УДК 004.052 DOI: 10.34759/trd-2020-114-15

Оценка влияния организации буферной памяти на скорость выполнения процедур определения источника сообщений

Таныгин М.О.*, Алшаиа Х.Я.А., Добрица В.П.*****

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: dobritsa@mail.ru*

Статья поступила 24.09.2020

Аннотация

В статье рассмотрена проблема влияния организации внутренней памяти приёмника на скорость выполнения операций анализа источника поступающих информационных блоков. Определены условия использования различных вариантов организации внутренней памяти приёмника, обеспечивающие высокую скорость обработки и приемлемою аппаратную сложность приёмников.

Ключевые слова: обработка данных, приёмник сообщений, оперативная память, быстродействие, имитационное моделирование.

Введение

Особенностью современного этапа развития информационных технологий является внедрение управляющих и контролирующих элементов и устройств

вычислительной техники практически во все процессы жизнедеятельности человека и их последующие объединение в распределённые информационные системы различного размера. Это обуславливает для элементов и устройств таких систем необходимость обмениваться информацией друг с другом. При этом, из-за особенностей эксплуатации таких устройств, например, низкого энергопотребления, высокой автономности, небольшого объём передаваемых и обрабатываемых данных, для организации их используют протоколы с небольшим (до нескольких байтов) размером кадра информации [1, 2]. Для них традиционные методы и алгоритмы идентификации источника поступающих данных и контроля целостности являются неэффективными с точки зрения высокой информационной избыточности, которая создаётся дополнительными служебными полями с атрибутивными [3, 4] и контрольными кодовыми последовательностями [5, 6].

Для снижения информационной избыточности, и, соответственно, повышения скорости передачи и обработки данных между устройствами распределённых информационных систем, при определении источника данных используются методы, основанные на анализе не отдельных пакетов (информационных блоков), а их множеств. Для таких множеств на основе содержимого отдельных информационных блоков и их дополнительных атрибутивных полей формируется некий критерий, по значению которого данное множество может быть определено как сформированное конкретным устройством – источником. Примером такого подхода может быть метод контроля целостности и аутентичности, описанный в работе [7]. Метод позволяет

формировать критерий принадлежности данных источнику за счёт операций над проверочной матрицей и вектором поступающих слов в полях Галуа. Другим методом, ориентированным на определение источника сообщений небольшой длины является метод контроля динамически конфигурируемых маршрутов доставки каждого из них [8]. Его особенностью является большой объём дополнительной служебной информации, доходящий до 30% от общего объёма передаваемой информации при размере контролируемых пакетов в несколько десятков байтов. Упомянутый ранее метод контроля аутентичности [3] предполагает последовательное исчисление небольших по объёму хешей из данных информационных блоков источника и добавлении полученной последовательности к следующему в цепочки, по аналогии с подходами, используемыми с технологии блок-чейн [9]. Аналогичный подход, основанный на преобразовании содержимого информационных полей в соответствии с некоторым ключом и формировании хеш-последовательностей описывается и в работах [10 – 12]. Общей отличительной их особенностью является принятие решения об источнике полученных данных с некоторой задержкой, определяемой используемыми операциями для преобразования данных и мощность множества анализируемых блоков данных. Это требует дополнительной буферной памяти для временного хранения как самих блоков данных, так и сформированных из них промежуточных результатов вычислений.

Целью работы является исследование определение потребности в ресурсах (объёме буферной памяти, времени поиска и извлечения буферизированной

информации) для исследуемого метода [13] определения источника данных, поступающих в приёмник

Материалы и методы

В нашем методе подход к определению источника информационных блоков (ИБ) небольшого размера, а также их расположения в рамах одного фрагментированного сообщения может быть описан следующим образом. Мы имеем: U – множество полученных приёмником ИБ, в которое как подмножество входит некоторое множество $\tilde{u}$, образующее фрагментированное сообщение, для которого мы устанавливаем факт выдачи всех его блоков целевым устройством – источником. Условие того, что сообщение $\tilde{u}$ выдано конкретными источником может быть записано в виде [14]:

$$\begin{gathered}\exists!\,\tilde{u}\subset U\left(\left(\left|\tilde{u}\right|=n\right)\vee\left(\boldsymbol{B}\left(\tilde{u},S^{\text{key}}\right)=1\right)\right),\\ \forall\underset{\sim}{u}\subset U\left(\left(\underset{\sim}{u}\neq\tilde{u}\right)\vee\left(\left|\underset{\sim}{u}\right|=\left|\tilde{u}\right|\right)\vee\left(\boldsymbol{B}\left(\underset{\sim}{u},S^{\text{key}}\right)=0\right)\right).\end{gathered}\qquad(1)$$

где: $\boldsymbol{B}$ – функция соответствия подмножества $\tilde{u}$ идентификатору S^{key}, принимающая истинное значения, если существует упорядоченное множество $\tilde{u}=\{s_i \mid i=\overline{1\ldots n}\}$ мощностью n, при этом позиция i каждого элемента s_i, $i=\overline{1\ldots n}$ этого множества в таком множестве однозначно определяется параметром S^{key} и содержимым элемента,

n – длина сообщения $\tilde{u}$, которая определяется информацией S^{key}, которой владеет приёмник об отправителе.

В общем случае устройству – приёмнику необходимо разделять всё множество поступающих в него ИБ, на подмножества, сформированные устройствами, с которыми оно обменивается информацией. Пусть для с каждого из них в приёмнике хранится некоторая ключевая информация: $S_1^{\text{key}},\dots,S_k^{\text{key}}$, k – количество источников информации. Тогда для каждого такого подмножества условие (1) запишется как :

$$\begin{aligned}&\exists!\,\tilde{u}_i \subset U\left(\left|\tilde{u}_i\right|=n,\vee \boldsymbol{B}\left(\tilde{u}_i,S_i^{\text{key}}\right)=1\right),\quad i=\overline{1\dots k}\\&\tilde{u}_i\cap\tilde{u}_j=\varnothing, i=\overline{1\dots k},\ j=\overline{1\dots k}, i\neq j\end{aligned}\qquad (2)$$

Рассматриваемый вариант определения источника сообщений основан на анализе позиции ИБ в сообщении (индекса) и хеше из данных предыдущего блока. К каждому блоку данных применяется операция f^{si} выделения информационной части, операция выделения индекса f^{ind} и операция выделения хеша f^{sh}:

$$\forall s\ \subset U\, s^{\text{hash}}=f^{sh}\left(s,S^{\text{key}}\right), s^{\text{ind}}=f^{\text{ind}}\left(s,S^{\text{key}}\right), s^{\text{inf}}=f^{si}\left(s,S^{\text{key}}\right)\qquad (3)$$

Рекуррентное правило для формирования фрагментированного сообщения запишется в виде:

$$\begin{aligned}&F^R\left(s_{\text{start}}\right)=0,\\&i=s_i^{\text{ind}}\Leftrightarrow s_i^{\text{hash}}=F_{\text{hash}}\left(s_{i-1}^{\text{inf}}\right)\wedge i=s_i^{\text{ind}},\\&F^R\left(s_{\text{stop}}\right)=n+1\Leftrightarrow s_{\text{stop}}^{\text{hash}}=F_{\text{hash}}\left(s_n^{\text{inf}}\right),\end{aligned}\qquad (4)$$

где: s_{start} и s_{stop} – служебные стартовые и стоповые блоки, не несущие никакой информации, а служащие лишь для обозначения границ передаваемого фрагментированного сообщения,

F^R – функция позиции i блока в сообщении $\tilde{u} \subset U$: $i = F^R\left(s_i, \tilde{u}, S^{\text{key}}\right)$, $s_i \in \tilde{u}$, $i \in \{1 \ldots n\}$,

F_{hash} – функция, формирующая хеш из данных,

s_i^{ind} – информация об индексе i –го ИБ в сообщении, содержащаяся в полях самого ИБ,

s_i^{inf} – содержимое информационного поля i –го ИБ,

s_i^{hash} – хеш предыдущего блока, содержащийся в i–м ИБ.

Решающая функция подмножества $\tilde{u}$ источнику сообщения запишется в виде:

$$\begin{aligned} &\boldsymbol{B}\left(\tilde{u}, S^{\text{key}}\right) = 1 \Leftrightarrow \tilde{u}^{\langle 0 \rangle} = s_{\text{start}} \wedge \left|\tilde{u}\right| = n \wedge \tilde{u}^{\langle n+1 \rangle} = s_{\text{stop}} \wedge \\ &\wedge_{i=1}^{n} f^{\text{ind}}\left(\tilde{u}^{\langle i \rangle}, S^{\text{key}}\right) = i \wedge_{i=1}^{n} f^{sh}\left(\tilde{u}^{\langle i \rangle}, S^{\text{key}}\right) = F_{\text{hash}}\left(f^{si}\left(\tilde{u}^{\langle i-1 \rangle}, S^{\text{key}}\right)\right), \tilde{u} \subset U \end{aligned} \quad (5)$$

Отличительной особенностью рассматриваемого метода определения источника сообщений на основании значений дополнительных полей s_i^{ind} и s_i^{hash}, является то, что размер данных полей меньше, чем размер стандартных полей атрибутов, используемых в сетях с ограниченным размером кадра сообщений [15 – 17], что и обеспечивает заявленную цель метода – снижение информационной избыточности передаваемых данных и повышение пропускной способности канала связи.

В общем случае всё множество U обрабатываемых приёмником ИБ есть объединение блоков сообщений $\tilde{u}_1$, $\tilde{u}_2$, …, $\tilde{u}_k$, сформированных различными устройствами – источниками. Априори приёмник не знает, какому из сообщений принадлежит конкретный ИБ и ему необходимо рассматривать возможность

принадлежности блока каждому из k сообщений. Это обуславливает, как и в в рассмотренных выше методах, необходимость предварительной буферизации данных до момента вычисления значения функции $\boldsymbol{B}$.

При этом его практическая реализация метода допускает два варианта буферизации, зависящие от момента выполнения операций f^{si}, f^{ind} и f^{sh} [18]:

1) Буферизация необработанного информационного блока с последующим выполнением операций лишь после получения стопового блока s_{stop}.

2) Выполнение операций выделения частей информационного блока до момента помещения его в буфер.

Каждый из двух вариантов обладает собственными достоинствами и недостатками, которые проистекают из принципов, на которых основан сам метод определения источника.

В первом варианте блок буферизируется необработанным, соответственно, объём буферной памяти должен быть незначительно больше (для обработки возможных ошибок) произведения размера блока на мощность множества U. Так как размер блока считаем некоторой константой, характерной для протокола связи, то в дальнейшем в настоящей работе будем измерять размер требуемой памяти в количестве таких блоков, которые можно разместить в ней. Недостаток данного подхода заключается в необходимости при формировании произвольного сообщения $\tilde{u}_r$, $r = 1 \ldots k$, производить последовательно чтение из буфера всех ИБ до момента обнаружения такого, который будет удовлетворять правилу (4). Даже если пренебречь возможностью совпадения

хешей за счёт увеличения размера соответствующего поля [19], количество таких операций чтения будут расти с ростом числа *k* устройств – источников.

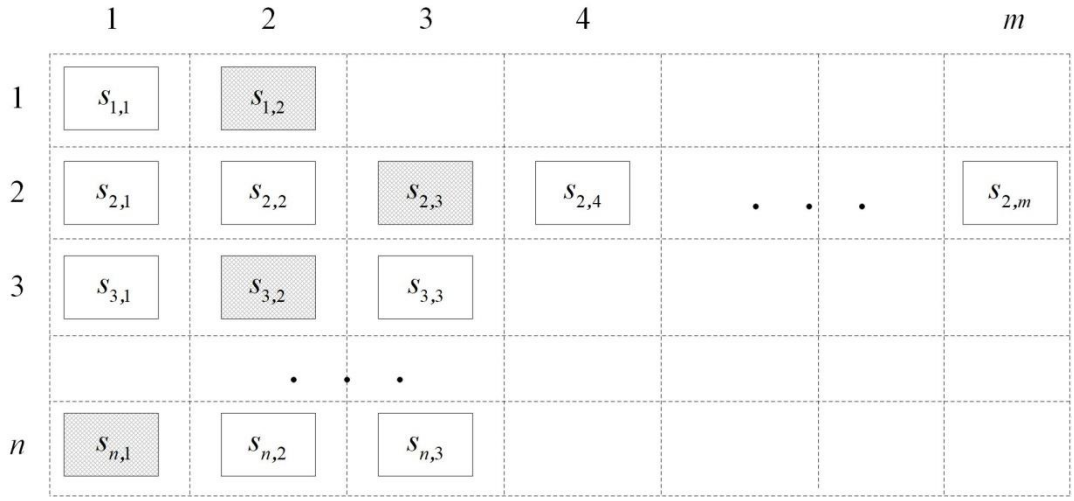

Рисунок 1 – Схема размещения блоков данных

Второй же вариант в свою очередь подразумевает разбитие всего адресного пространства буфера на *k* изолированных областей, хранящее по $|U|$ блоков каждое. В таких областях размещаются элементы блоков данных, над которыми произведены операции f^{si}, f^{ind} и f^{sh} на основе соответствующих ключей S_1^{key},… , S_k^{key} . По своему заполнению они представляют из себя матрицу (рис. 1), где $s_{i,j}$ – блок с индексом *i*, который поступил в устройство *j*–м среди всех ИБ с таким индексом, *m* – максимально возможное число блоков с одинаковым индексом для такого подмножества. При этом $i = s_{i,j}^{\text{ind}} = f^{\text{ind}}\left(s_{i,j}, S_r^{\text{key}}\right)$, $r = 1\ldots k$ – порядковый номер области памяти. Тоном выделены блоки, которые входят в состав сообщения $\tilde{u}_r$, белые блоки – остальные ИБ множества *U*. При подобной организации снижается число операций выбора данных из буфера

при формировании сообщений по правилу (4), так как для добавления одного блока требуется максимум m операций чтения из памяти.

Первый вариант является наиболее распространённым для рассмотренных выше систем определения структуры и источника сообщений, передаваемых по открытым каналам связи. Второй методом, ориентирован на высокую скорость обработки данных и использования его в каналах связи с высокой пропускной способностью [23]. Целью исследования является определение параметров работы информационной системы, в составе которой устройства, обменивающиеся данными, используют второй подход к организации буферной памяти.

Результаты и их обсуждение

Число операций чтения из памяти является одним из важнейших факторов, влияющих на время анализа ИБ и определения источников каждого поступившего в устройство сообщения, так как быстродействие популярных и дешёвых элементов ОЗУ меньше быстродействия микроконтроллеров, даже выполненных по технологии ПЛИС. Кроме того, если операции анализа данных можно распараллелить на независимых вычислительных ядрах, то операции доступа к памяти выполняются только последовательно, так как этот ресурс является неделимым [20, 21].

Количество операций обращений к памяти в первом варианте организации буфера определится исходя из того, что для добавления одного ИБ к сообщению в соответствии с правилом (4) потребуется в среднем прочитать данные $|U|/2$ блоков

(считаем, что поступление ИБ различных источников случайно, что даёт нам случайное их размещение в буфере). Общее число N_{I} операций обращения к памяти при построении k фрагментированных сообщений определится как произведение:

$$N_{\text{I}} = k \cdot n \cdot \frac{|U|}{2} \qquad (6)$$

Для второго варианта организации памяти это число будет равно:

$$N_{\text{II}} = k \cdot \sum_{i=1}^{n} \frac{m_i}{2} = k \cdot \frac{|U|}{2} \qquad (7)$$

где: m_i – число блоков в i-й строке памяти (см. рис. 1)

Видно, что выигрыш в скорости выполнения операций анализа составляет n раз, n – число блоков, составляющих одно фрагментированное сообщение. При этом потребность в объёме памяти возрастёт в $k \cdot n \cdot m / |U| = m$ раз, где m – максимальное число столбцов в одной изолированной области памяти, а $|U| = k \cdot n$. Увеличение числа m ведёт к росту требуемой ёмкости буферной памяти, уменьшение же ведёт к вероятности возникновения ошибки, при которой у блока $s_{i,j} \in \tilde{u}_r$, значение j окажется больше m. Вероятность этого события $p_i^{\text{err}}(j > m)$ для произвольной строки в памяти определится соотношением:

$$p_i^{\text{err}}(j > m) = \frac{m_i - m}{m} p_i(m_i),\ m_i > m \qquad (8)$$

где: $p_i(m_i)$ – вероятность записи на i–ю строку ровно m_i–1 блока, не входящего в сообщение $\tilde{u}_r$ (один блок, входящий в данное сообщение, всегда будет записан)

Эта вероятность определится по рекуррентной формуле, исходя из биномиального закона распределения числа ИБ в одной строке области памяти:

$$p_i(m_i) = \prod_{j=1}^{i-1} p_j(m_j) \cdot C_{|U|-v_i}^{m_i} \left(\frac{n-i+1}{|U|-v_i}\right)^{m_i} \left(1-\frac{n-i+1}{|U|-v_i}\right)^{|U|-v_i-m_i}, \quad (9)$$

$$v_i = \sum_{j=1}^{i-1} m_j$$

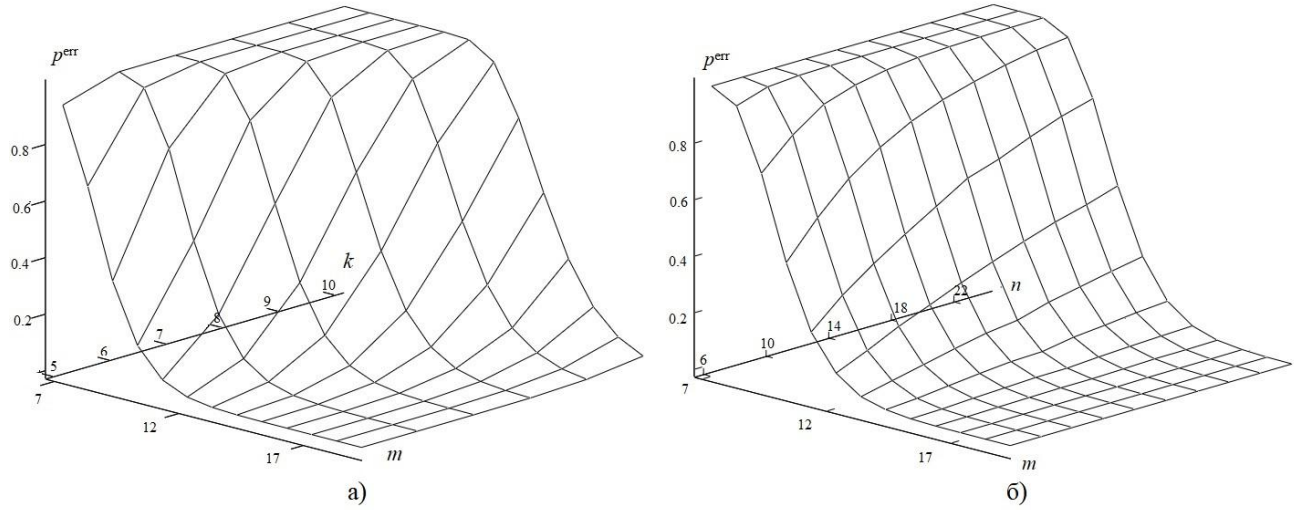

Рисунок 2 – Зависимость частоты возникновения ошибок p^{err} от:

а) количества столбцов в изолированной области памяти m и числа взаимодействующих устройств k б) количества столбцов в изолированной области памяти m и длины фрагментированного сообщения n

Непосредственное вычисление вероятности ошибки по формулам (8) и (9) достаточно трудоёмко и приводит к значительным накопленным ошибкам в результате [22], поэтому вероятность была определена путём имитационного моделирования. С помощью специально разработанного программного обеспечения моделировалось

распределение ИБ по строкам области памяти и подсчитывалась частота возникновения ошибок непопадания блока $s_{i,j} \in \tilde{u}_r$, $r = 1 \ldots k$ в соответствующую строку матрицы памяти. График частоты возникновения ошибок для числа экспериментов 10^4 в зависимости от параметров k, n и m приведены на рисунке 2. Из его анализа видно, что как с ростом длины фрагментированного сообщения, так и с ростом числа взаимодействующих устройств. Однако зависимость вероятности ошибки от длины сообщения не имеет характерной области резкого роста, как соответствующая зависимость от числа устройств (рис. 2. а).

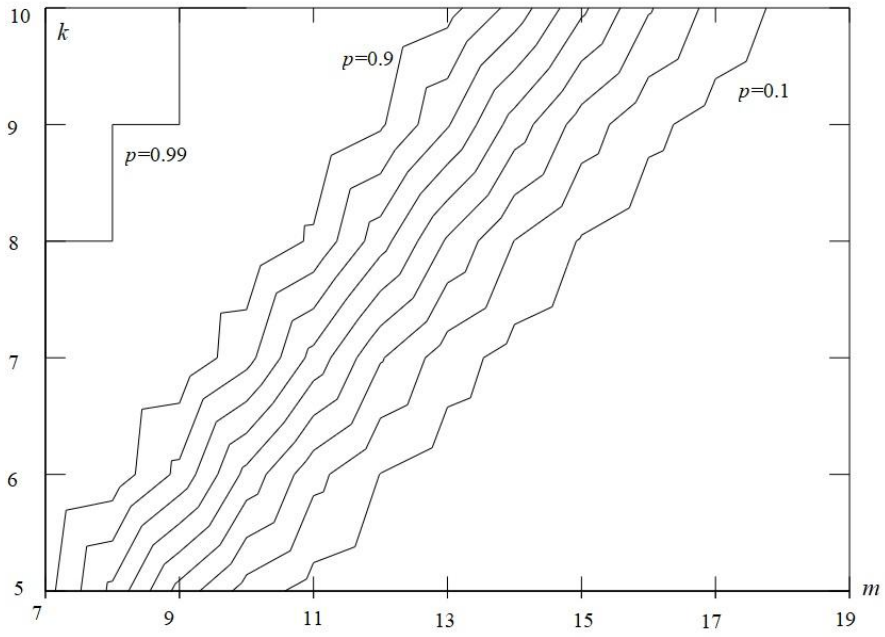

Рисунок 3 – Зависимость между числом взаимодействующих устройств k и количеством столбцов в изолированных области памяти m при различных вероятностях возникновения ошибок p

Кроме того, профилирование графика зависимости частоты возникновения ошибок от числа взаимодействующих устройств позволяет построить графики зависимости между числом взаимодействующих устройств и количества столбцов в изолированной области памяти m при различных вероятностях возникновения ошибок непопадания блока данных целевого источника в буфер приёмника (рис. 3, графики приведены для вероятности, меняющейся в диапазоне от 0.1 до 0.9 с шагом 0.1). Результаты моделирования показывают, что в исследуемых диапазонах изменения параметров ($4<k<12$, $4<n<25$)для того, чтобы вероятность ошибки не превышала 0.1, между числом устройств k и шириной буфера m должно выполняться соотношение $m > k + 7$.

Выводы

Полученные в результате имитационного моделирования зависимости позволяют сделать выводы о применимости рассматриваемого метода организации памяти на основе изолированных областей для повышения скорости обработки данных по сравнению с традиционным методом с общим буфером всех поступающих блоков данных. Для удобства восприятия они представлены в таблице 1.

Таблица 1 Сравнение методов организации буферной памяти

Методы организации памяти	Число устройств – источников		
	Менее 5	От 5 до 10	Более 12
Единое адресное пространство для всех источников	Может использоваться при работе по протоколам связи с низкой пропускной способностью	Целесообразно использовать при небольшой длине фрагментированного сообщения (n<20)	Использование целесообразно
Изолированное адресное пространство для каждого источника	Может использоваться при любой длине фрагментированного сообщений	Целесообразно использовать при длине фрагментированного сообщения большей 20	Нецелесообразно использовать, так как значительно возрастает требуемый объём буферной памяти

Результаты моделирования позволяют выделить три области значений числа взаимодействующих устройств, в каждой из которых применимость рассматриваемого и известного подхода к организации буфера данных различна. При $k<5$ использование изолированных областей памяти даёт прирост скорости, определяемый длиной фрагментированного сообщения (формулы (6) и (7)). При этом, учитывая, что произведение длины сообщения на число взаимодействующих устройств (требуемый исходный объём памяти) будет невелико, несколько десятков блоков памяти, требуемых для хранения одного сообщения, то и его кратное увеличение не создаст трудностей при практической реализации. Традиционный буфер при этом может быть использован в устройствах, взаимодействующих по каналам связи с низкой

пропускной способностью, где скорость обработки не так важна, как объём передаваемых данных. С ростом числа взаимодействующих устройств будет расти вероятность ошибки размещения данных в памяти, что требует увеличения объёма буферного ОЗУ уже на порядки, по сравнению с традиционным единым буфером всех поступающих данных. Поэтому рекомендовать изолированные области памяти для хранения сообщений каждого источника можно только при условии значительного выигрыша в производительности, при больших значениях длины сообщений и высоких требований по скорости обработки данных. При числе взаимодействующих устройств $k>12$ использование изолированных областей становится слишком затратным и необходимо использовать иные методы повышения скорости обработки данных при определении их атрибутов.

Библиографический список

1. Лихтциндер Б.Я., Киричек Р.Ва., Федотов Е.Д., Голубничая Е.Ю., Кочуров А.А. Беспроводные сенсорные сети. - М.: Горячая линия–Телеком, 2020. – 236 с.

2. Талаев А.Д., Бородин В.В., Петраков А.М. Макромодель мультипротокольного взаимодействия сетей LPWAN // Труды МАИ. 2019. № 108. URL: trudymai.ru/published.php?ID=109460. DOI: 10.34759/trd-2019-108-8

3. Black J., Rogaway P. CBC MACs for arbitrary-length messages: The three-key constructions // Advances in Cryptology, CRYPTO – 2000, pp 197 - 215. URL: https://link.springer.com/chapter/10.1007/3-540-44598-6_12

4. W. Stallings. NIST Block Cipher Modes of Operation for Confidentiality // Cryptologia, 2010, no. 34 (2), pp. 163 - 175.

5. Соломатин М.С., Митрофанов Д.В. Модель интеллектуального детектора системы защиты автоматизированной системы управления // Труды МАИ. 2020. № 110. URL: http://trudymai.ru/published.php?ID=112926. DOI: 10.34759/trd-2020-110-16.

6. 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.

7. Papadimitratos P., Haas Z.J. 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. Ben Othman S., Alzaid H., Trad A., Youssef, H. An efficient secure data aggregation scheme for wireless sensor networks // Information, Intelligence, Systems and Applications (IISA), 2013 4th International Conference on Digital Object Identifier, 2013, pp. 1 – 4. DOI: 10.1109/IISA.2013.6623701

9. Fangfang Dai, Yue Shi, Nan Meng, Liang Wei and Zhiguo Ye. From Bitcoin to Cybersecurity: a Comparative Study of Blockchain Application and Security Issues // 4th International Conference on Systems and Informatics (ICSAI 2017), Hangzhou, China, 2017. DOI:10.1109/ICSAI.2017.8248427

10. Dworkin M. Recommendatin for Block Cipher Modes of Operation: The CCM Mode for Authentication and Confidentiality, NIST Special Publication, 2004, SP 800-38C. DOI:10.6028/NIST.SP.800-38C

11. Iwata T., Kurosawa K. OMAC: one-key CBC MAC, Fast Software Encryption, 2003, pp. 129 - 153.

12. Смирнов А.А. Использование метода внесения цифровых предискажений для повышения энергоэффективности инфокоммуникационных радиосредств // Труды МАИ. 2019. № 105. URL: http://trudymai.ru/published.php?ID=104214

13. 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.

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

15. 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

16. 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

17. 802.15.4-2015. IEEE Standard for Low-Rate Wireless Personal Area Networks // IEEE Computer Society. URL: https://standards.ieee.org/standard/802_15_4-2015.html

18. Хоуп Г. Проектирование цифровых вычислительных устройств на интегральных системах. – М.: Радио и связь, 1983. - 538 с.

19. Tanygin M.O. Alshaeaa H.Y. Efremov M.A. Analysis of the Secure Data Transmission System Parameters // Advances in Automation Proceedings of the International Russian Automation Conference, RusAutoCon 2019, September 8–14, 2019, Sochi, Russia, pp. 675 – 683. DOI: 10.1007/978-3-030-39225-3

20. Джон Ф., Уэйкерли М. Проектирование цифровых устройств. - М.: Постмаркет, 2002. – 543 с.

21. Сохранный Е.П. Подготовка данных и расчёт значений приоритетов запросов на проведение сеансов связи с космическими аппаратами научного и социально-экономического назначения // Труды МАИ. 2020. № 111. URL: http://trudymai.ru/published.php?ID=115156. DOI: 10.34759/trd-2020-111-13

22. Турчак Л.И. Численные методы. – М.: Наука, 1987. – 320 с.

23. Tanygin M.O. Method of Control of Data Transmitted Between Softwareand Hardware // Материали IV Міжнародної конференції молодих вчених CSE «Комп'ютерні науки та інженерія». - Львів: Видавництво Львівскої політехніки. 2010. С. 344 - 345.

Evaluating buffer memory organization impact on the message source detection procedures speed

Tanygin M.O.*, Alshaea H.Y.A., Dobritsa V.P.*****

Southwestern State University, SWSU,

94, str. 50 Let Oktyabrya, Kursk, 305040, Russia

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

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

****e-mail: dobritsa@mail.ru*

Abstract

Rather strict requirements to the control cycle duration are being laid in certain types of information systems, such as mobile objects control systems, robotic systems and other real-time systems. Thus, the bit capacity reduction problem of messages transmitted between controlling, monitoring, switching and executing devices is urgent for them. One of the approaches to this is size reduction of the additional service information fields, intended for data integrity and authenticity control. The purpose of the work consists in obtaining numerical dependencies between the required buffer memory volume of the receiver and the execution speed increasing of analysis operations, as well as determining conditions of the memory organization option, being under consideration, application.

The authors established the relationships between the probability error value of the data placing in the receiver buffer and the number of interacting devices, the buffer memory size, and the length of the fragmented message. The article demonstrates that with buffer memory

organized as isolated areas, the speed of memory attribute analysis increases proportionally to the length of the fragmented message transmitted between the source and receiver.

The article shows that with a small number of interacting devices, buffering messages from various sources in isolated memory areas can increase the speed of analysis of attribute information by a factor determined by the fragmented message length. The ratios between the buffer size and the interacting devices number were determined, which reduced the probability of errors in data placement in the buffer up to a value not exceeding 0.1.

Keywords: data processing, message receiver, RAM, performance, simulation.

References

1. Likhttsinder B.Ya., Kirichek R.Va., Fedotov E.D., Golubnichaya E.Yu., Kochurov A.A. *Besprovodnye sensornye seti* (Wireless sensor network), Moscow, Goryachaya liniya - Telekom, 2020, 236 p.

2. Talaev A.D., Borodin V.V., Petrakov A.M. *Trudy MAI*, 2019, no. 108. URL: trudymai.ru/published.php?ID=109460. DOI: 10.34759/trd-2019-108-8

3. Black J., Rogaway P. CBC MACs for arbitrary-length messages: The three-key constructions, *Advances in Cryptology, CRYPTO – 2000*, pp 197 - 215. URL: https://link.springer.com/chapter/10.1007/3-540-44598-6_12

4. W. Stallings. NIST Block Cipher Modes of Operation for Confidentiality, *Cryptologia*, 2010, no. 34 (2), pp. 163 - 175.

5. Solomatin M.S., Mitrofanov D.V. *Trudy MAI*, 2020, no. 110. URL: http://trudymai.ru/published.php?ID=112926. DOI: 10.34759/trd-2020-110-16.

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

7. Papadimitratos P., Haas Z.J. 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. Ben Othman S., Alzaid H., Trad A., Youssef, H. An efficient secure data aggregation scheme for wireless sensor networks, *Information, Intelligence, Systems and Applications (IISA), 2013 4th International Conference on Digital Object Identifier*, 2013, pp. 1 – 4. DOI: 10.1109/IISA.2013.6623701

9. Fangfang Dai, Yue Shi, Nan Meng, Liang Wei and Zhiguo Ye. From Bitcoin to Cybersecurity: Comparative Study of Blockchain Application and Security Issues, *4th International Conference on Systems and Informatics (ICSAI 2017)*, Hangzhou, China, 2017. DOI: 10.1109/ICSAI.2017.8248427

10. Dworkin M. *Recommendatin for Block Cipher Modes of Operation: The CCM Mode for Authentication and Confidentiality*, NIST Special Publication, 2004, SP 800-38C. DOI:10.6028/NIST.SP.800-38C

11. Iwata T., Kurosawa K. *OMAC: one-key CBC MAC*, Fast Software Encryption, 2003, pp. 129 - 153.

12. Smirnov A.A. *Trudy MAI*, 2019, no. 105. URL: http://trudymai.ru/eng/published.php?ID=104214

13. 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.

14. Tanygin M.O. *Teoreticheskie osnovy identifikatsii istochnikov informatsii, peredavaemoi blokami ogranichennogo razmera* (Theoretical basis for identifying sources of information transmitted by limited size blocks), Kursk, Universitetskaya kniga, 2020, 198 p.

15. *Predvaritel'nyi natsional'nyi standart RF. PNST 354-2019. Informatsionnye tekhnologii. Internet veshchei. Protokol besprovodnoi peredachi dannykh na osnove uzkopolosnoi modulyatsii radiosignala (NB-Fi)* (Preliminary National Standard of the Russian Federation. PNST 354-2019. Information technology. Internet of things. Wireless data transfer Protocol based on narrow-band radio signal modulation). URL: http://docs.cntd.ru/document/1200162760

16. *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

17. 802.15.4-2015. IEEE Standard for Low-Rate Wireless Personal Area Networks, *IEEE Computer Society*. URL: https://standards.ieee.org/standard/802_15_4-2015.html

18. Khoup G. *Proektirovanie tsifrovykh vychislitel'nykh ustroistv na integral'nykh sistemakh* (Digital computing devices design based on integrated systems), Moscow, Radio i svyaz', 1983, 538 p.

19. Tanygin M.O. Alshaeaa H.Y. Efremov M.A. Analysis of the Secure Data Transmission System Parameters, *Advances in Automation Proceedings of the International Russian Automation Conference, RusAutoCon 2019*, September 8–14, 2019, Sochi, Russia, pp. 675 – 683. DOI: 10.1007/978-3-030-39225-3

20. Dzhon F., Ueikerli M. *Proektirovanie tsifrovykh ustroistv* (Design of digital devices), Moscow, Postmarket, 2002, 543 p.

21. Sokhrannyi E.P. *Trudy MAI*, 2020, no. 111. URL: http://trudymai.ru/published.php?ID=115156. DOI: 10.34759/trd-2020-111-13

22. Turchak L.I. *Chislennye metody* (Numerical methods), Moscow, Nauka, 1987, 320 p.

23. Tanygin M.O. Method of Control of Data Transmitted Between Software and Hardware, *Materiali IV Mizhnarodnoï konferentsiï molodikh vchenikh CSE "Komp'yuterni nauki ta inzheneriya"*, L'viv, Vidavnitstvo Lvivskoï politekhniki, 2010, pp. 344 - 345.