_A$), $S_{1,M}$ — $S_{M-W_{\text{back}},M}$ — непопаданию в U' части сообщений из U_A ($U_A \cap U' \neq U_A$). Сам граф марковского процесса и описывающая его система уравнений Колмогорова подробно рассмотрены в работе [20], поэтому в настоящей статье мы будем лишь использовать полученные на основе данной математической модели результаты.

График зависимости вероятности P_U успешного формирования множества U' (когда в него попадут все сообщения множества U_A) приведён на рис. 2. В результате моделирования установлено, что величина W_{forw} практически не влияет на вероятность P_U, а лишь увеличивает мощность множества U'. Поэтому этот и последующий результаты приведены для значения $W_{\text{forw}} = 1$.

3. РЕЗУЛЬТАТЫ И ИХ ОБСУЖДЕНИЕ

С учётом того, что ошибка идентификации источника сообщений наступит либо в случае непопадания в U' части сообщений из U_A (вероятность $1-P_U$), либо, при $U_A \cap U' = U_A$ (вероятность P_U), в случае формирования более чем одной группы сообщений мощностью M, для каждой из которых выполнится условие (4) (вероятность $1-p_{\text{tr}}^M$), то общая вероятность возникновения ошибки определится как [21]:

$$P_{\text{err}} = 1 - P_U + P_U\left(1 - p_{\text{tr}}^M\right) = \\ = 1 - P_U p_{\text{tr}}^M. \quad (17)$$

Графики зависимости вероятности ошибки идентификации от размера группы сообщений M, ширины окна запаздывания W_{back}, размера поля идентификационной информации H и числа сообщений в множестве U

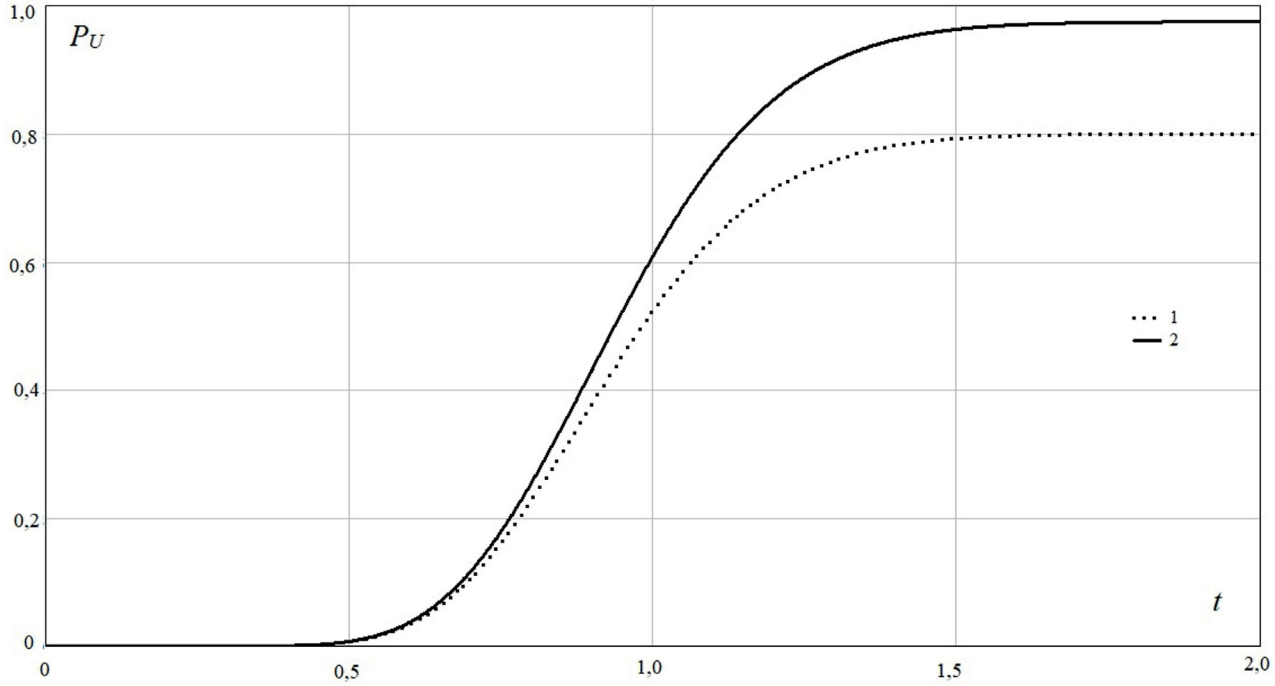

Рис. 2. График зависимости вероятности успешного формирования множества U' от условного времени

1) $H=6$, $|U|=70$, $M=20$, $W_{\text{back}}=10$; 2) $H=6$, $|U|=70$, $M=20$, $W_{\text{back}}=12$

[Fig. 2. Graph of the dependence of the probability of successful formation of the set on the conditional time

1) $H=6$, $|U|=70$, $M=20$, $W_{\text{back}}=10$; 2) $H=6$, $|U|=70$, $M=20$, $W_{\text{back}}=12$]

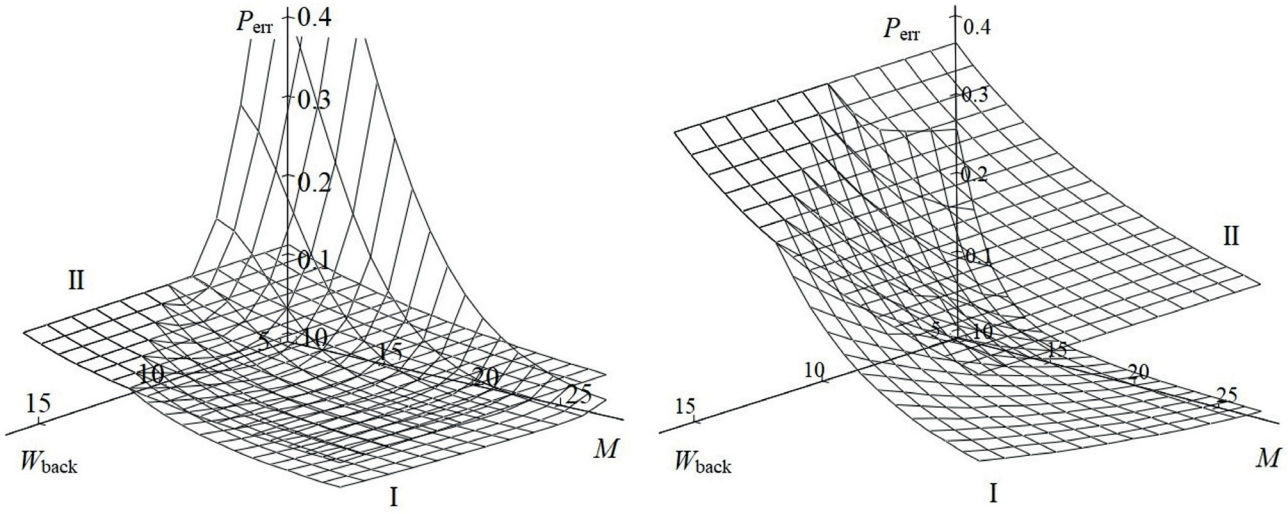

Рис. 3. Графики зависимости вероятности ошибки идентификации при $|U| = 150$:
I — с использованием метода ограничения числа анализируемых сообщений,
II — без использования метода ограничения числа анализируемых сообщений
a) $H = 7$; *b)* $H = 6$

[Fig. 3. Graphs of the dependence of the probability of identification error at $|U| = 150$:
I — using the method of limiting the analyzed messages number,
II — without using the method of limiting the analyzed messages number
a) $H = 7$; *b)* $H = 6$*]*

приведены на рис. 3. График I построен для случая использования метода ограничения числа анализируемых сообщений. Для сравнения: график II — зависимость вероятности ошибки идентификации при анализе всего множества сообщений U. Так же видно, что в области значений, где $W_{back} \geq M$ оба графика совпадают, так как в таком случае мощности множеств U и U' равны.

ЗАКЛЮЧЕНИЕ

В условиях ограниченной длины сообщений и ограниченной длины идентификаторов, входящих в состав таких сообщений, использование методов анализа групп сообщений является единственным средством повышения достоверности идентификации. При этом, как было отмечено выше, достоверность методов анализа групп сообщений вступает в противоречие с вычислительной сложностью процедур определения источников сообщений. Проведённые серии математических экспериментов позволяют утверждать, что использование стационарности свойств потока сообщений (длительности временных интервалов между моментами получения сообщений приёмником) от какого-либо источника является предпосылкой к созданию эффективных методов идентификации, отличающихся более высокой достоверностью и низкой вычислительной сложностью [22].

В работе показано, как с помощью ограничения числа обрабатываемых сообщений можно снизить в 1,5…3,0 раза вероятность возникновения ошибки идентификации источника сообщений. Направлением дальнейших исследований является формулирование комплексной целевой характеристики работы приёмников сообщений ограниченной длины, учитывающей достоверность и трудоёмкость процедур идентификации. После чего в пространстве параметров работы приёмников будут определены области максимальных значений данной функции, а также области максимальных значений её производной, что является теоретическим базисом синтеза протоколов и устройств, обладающих высокими эксплуатационными характери-

стиками в условиях изменения характеристик каналов связи.

КОНФЛИКТ ИНТЕРЕСОВ

Авторы декларируют отсутствие явных и потенциальных конфликтов интересов, связанных с публикацией настоящей статьи.

СПИСОК ЛИТЕРАТУРЫ

1. *Burda, K.* Error Propagation in Various Cipher Block Modes / K. Burda // Int. J. Comput. Sci. Netw. Secur. – 2006. – Vol. 6 – November 2006 – P. 235–239.

2. *Stallings, W.* NIST Block Cipher Modes of Operation for Authentication and Combined Confidentiality and Authentication / W. Stallings // Cryptologia – 2010. – № 34 – P. 225–235 doi: 10.1080/01611191003598295.

3. *Iwata, T.* OMAC: one-key CBC MAC / T. Iwata, K. Kurosawa // Fast Software Encryption, 10th International Workshop. – 2003. – P. 129–153 doi 10.1007/978-3-540-39887-5_11.

4. *Dworkin M.* SP 800-38D: Recommendation for Block Cipher Modes of Operation: Galois/Counter Mode (GCM) and GMAC / M. Dworkin // Computer Security Division Information Technology Laboratory National Institute of Standards and Technology Gaithersburg, MD 20899-8930, 2007.

5. *Ifzarne, S.* Homomorphic Encryption for Compressed Sensing in Wireless Sensor Networks / S. Ifzarne, H. Imad, N. Idrissi // SCA '18, October 10–11, 2018, Tetouan, Morocco DOI 10.1145/3286606.3286857

6. *Бухарин, В. В.* Патент 2 710 284 RU H04L 9/32; G06F 21/00. Способ и устройство управления потоками данных распределенной информационной системы с использованием идентификаторов / В. В. Бухарин, А. В. Казачкин, С. Ю. Карайчев, В. А. Шалагинов, Е. Д. Пикалов, И. Г. Ступаков; заявл. 17.06.2019, опубл. 25.12.2019.

7. *Bogdanov, A.* Biclique Cryptanalysis Of The Full AES / A. Bogdanov, D. Khovratovich, C. Rechberger // LNCS – 2011. – Vol. 7073 – P. 344–371, doi: 10.1007/978-3-642-25385-0_19.

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

9. *Алшаиа, Х. Я.* Формальное описание модели предобработки блока данных для систем с ограниченным размером дополнительных служебных полей / Х. Я. Алшаиа // Инфокоммуникации и космические технологии: состояние, проблемы и пути решения : Сборник научных статей по материалам V Всероссийской научно-практической конференции. – Курск : Юго-Западный государственный университет, 2021. – С. 362–365.

10. *Premkumar, P.* Block Level Data Integrity Assurance Using Matrix Dialing Method towards High Performance Data Security on Cloud Storage / P. Premkumar, D. Shanthi // Circuits and Systems. – 2016. – V. 7, No 11. – P. 3626–3644. doi: 10.4236/cs.2016.711307

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

12. *Ling, Q.* Decentralized Sparse Signal Recovery for Compressive SleepingWireless Sensor Networks / Q. Ling, Z. Tian // IEEE Transactions on Signal Processing. – 2010. – V. 58, No 7. – P. 3816–3827.

13. *Liang, Wei.* A distributed data secure transmission scheme in wireless sensor network / Wei Liang, Yin Huang, Jianbo Xu and Songyou Xie // International Journal of Distributed Sensor Networks, 2017 Volume: 13 Issue: 4, 155014771770555,doi: 10.1177/1550147717705552.

14. *Ashwin Jha.* On Random Read Access in OCB / Ashwin Jha, Cuauhtemoc Mancillas-López, Mridul Nandi Sourav Sen Gupta // IEEE Transactions on Information Theory. – 2019. – PP(99):1-1 doi: 10.1109/TIT.2019.2925613.

15. *Ratnesh, Mishra.* Tewari Energy Efficient Wireless Network Security With Using Block Cipher Technique / Mishra Ratnesh, Ravi Shanker Shukla, K. Rajesh, R. R. Shukla // International Journal of Management, Technology And

Engineering. – 2019. – Volume IX, Issue V. – P. 3704–3718.

16. *Black, J.* CBC MACs For Arbitrary-Length Messages: The Three-Key Constructions / J. Black, P. Rogaway // Advances in Cryptology CRYPTO '00 (2000), vol. 1800 of Lecture Notes in Computer Science, Springer-Verlag. – P. 197–215.

17. *Premkumar, P.* Block Level Data Integrity Assurance Using Matrix Dialing Method Towards High Performance Data Security On Cloud Storage / P. Premkumar, D. Shanthi // Circuits and Systems. – 2016. – 07(11): 3626-3644 doi: 10.4236/cs.2016.711307

18. *Tanygin, M. O.* A Method Of The Transmitted Blocks Information Integrity Control / M. O. Tanygi, H. Y. Alshaeaa, E. A. Kuleshova // Radio Electronics, Computer Science, Control. – 2020. – № 1. – P. 181–189. DOI: doi: 10.15588/1607-3274-2020-1-18.

19. *Таныгин, М. О.* Теоретические основы идентификации источников информации, передаваемой блоками ограниченного размера : монография. – Курск : Изд-во ЗАО «Университетская книга», 2020. – 198 с.

20. *Таныгин, М. О.* Метод ограничения множества обрабатываемых приёмником блоков данных для повышения достоверности операций определения их источника / М. О. Таныгин, О. Г. Добросердов, А. О. Власова, А. А. Ахмад // Труды МАИ. – 2021. – Т. 118, № 3. – С. 15. – doi 10.34759/trd-2021-118-14.

21. *Tanygin, M. O.* Study of the Influence of the Unauthorized Blocks Number on the Collision Probability / M. O. Tanygin, H. Y. Alshaeaa, V. P. Dobritsa // Advances in Automation II, RusAutoConf 2020 Lecture Notes in Electrical Engineering, 2021, 729 LNEE. – P. 111–120. doi: 10.1007/978-3-030-71119-1_12

22. *Муравьева-Витковская, Л. А.* Вероятность распределения интервала времени между пакетами в корпоративной компьютерной сети / Л. А. Муравьева-Витковская, М. А. Фарашиани // Изв. вузов. Приборостроение. – 2017. – Т. 60, № 10. – С. 957–960. – doi: 10.17586/0021-3454- 2017-60-10-957-960

Ахмад Али Айед Ахмад — аспирант кафедры информационной безопасности Юго-Западного государственного университета.
E-mail: aliayid2013@gmail.com
ORCID iD: https://orcid.org/0000-0002-6031-9414

Добрица Вячеслав Порфирьевич — д-р физ.-мат. наук, проф., профессор кафедры информационной безопасности Юго-Западного государственного университета.
E-mail: dobritsa@mail.ru
ORCID iD: https://orcid.org/0000-0001-7533-3684

Марухленко Анатолий Леонидович — канд. техн. наук, доц., доцент кафедры информационной безопасности Юго-Западного государственного университета.
E-mail: proxy33@mail.ru
ORCID iD: https://orcid.org/0000-0002-3575-924X

Таныгин Максим Олегович — канд. техн. наук, доц., заведующий кафедрой кафедры информационной безопасности Юго-Западного государственного университета.
E-mail: tanygin@yandex.ru
ORCID iD: https://orcid.org/0000-0002-4099-1414

DOI: https://doi.org/10.17308/sait/1995-5499/2022/2/38-49 ISSN 1995-5499
Received 05.11.2021
Accepted 29.06.2022

A METHOD FOR INCREASING THE RELIABILITY OF DATA EXCHANGE BETWEEN REMOTE NODES IN CONDITIONS OF A LIMITED SIZE OF MESSAGE IDENTIFICATION FIELDS

© 2022 A. A. Ahmad, A. L. Marukhlenko, V. P. Dobritsa, M. O. Tanygin✉

Southwest State University
94, 50 let Oktyabrya Street, 305040 Kursk, Russian Federation

Annotation. The widespread use of distributed information systems for managing technological processes and complex technical objects has led to the creation of a special class of communication protocols. These protocols are characterized by high energy efficiency and low bandwidth. This cause strict restriction on the size of the transmitted information frame and reduces the size of the service and identification information fields. These fields are used by the distributed system components for determination the source that formed the transmitted control or information message. To increase the reliability of identification, methods based on determining the source for groups of messages have been created. Their disadvantage is the high computational complexity, determined by the number of possible options for forming such groups from the entire set of received messages. The article considers a method of limiting the processed blocks set to increase the identification reliability and reduce the computational complexity of the algorithms implemented in this case under conditions of a limited size of the identification information field by several bits. Mathematical models of the formation and processing of sets of messages by receivers are described. Based on the obtained results, it is shown that using the stability of the message flow characteristics allows us to significantly increase the reliability of methods based on determining the source for messages groups. The conditions for the discussed method application, which the greatest decrease in the identification error probability is observed, are determined. The practical result of the conducted research is to reduce the identification information fields size in data packets transmitted between devices of distributed information systems via communication channels with limited bandwidth, and to reduce the number of re-queries caused by errors. It reduces the transmitted data information redundancy and increases the devices performance.
Keywords: message flow processing, information security, identification, mathematical modeling, identification error.

CONFLICT OF INTEREST

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

REFERENCES

1. *Burda K.* (2006) Error Propagation in Various Cipher Block Modes. *Int. J. Comput. Sci. Netw. Secur*. 6. P. 235–239.

2. *Stallings W.* (2010) NIST Block Cipher Modes of Operation for Authentication and Combined Confidentiality and Authentication. *Cryptologia*. 34. P. 225–235 doi: 10.1080/01611191003598295.

3. *Iwata T. and Kurosawa K.* (2003) OMAC: one-key CBC MAC. *Fast Software Encryption, 10th International Workshop*. P. 129–153. doi 10.1007/978-3-540-39887-5_11.

4. *Dworkin M.* (2007) SP 800-38D: Recommendation for block cipher modes of operation: galois/counter mode (GCM) and GMAC. *Computer Security Division Information Technology Laboratory National Institute of Standards and Technology Gaithersburg*, MD 20899-8930.

5. *Ifzarne S., Imad H. and Idrissi N.* (2018) Homomorphic encryption for compressed sensing in wireless sensor networks. *SCA '18, Tetouan, Morocco.* doi 10.1145/3286606.3286857

✉ Tanygin Maxim Olegovich
e-mail: tanygin@yandex.ru

6. *Bukharin V. V. et al.* (2019) Method and device for managing data flows of a distributed information system using identifiers Patent 2710284 RU H04L 9/32; G06F 21/00.

7. *Bogdanov A., Khovratovich D. and Rechberger C.* (2011) Biclique cryptanalysis of the full. *AES LNCS*, 7073. P. 344–371. doi: 10.1007/978-3-642-25385-0_19.

8. *Mytsko E. A., Malchukov A. N. and Ivanov S. D.* (2018) CRC8 computation algorithms research in microprocessor systems with resource deficiency. *Devices and systems. Management, monitoring, diagnostics*. 6. P. 22–29.

9. *Alshaia H. Y.* (2021) Formal descrip-tion of the data block preprocessing model for systems with a limited size of additional service fields. *Infocommunications and space technolo-gies: state, problems and solutions. All-Russian Scientific and Practical Conference*. P. 362–365.

10. *Shant D. and Premkumar P.* (2016) Block level data integrity assurance using matrix dialing method towards high performance data security on cloud storage. *Circuits and Systems*. 7. 11. P. 3626–3644. doi: 10.4236/cs.2016.711307

11. *Othman B. S., Alzaid H., Trad A. and Youssef H.* (2013) An efficient secure data aggregation scheme for wireless sensor networks. *IISA*. doi:10.1109/iisa.2013.6623701

12. *Ling Q. and Tian Z.* (2010) Decentralized Sparse Signal Recovery for Compressive SleepingWireless Sensor Networks. *IEEE Transactions on Signal Processing*. Vol. 58, No 7. P. 3816–3827.

13. *Wei Liang et al.* (2017) A distributed data secure transmission scheme in wireless sensor network. *International Journal of Distributed Sensor Networks*. Volume 13, Issue 4. 155014771770555. doi: 10.1177/ 1550147717705552.

14. *Ashwin J., Mancillas-Lopez C. and Gupta M. N. S. S.* (2019) On random read access in OCB. *IEEE Transactions on Information Theory*. PP(99), 1-1 doi: 10.1109/TIT.2019.2925613.

15. *Mishra R., Shukla R. Sh., Shukla R. K. and Tewari R. R.* (2019) Energy efficient wireless network security with using block cipher technique. *International Journal of Management, Technology And Engineering*. Volume IX, Issue V. P. 3704–3718.

16. *Black J. and Rogaway P.* (2000) CBC MACs for arbitrary-length messages: The Three-Key. *Constructions Advances in Cryptology CRYPTO '00 Lecture Notes in Computer Science*. Vol. 1800. – P. 197–215.

17. *Premkumar P. and Shanthi D.* (2016) Block level data integrity assurance using matrix dialing method towards high performance data security on cloud storage. *Circuits and Systems*. 07(11). P. 3626–3644. doi: 10.4236/cs.2016.711307

18. *Tanygin M. O., Alshaeaa H. Y. and Kuleshova E. A.* (2020) A method of the transmitted blocks information integrity control. *Radio Electronics, Computer Science, Control*. 1. P. 181–189. doi: 10.15588/1607-3274-2020-1-18.

19. *Tanygin M. O.* (2020) Theoretical basics of sources identification of information transmitted by limited size. *blocks Kursk, Universitetskaya kniga*. 198 p.

20. *Tanygin M. O. et al.* (2021) A method for limiting data blocks set being processed by the receiver to increase their source detection operations reliability. *Proceedings of MAI*. Vol. 118. 3. 15. doi 10.34759/trd-2021-118-14.

21. *Tanygin M. O., Alshaia H. Y. et al.* (2021) Study of the Influence of the Unauthorized Blocks Number on the Collision Probability. *Advances in Automation II, Lecture Notes in Electrical Engineering*. 729. P. 111–120. doi: 10.1007/978-3-030-71119-1_12

22. *Muravyeva-Vitkovskaya L. A. and Farashiani M. A.* (2017) Probability distribution for the time interval between packets in corporate computer network. *Journal of Instrument Engineering*. Vol. 60. 10. P. 957–960 doi: 10.17586/0021-3454-2017-60-10-957-960.

Ali Ayid Ahmad Ahmad — postgraduate student of the Department of Information Security, Southwest State University, Kursk, Russian Federation.
E-mail: aliayid2013@gmail.com
ORCID iD: https://orcid.org/0000-0002-6031-9414

Dobritsa Vyacheslav Porfirevich — DSc in Physics and Mathematics, Prof., Professor, Department of Information Security, Southwest State University.
E-mail: dobritsa@mail.ru
ORCID iD: https://orcid.org/0000-0001-7533-3684

Marukhlenko Anatoly Leonidovich — PhD in Technical Sciences, Associate Prof., Associate Professor of the Department of Information Security of the Southwest State University.
E-mail: proxy33@mail.ru
ORCID iD: https://orcid.org/0000-0002-3575-924X

Tanygin Maxim Olegovich — PhD in Technical Sciences, Associate Prof., Head of the Department of Information Security, Southwest State University.
E-mail: tanygin@yandex.ru
ORCID iD: https://orcid.org/0000-0002-4099-1414