МИНИСТЕРСТВО ОБРАЗОВАНИЯ И НАУКИ РОССИЙСКОЙ ФЕДЕРАЦИИ
ИЗВЕСТИЯ ВЫСШИХ УЧЕБНЫХ ЗАВЕДЕНИЙ
ПРИБОРОСТРОЕНИЕ
ИЗДАНИЕ САНКТ-ПЕТЕРБУРГСКОГО НАЦИОНАЛЬНОГО ИССЛЕДОВАТЕЛЬСКОГО УНИВЕРСИТЕТА ИНФОРМАЦИОННЫХ ТЕХНОЛОГИЙ, МЕХАНИКИ И ОПТИКИ
Журнал издается с января 1958 г.

ТОМ 56 **АВГУСТ 2013** **№ 8**

СПЕЦИАЛЬНЫЙ ВЫПУСК

ВОПРОСЫ ХРАНЕНИЯ И ПЕРЕДАЧИ ИНФОРМАЦИИ

Под редакцией доктора технических наук, профессора Е. А. Крука

СОДЕРЖАНИЕ

СИСТЕМЫ ХРАНЕНИЯ ИНФОРМАЦИИ

SPECIAL ISSUE

PROBLEMS OF INFORMATION STORAGE AND TRANSFER

By Edition of E. A. Krouk, Doctor of Technical Sciences, Professor

CONTENTS

INFORMATION STORAGE SYSTEMS

ПРЕДИСЛОВИЕ

Настоящий сборник посвящен десятилетию кафедры безопасности информационных систем Санкт-Петербургского университета аэрокосмического приборостроения. Десять лет — не слишком большой срок для такой консервативной структуры, как кафедра высшего учебного заведения, однако все же достаточный для того, чтобы отметить это событие публикацией спецвыпуска.

Прошедшие десять лет были напряженным и, хочется думать, успешным временем. За эти годы на кафедре было защищено 10 кандидатских и 3 докторские диссертации. Издано 5 монографий (в том числе в издательстве John Wiley & Sons, Ltd: “Error Correcting Coding and Security for Data Networks. Analysis of the Superchannel Concept” и “Modulation and Coding Techniques in Wireless Communications”) и 2 сборника трудов, опубликованы сотни статей в том числе более 20 в ведущих мировых периодических изданиях, получено более 30 международных патентов.

Изначально научные интересы кафедры складывались в рамках теоретической информатики — теории помехоустойчивого кодирования и криптографии с открытым ключом, к настоящему времени на ней развивается тематика построения систем передачи информации, множественного доступа, сетевой безопасности, сжатия и обработки видеоинформации. Значительное влияние на развитие кафедры оказало то обстоятельство, что сегодняшние реалии недофинасирования высшей школы потребовали поиска и проведения работ по заказам промышленных предприятий. Заказчиками научно-исследовательских работ кафедры стали такие крупнейшие мировые компании, как Интел, Самсунг, Сименс, EMC и др. Соответственно на кафедре увеличился удельный вес прикладных исследований.

Указанные обстоятельства нашли отражение в предлагаемом вниманию читателей сборнике. Его тематика широка.

Значительное место в нем занимают статьи, посвященные помехоустойчивому кодированию. Коды, исправляющие ошибки, являются универсальным средством борьбы с искажениями, возникающими при передаче, хранении и обработке информации. Созданные и широко используемые для борьбы с искажениями на физическом уровне сетей связи коды находят сегодня применение на транспортном и прикладном уровнях сетей, в задачах обеспечения безопасности, при организации систем хранения информации. В сборнике представлены как статьи по классической теории кодирования (А. В. Козлов и др., С. В. Федоренко), так и по ее нестандартным применениям (М. О. Алексеев, Е. А. Крук и Д. А. Маличенко).

Задача организации надежной связи для широкого спектра современных приложений остается одной из наиболее актуальных в области развития современных информационных технологий. Современные сети передачи данных (мобильные сети, сенсорные сети, автоматизированные системы контроля и учета потребления электроэнергии и т.п.), с одной стороны, находят широкое применение в промышленности и становятся важным элементом информационной инфраструктуры общества, а с другой — предполагают использование специальных телекоммуникационных технологий. На сегодняшний день не только не решены вопросы создания аппаратуры, реализующей эти технологии, но и сами указанные технологии нуждаются в дальнейшем развитии. Вопросам передачи информации в беспроводных сетях посвящен

раздел настоящего сборника. Рассматриваются как методы повышения качества приема сообщений (К. Б. Гурнов и Г. С. Евсеев), так и методы организации сетей (М. А. Гранкин и др.).

Увеличение доли видеоинформации в общем объеме передачи, характерное для систем связи 4—5 поколений, привело к возникновению новых задач и возможностей в области обработки и передачи видео. В сборнике рассматриваются вопросы кодирования видеоинформации как с целью повышения его эффективности (А. И. Веселов и др.), так и с целью обеспечения безопасности (А. В. Афанасьева и др.).

В сборнике рассматриваются также вопросы организации систем хранения информации (Е. М. Линский и др., В. А. Богатырев и др.).

В заключение хочется отметить, что настоящий сборник является третьим, который выпускает кафедра за последние пять лет, но первым, который выходит в качестве специального выпуска журнала „Известия вузов. Приборостроение“.

Заведующий кафедрой безопасности информационных систем ГУАП,
доктор технических наук, профессор, Заслуженный деятель науки РФ
Е. А. КРУК

PREFACE

This collection of papers is dedicated to the 10th anniversary of Information Systems Security Department of St. Petersburg State University of Aerospace Instrumentation. Ten years is not too long a period for such a conservative structure as higher education department; however, it is sufficient to mark this event.

The past ten years were intensive, but successful time, as I believe. There were ten PhD and three Doctoral theses defended at the department during these years. Five monographs (including "Error Correcting Coding and Security for Data Networks. Analysis of the Superchannel Concept" and "Modulation and Coding Techniques in Wireless Communications" published by John Wiley & Sons, Ltd), two collections of papers, hundreds of papers (including publications in more than 20 leading periodical journals) were published, more than 30 international patents were obtained.

The department was created with very young staff (surely, the author factors out of this statement himself and several of his friends), their activity and growing up determined the wide range of department's interests. Initially, the scientific interests of the department have been concentrated in the framework of theoretical informatics — error-correcting coding theory and public-key cryptography, but today the subjects of data transmission systems development, multiple access, network security, video data processing and compression are investigated. Today's reality with insufficient financing of higher school has had a significant impact on department development to require searching and performing works by orders from industrial companies. The biggest international companies such as Intel, Samsung, Siemens, EMC and others have become the customers of the department research and development works. This leads to increasing of applied investigations at the department.

The mentioned circumstances are reflected in the presented collection. Its subjects are very wide.

Significant place is dedicated to the papers on error-correcting coding. Error-correcting codes are universal mean to fight the impairments arise during data transmission, storage and processing. Codes were developed and are widely used for error-protection at the physical layer of the network, today they may be applied at transport and application layers, in the tasks of security, in organization of data storage systems. Papers on classical coding theory (A. V. Kozlov et al., S. V. Fedorenko) and on non-traditional coding applications (M. O. Alekseev, E. A. Krouk and D. A. Malichenko) are both presented in the collection.

The problem of reliable communication organization for the wide spectrum of modern applications remains one of the most actual in the area of modern information technologies development. Modern data transmission networks (mobile networks, sensor networks, automated systems for electro energy consumption control and accounting and so on) are from the one hand widely applied in industry and become important element of society's informational infrastructure, and from the other hand assume usage of special telecommunications technologies. For today not only the problems of hardware techniques development for implementing these technologies are not solved, but mentioned technologies themselves require further development. Significant part of present collection is

dedicated to the problems of data transmission in wireless networks. Both methods of improving the quality of message receiving (K. B. Gournov and G. S. Evseev) and methods of networks organization (M. A. Grankin et al.) are considered.

Video data portion increasing in the common value of traffic which is typical for 4—5 G communication systems leads to new tasks and possibilities arising in the area of video processing and transmission. Both problems of video data coding for improving its effectiveness (A. I. Veselov et al.) and for providing security (A. V. Afanasyeva et al.) are considered in the collection.

Also the questions of data storage systems organization are considered (E. M. Linsky et al., V. A. Bogatyrev et al.).

In conclusion, it should be noticed that this collection is third published by the department during the last five years, but it is the first published as special issue of "Priborostroenie" journal.

Head of Information Systems Security Department,
Doctor of Sciences, Professor, Honored Scientist of Russian Federation,
E. A. KROUK

КОДЫ, ИСПРАВЛЯЮЩИЕ ОШИБКИ

УДК 621.391

А. В. Козлов, Е. А. Крук, А. А. Овчинников

ПОДХОД К ПОСТРОЕНИЮ БЛОЧНО-ПЕРЕСТАНОВОЧНЫХ КОДОВ С МАЛОЙ ПЛОТНОСТЬЮ ПРОВЕРОК НА ЧЕТНОСТЬ

Предложены некоторые способы построения кодов с малой плотностью проверок на четность, приводятся конструкции кодов и результаты их использования для передачи в канале с аддитивным белым гауссовым шумом.

Ключевые слова: *LDPC-коды, коды Гилберта, блочно-перестановочные конструкции.*

Введение и основные понятия. Коды с малой плотностью проверок на четность (LDPC-коды) были предложены Р. Галлагером в 1963 г. [1], авторы статьи [2] доказали, что они обладают уникальными свойствами. LDPC-коды обеспечивают экспоненциальное убывание вероятности ошибки с увеличением длины кода при логарифмическом росте числа операций, необходимых для декодирования одного символа кодового слова. Однако долгое время исследования в области LDPC-кодов носили в основном теоретический характер. Это было связано, прежде всего, с тем, что высокая корректирующая способность этих кодов достигается при большой длине кодовых слов (порядка нескольких тысяч символов). Реализация декодеров таких кодов представляла трудности. В последние годы развитие микроэлектронных технологий вернуло интерес к исследованиям практических аспектов применения LDPC-кодов. Развитие новых стандартов связи, таких как IEEE 802.3an (10G Ethernet), IEEE 802.15.3c (передача данных на частоте 60 ГГц), IEEE 802.11n (WiFi), IEEE 802.16e (WiMAX), а также систем хранения данных — многоуровневой флэш-памяти, магнитных носителей с высокой плотностью хранения информации, требующих обеспечения скоростей декодирования в несколько гигабит в секунду, — привело к необходимости поиска методов кодирования/декодирования, способных функционировать на таких скоростях при одновременном обеспечении требуемого уровня помехоустойчивости.

LDPC-код задается своей проверочной матрицей H, обладающей свойством разреженности, т.е. строки и столбцы матрицы содержат мало ненулевых позиций по сравнению с ее размерностью. Определим (n, γ, ρ)-код как линейный код длины n, каждый столбец и каждая строка проверочной матрицы которого содержит соответственно γ и ρ ненулевых позиций.

Минимальное расстояние Хэмминга рассматриваемых кодов, через которое определяется число исправляемых кодом ошибок, будем обозначать d_0. Расстояние LDPC-кодов, как правило, невелико, тем не менее эти коды показывают очень хорошие результаты. Связано это, с одной стороны, с хорошими спектральными свойствами кода, т.е. в коде присутствует лишь незначительное количество слов малого веса, а с другой — с особенностями работы декодера.

Итеративный алгоритм декодирования LDPC-кодов принимает решения по каждому символу в отдельности. Таким образом, даже при большом числе возникших в канале ошибок и принятии декодером неправильного решения о кодовом слове в целом вероятность ошибки на информационный бит для LDPC-кодов может оставаться достаточно низкой.

Несмотря на большое число публикаций [1—6] задача построения эффективных LDPC-кодов далека от своего решения. В настоящей статье предлагаются некоторые подходы к построению этих кодов.

Блочно-перестановочные конструкции. Наиболее общий подход к построению LDPC-кодов, предложенный еще в работе Р. Галлагера [1], — использование проверочной матрицы H, состоящей из блоков:

$$\mathrm{H}=\begin{bmatrix} \mathrm{H}_{1,1} & \mathrm{H}_{1,2} & \dots & \mathrm{H}_{1,\rho} \\ \mathrm{H}_{2,1} & \mathrm{H}_{2,2} & \dots & \mathrm{H}_{2,\rho} \\ \dots & \dots & \dots & \dots \\ \mathrm{H}_{\gamma,1} & \mathrm{H}_{\gamma,2} & \dots & \mathrm{H}_{\gamma,\rho} \end{bmatrix}. \qquad (1)$$

В качестве блоков $\mathrm{H}_{i,j}$ могут быть выбраны, например, матрицы перестановки, в каждой строке и столбце которых содержится ровно одна единица, и тогда такая конструкция задает регулярный LDPC-код. Наиболее часто в качестве блока рассматривается матрица циклической перестановки, степень которой задает параметр циклического сдвига. Например, коды такого семейства представлены в стандартах IEEE 802.16e и IEEE 802.11n.

В случае $\gamma=2$ такие коды становятся кодами Гилберта, исследованными в [6—8]:

$$\mathrm{H}_l=\begin{bmatrix} \mathrm{I}_m & \mathrm{I}_m & \mathrm{I}_m & \dots & \mathrm{I}_m \\ \mathrm{I}_m & \mathrm{C} & \mathrm{C}^2 & \dots & \mathrm{C}^{l-1} \end{bmatrix}, \qquad (2)$$

где I_m — единичная $(m\times m)$-матрица, а C — $(m\times m)$-матрица циклической перестановки. Такие коды имеют минимальное расстояние $d_0=4$, однако его можно повысить, выбрав другие степени C.

Теорема 1. Пусть H_l — матрица вида (2), $Z_l=\{0,1,\dots,l-1\}$ — множество вычетов по модулю $l-1$. Тогда в коде с проверочной матрицей H_l есть слово веса 2ω, если существуют наборы чисел $\{a_i\}$, $\{b_i\}$ такие, что выполняется равенство:

$$\sum_{i=0}^{\omega-1}(-1)^i\left(a_i-b_i\right)=0 \mod m,$$

где $a_i\in Z_l, b_i\in Z_l, a_0\neq b_0, a_{\omega-1}\neq b_{\omega-1}, a_i\neq a_{i-1}, b_i\neq b_{i-1}$.

Пользуясь этой теоремой, можно показать, что если $\{z_1,\dots,z_\rho\}$ — разностное (m, ρ, 1)-множество, тогда код с проверочной матрицей

$$\mathrm{H}=\begin{bmatrix} 0 & 0 & \dots & 0 \\ \mathrm{C}^{z_1} & \mathrm{C}^{z_2} & \dots & \mathrm{C}^{z_\rho} \end{bmatrix} \qquad (3)$$

имеет длину $n=m\rho$, скорость $R=\dfrac{m(\rho-2)+1}{m\rho}$ и минимальное расстояние $d_0=6$.

Обобщим конструкцию кодов Гилберта до случая $\gamma>2$:

$$\mathrm{H}_{s,l} = \begin{bmatrix} \mathrm{I}_m & \mathrm{I}_m & \mathrm{I}_m & \dots & \mathrm{I}_m \\ \mathrm{C}^0 & \mathrm{C}^1 & \mathrm{C}^2 & \dots & \mathrm{C}^{l-1} \\ \mathrm{C}^{i_0^{(3)}} & \mathrm{C}^{i_1^{(3)}} & \mathrm{C}^{i_1^{(3)}} & \dots & \mathrm{C}^{i_{l-1}^{(3)}} \\ \dots & \dots & \dots & \dots & \dots \\ \mathrm{C}^{i_0^{(s)}} & \mathrm{C}^{i_1^{(s)}} & \mathrm{C}^{i_2^{(s)}} & \dots & \mathrm{C}^{i_{l-1}^{(s)}} \end{bmatrix}, \quad (4)$$

где $\mathrm{H}_{s,l}$ — $(s \times l)$-матрица, $i_j^{(k)} \in \{0,\dots,m-1\}$. Так как одним из параметров LDPC-кода является длина минимального цикла в графе, соответствующем проверочной матрице, числа $i_j^{(k)}$ в любой полосе k не должны повторяться. Тогда множество $\left\{i_j^{(k)} : j = 0, ..., l-1\right\}$ задается перестановкой различных вычетов целых чисел по модулю m.

В этом случае кодовому слову соответствует набор связанных вложенных циклов (рис. 1, γ=3), поэтому добавление полос может обеспечить увеличение расстояния LDPC-кодов.

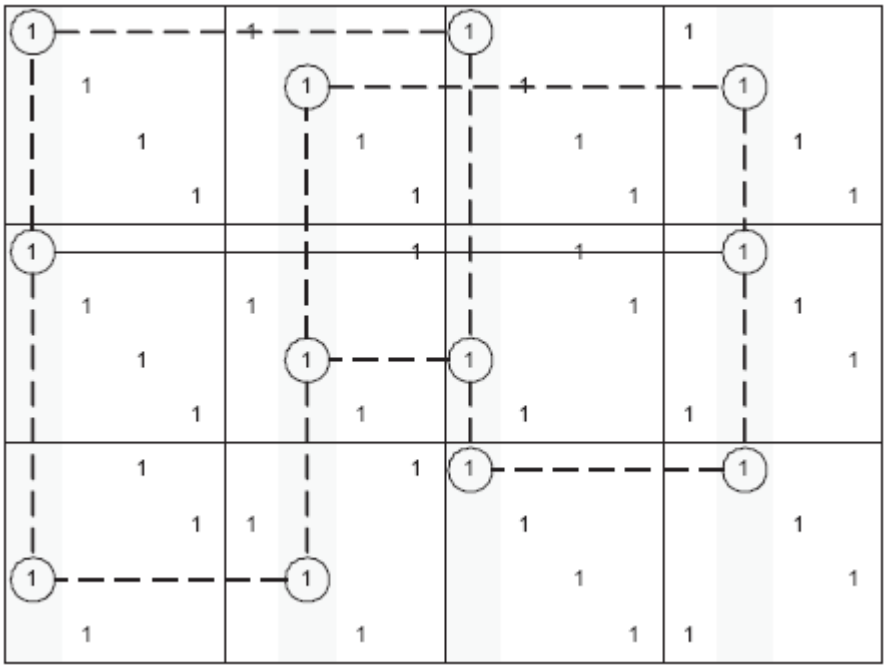


Рис. 1

В работе [9] предложено в качестве степеней матрицы циклической перестановки выбирать степени примитивного элемента матрицы Вандермонда:

$$\mathrm{H}_W = \begin{bmatrix} \mathrm{I}_m & \mathrm{I}_m & \dots & \mathrm{I}_m \\ \mathrm{I}_m & \mathrm{C} & \dots & \mathrm{C}^{\rho-1} \\ \dots & \dots & \dots & \dots \\ \mathrm{I}_m & \mathrm{C}^{\gamma-1} & \dots & \mathrm{C}^{(\gamma-1)(\rho-1)} \end{bmatrix}, \quad (5)$$

где $\rho \le m$. Такие коды имеют длину $n=m\rho$, и $\gamma + 1 \le d_0 \le 2m$.

Дальнейшую модификацию блочно-перестановочной конструкции (1) можно получить, если рассмотреть в качестве варианта заполнения блока $\mathrm{H}_{i,j}$ матрицей, состоящей из всех нулей. С одной стороны, это позволяет получать нерегулярные LDPC-коды и оптимизировать распределения весов строк и столбцов. С другой, как было показано на рис. 1, кодовым словам в блочно-перестановочной конструкции соответствуют множества вложенных циклов и

добавление нулевого блока может „разрывать“ эти циклы, уменьшая, таким образом, количество слов малого веса и улучшая спектр кода.

Выбор мест для расстановки нулевых блоков является отдельной задачей и зависит от конкретной проверочной матрицы. Несколько вариантов шаблонов, сохраняющих регулярную структуру матрицы, приведено на рис. 2.

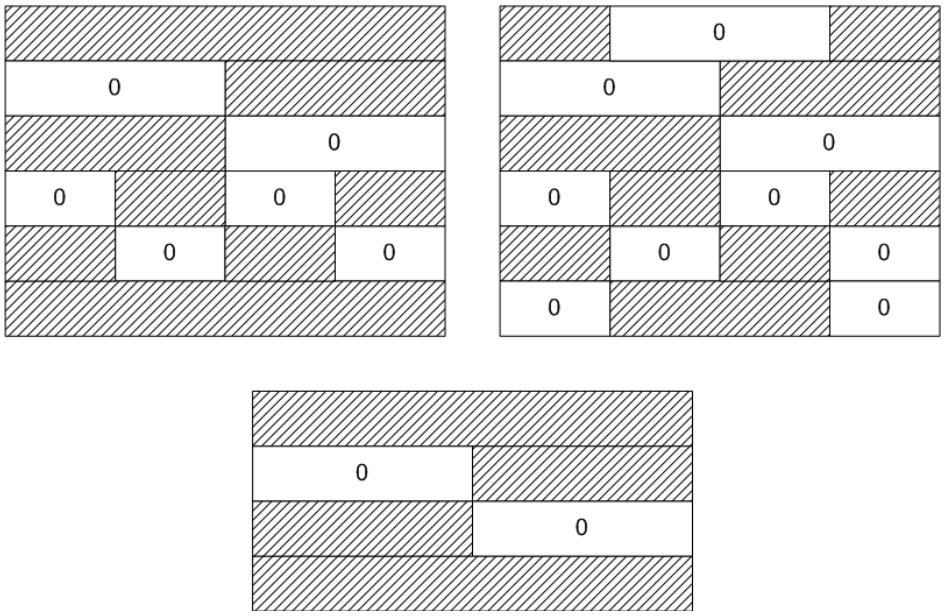


Рис. 2

На рис. 3, 4 приведены результаты моделирования описанных конструкций в канале с аддитивным белым гауссовым шумом (BER — вероятность ошибки на информационный бит; SNR — отношение сигнал/шум). На рис. 3 сравнивается классический код Гилберта (2) при $m = 29$ с кодом GGC (3), вторая полоса которого образована разностным множеством $\{0,5,7,18,19,28\}$. Код Гилберта имеет минимальное расстояние $d_0 = 4$, а у кода на основе (3) $d_0 = 6$.

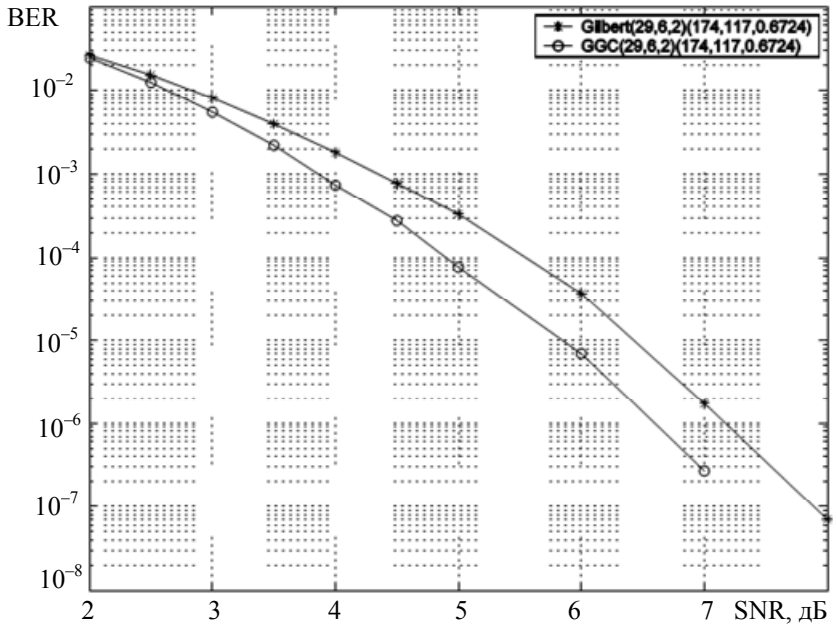


Рис. 3

На рис. 4 представлены кривые для кодов из четырех полос. Здесь W-LDPC обозначает выбор степеней в соответствии с матрицей Вандермонда (5) при $m = 79$, ρ=8, γ=4.

В качестве GGC использован код с проверочной матрицей

$$\mathrm{H} = \begin{bmatrix} 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 5 & 12 & 15 & 16 & 29 & 35 & 37 \\ 0 & 10 & 24 & 30 & 32 & 58 & 70 & 1 \\ 0 & 15 & 36 & 45 & 48 & 14 & 32 & 38 \end{bmatrix}, \qquad (6)$$

где $D = \{0,5,12,15,16,29,35,37\}$ — разностное множество, использованное для построения второй полосы проверочной матрицы. Третья и четвертая полосы получены как $2D \bmod 73$ и $3D \bmod 73$ соответственно. Выбранный таким образом код дает выигрыш над W-LDPC около 1 дБ при вероятности ошибки 10^{-6}.

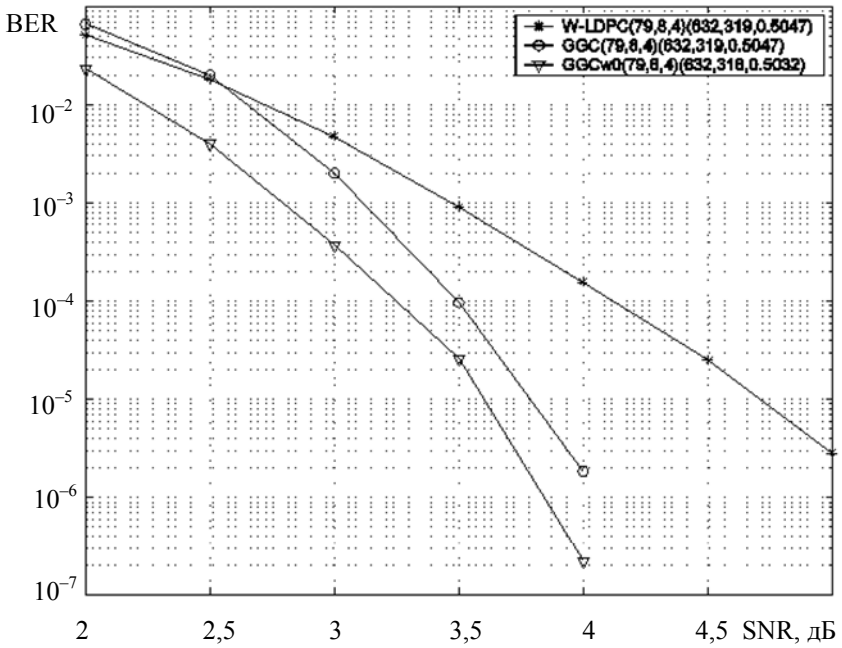


Рис. 4

Наконец, код GGCw0 соответствует проверочной матрице (6) с добавленными нулевыми блоками:

$$\mathrm{H} = \begin{bmatrix} 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & -1 & 12 & -1 & 16 & -1 & 35 & -1 \\ -1 & 10 & -1 & 30 & -1 & 58 & -1 & 1 \\ 0 & 15 & 36 & 45 & 48 & 14 & 32 & 38 \end{bmatrix},$$

где -1 соответствует нулевому блоку. Полученный код является регулярным LDPC-кодом с γ=3, он дает 0,5—0,25 дБ преимущества по сравнению с первоначальным GGC кодом при одновременном снижении сложности декодирования, так как содержит меньше ненулевых позиций в проверочной матрице. Однако этот выигрыш снижается с ростом отношения сигнал/шум, так как выигрыш в спектре кода, полученный за счет нулевых блоков, дает преимущество при достаточно высоком уровне шума, однако с ростом отношения сигнал/шум, когда ошибки в канале сами по себе редки, вероятность ошибки определяется минимальным расстоянием кода.

Заключение. В настоящей статье рассмотрены подходы к построению кодов с малой плотностью проверок на четность с использованием блочно-перестановочных конструкций. Приведены методики выбора блоков на основе разностных множеств, а также подход к улучшению спектральных свойств кода на основе использования нулевых блоков.

СПИСОК ЛИТЕРАТУРЫ

1. *Gallager R. G*. Low Density Parity Check Codes. Cambridge, MA: MIT Press, 1963.
2. *Зяблов В. В., Пинскер М. С*. Оценка сложности исправления ошибок низкоплотностными кодами Галлагера // Проблемы передачи информации. 1975. Т. XI(1). С. 23—26.
3. *Белоголовый А. В., Крук Е. А*. Многопороговое декодирование кодов с низкой плотностью проверок на четность // ИУС. 2005. № 1(14). С. 25—31.
4. *Овчинников А. А*. К вопросу о построении LDPC-кодов на основе Евклидовых геометрий // ИУС. 2005. № 1(14). С. 32—40.
5. *Козлов А. В*. Декодирование LDPC-кодов в дискретном канале flash-памяти // ИУС. 2007. № 5(30). С. 31—35.
6. *Gilbert E*. A problem in binary encoding // Proc. of the Symp. in Applied Mathematics. 1960. Vol. 10. P. 291—297.
7. *Krouk E., Semenov S*. Low-density parity-check burst error-correcting codes // Proc. of 2nd Intern. Workshop on Algebraic and combinatorial coding theory. Leningrad, 1990. P. 121—124.
8. *Овчинников А. А*. Об одном классе кодов, исправляющих пакеты ошибок // Тез. докл. 2-й Междунар. школы-семинара БИКАМП'99. СПб, 1999. С. 34—35.
9. *Kabatiansky G., Krouk E., Semenov S.* Error correcting coding and security for data networks: Analysis of the superchannel concept. Wiley, 2005.

Сведения об авторах

Александр Владимирович Козлов — Санкт-Петербургский государственный университет аэрокосмического приборостроения, кафедра безопасности информационных систем; ведущий программист; E-mail: akozlov@vu.spb.ru

Евгений Аврамович Крук — д-р техн. наук, профессор; Санкт-Петербургский государственный университет аэрокосмического приборостроения, кафедра безопасности информационных систем; E-mail: ekrouk@vu.spb.ru

Андрей Анатольевич Овчинников — канд. техн. наук, доцент; Санкт-Петербургский государственный университет аэрокосмического приборостроения, кафедра безопасности информационных систем; E-mail: mldoc@vu.spb.ru

Рекомендована кафедрой
№ 51 безопасности информационных систем

Поступила в редакцию
01.02.13 г.

УДК 004.056.2

М. О. АЛЕКСЕЕВ

НИЖНЯЯ ГРАНИЦА ДЛИНЫ СИСТЕМАТИЧЕСКИХ РАВНОМЕРНО НАДЕЖНЫХ КОДОВ

Приведены основные определения надежных кодов, обнаруживающих ошибки, указана область их применения. Выведена нижняя граница длины систематических R-равномерно надежных кодов.

Ключевые слова: *нелинейный код, надежный код, нижняя граница, минимальная длина кода.*

Аппаратные реализации криптографических алгоритмов могут быть уязвимы к так называемым атакам по сторонним каналам [1, 2]. Такие атаки основаны на изучении и последующем анализе физических особенностей работы криптосхем, что может привести к вычислению секретного ключа. Анализируемые характеристики аппаратной реализации могут быть

различны: энергопотребление, время выполнения операций, работа схемы в условиях воздействия помех.

В работе [3] описан метод дифференциального криптоанализа, позволяющий вычислять значение секретного ключа, если возможно задать разности между входными последовательностями на определенных этапах блокового DES-подобного шифра. Этот метод применяется для большинства симметричных блоковых шифров, включая AES (например, [4]).

Одну из наиболее серьезных угроз для криптосхем представляет комбинирование атаки с привнесением помех и дальнейшего дифференциального анализа. Внося помехи в определенные участки схемы, злоумышленник может контролировать выходы атакуемых блоков алгоритма, что значительно увеличивает вероятность успешного взлома устройства [5].

В ситуации, когда атакующий контролирует возникающие в устройстве ошибки, классические методы защиты аппаратных схем, основанные на дублировании оборудования и использовании линейных помехоустойчивых кодов, не могут обеспечить требуемый уровень защиты информации. Преодолеть эту проблему позволяют надежные коды, обнаруживающие ошибки. Использование таких кодов дает возможность значительно снизить вероятность успешного проведения рассматриваемой атаки.

Надежные коды также могут применяться в каналах, в которых конфигурация возникающих ошибок не может быть предсказана заранее, например, в системах, подверженных воздействию радиации, заряженных частиц и других факторов. Кроме того, надежные коды, обнаруживающие ошибки, применяются в схемах надежного разделения секрета и смежных с ними областях [6].

Надежным называется код, для которого не существует необнаруживаемых ошибок, т.е. любая ошибка выявляется с заданной вероятностью.

Пусть $C \in GF(p^n)$ является (n, M)-кодом, где $M = |C|$.

Определение 1. Код C называется *надежным*, если значение вероятности $Q(e)$ необнаружения ошибки e меньше единицы для всех ненулевых e:

$$Q(e) = \frac{|\{w \mid w \in C, w + e \in C\}|}{|C|} < 1, \; e \neq 0,$$

где $w, e \in GF(p^n)$.

На практике наиболее востребованы систематические надежные коды, поскольку они обеспечивают минимальную задержку декодирования — это является одним из основных требований к проектированию аппаратных схем. В настоящей статье рассматриваются только систематические коды, для длины которых и будет выведена нижняя граница.

Определение 2. Код C называется *равномерно надежным* к вероятности обнаружения ошибки, если вероятность $Q(e)$ постоянна и не зависит от ненулевого вектора e:

$$Q(e) = \frac{|\{w \mid w \in C, w + e \in C\}|}{|C|} = \text{const} < 1, \; e \neq 0.$$

Равномерно надежные коды достаточно хорошо изучены, это наиболее используемый вид надежных кодов благодаря простоте их построения. Проверочные символы таких кодов вычисляются с помощью нелинейных функций, при этом кодовое слово c представляет собой конкатенацию информационной части x и проверочных символов $y = f(x)$, где $f(\cdot)$ — используемая нелинейная функция. Более подробно эти коды описаны в работе [7]. На данный момент хорошо исследованы классы функций, обладающих высокой степенью нелинейности [8].

Определение 3. *R-надежным кодом* называется код, у которого $R = \max |\{w \mid w \in C, w + e \in C\}|$ для всех $e \neq 0$.

Очевидно, что вероятность обнаружения ошибки для *R*-равномерно надежного кода определяется как $P_{\text{det}} = 1 - R/M$.

Необходимо отметить, что для кодов над полем с характеристикой 2 наименьшим достижимым значением *R* является 2 (в силу идентичности операций сложения и вычитания), для других полей — $R = 1$.

Исследуем минимальную длину (обозначим ее через *n*) систематического *R*-равномерно надежного кода. Пусть *k* — размерность кода, т.е. $p^k = M$. В силу равномерной надежности кода число различных разностей между кодовыми словами составляет $\frac{M(M-1)}{R}$. Каждая из этих разностей является элементом поля $GF(p^n)$, над которым построен код. Следовательно, поле должно содержать не менее $\frac{M(M-1)}{R}$ элементов. Кроме того, для систематического кода p^{n-k} элементов поля не могут быть разностями между кодовыми словами, потому что разность систематических частей кодовых слов не может равняться $0 \in GF(p^k)$. Для такого кода только $p^n - p^{n-k}$ элементов поля могут являться разностями кодовых слов, и их должно быть не менее $\frac{M(M-1)}{R}$. Из этого утверждения можно получить нижнюю границу длины систематического *R*-равномерно надежного кода:

$$p^n - p^{n-k} \geq \frac{M(M-1)}{R},$$

$$p^n(1 - p^{-k}) \geq \frac{M(M-1)}{R},$$

$$P^n\left(\frac{M-1}{M}\right) \geq \frac{M(M-1)}{R},$$

$$p^n \geq \frac{M^2}{R},$$

$$n \geq \left\lceil \log_p \frac{M^2}{R} \right\rceil.$$

Легко заметить, что при $p = 2$ и $R = 2$ $n \geq 2k - 1$. При $k = 2$ ($n \geq 2k - 1 = 3$) примерами кодов, лежащих на этой границе, являются $C_1 = \{(00|1), (01|0), (10|0), (11|1)\}$ и $C_2 = \{(00|0), (01|1), (10|1), (11|1)\}$ над $GF(2^3)$, где символ „|“ разделяет информационную и проверочную части слова соответственно. Данные коды являются равномерно надежными систематическими с $R = 2$ и $Q(e) = 1 - 2/4 = 0,5$, являясь при этом кодами с минимальной возможной длиной.

Для сравнения, в работе [9] были предложены конструкции кодов над полем $GF(2^n)$ с $R = 2$ для любых *k*. Коды такой конструкции обладают скоростью $1/2$, т.е $n = 2k$. Представленные коды C_1 и C_2 для $k = 2$ обладают меньшей избыточностью при сохранении той же вероятности обнаружения ошибки $P_{\text{det}} = 0,5$.

Данная граница может быть использована для оценки вводимой избыточности надежных кодов. Условие применимости данной границы следующее: параметр *R* должен делить величину *M*(*M*–1). В общем случае задача построения оптимальных надежных кодов, соответствующих нижней границе, является открытой.

СПИСОК ЛИТЕРАТУРЫ

1. *Беззатеев С. В., Литвинов М. Ю., Трояновский Б. К.* Использование помехоустойчивых кодов для шифрации видеоинформации // ИУС. 2007. № 5(30). С. 23—26.

2. *Koeune F., Quisquater J. J.* Side Channel Attacks. Scientific Report. K2Crypt, 2002.

3. *Biham E., Shamir A.* Differential Cryptanalysis of DES-like Cryptosystems. The Weizmann Institute of Science, Department of Applied Mathematics. July 19, 1990.

4. *Dusart P., Letourneux G., Vivolo O.* Differential Fault Analysis on AES // Cryptology ePrint Archive. Report 2003/010.

5. *Kulikowski K. J., Karpovsky M. G., Taubin A.* Robust Codes and Robust, Fault Tolerant Architectures of the Advanced Encryption Standard // J. of System Architecture. 2007. Vol. 53. P. 138—149.

6. *Cramer R., Dodis Y., Fehr S., Padry C., Wichs D.* Detection of Algebraic Manipulation with Applications to Robust Secret Sharing and Fuzzy Extractors // Advances in Cryptology. Eurocrypt Lecture Notes in Computer Science. 2008. Vol. 4965. P. 471—488.

7. *Akdemir K. D., Wang Z., Karpovsky M. G., Sunar B.* Design of Cryptographic Devices Resilient to Fault Injection Attacks Using Nonlinear Robust Codes // Fault Analysis in Cryptography. 2011.

8. *Тужилин М. Э.* Почти совершенные нелинейные функции // ПДМ. 2009. № 3. С. 14—20.

9. *Kulikowski K., Karpovsky M. G.* Robust Correction of Repeating Errors by Nonlinear Codes // Communications. IET. 2011. Vol. 5, N 4. P. 2317—2327.

Сведения об авторе

Максим Олегович Алексеев — аспирант; Санкт-Петербургский государственный университет аэрокосмического приборостроения, кафедра аэрокосмических компьютерных технологий; E-mail: alexeevmo@gmail.com

Рекомендована кафедрой
№ 51 безопасности информационных систем

Поступила в редакцию
01.02.13 г.

УДК 621.391

С. В. ФЕДОРЕНКО

МОДИФИКАЦИЯ АЛГОРИТМА ГЕРЦЕЛЯ—БЛЕЙХУТА

Рассматриваются классический алгоритм Герцеля—Блейхута вычисления дискретного преобразования Фурье над конечным полем, а также его модификации. Показано, что модифицированный алгоритм относится скорее к классу быстрых алгоритмов вычисления дискретного преобразование Фурье, чем к классу полубыстрых.

Ключевые слова: *дискретное преобразование Фурье, быстрое преобразование Фурье, сложность алгоритма, быстрый алгоритм, полубыстрый алгоритм, конечное поле.*

Быстрый алгоритм — это вычислительная процедура, которая значительно сокращает число необходимых операций сложения и умножения по сравнению с прямым метод вычисления. Быстрое преобразование Фурье (БПФ) — это метод вычисления n-точечного преобразования, который использует около $n \log n$ операций умножения и около $n \log n$ операций сложения в поле вычисления преобразования Фурье [1].

Полубыстрый алгоритм — это вычислительная процедура, позволяющая значительно сократить число необходимых операций умножения по сравнению с прямым метод вычисления, не уменьшая число сложений. Полубыстрый алгоритм вычисления преобразования Фурье —

это метод вычисления n-точечного преобразования Фурье, который использует около $n \log n$ операций умножения и около n^2 операций сложения в поле вычисления преобразования Фурье [1].

Дискретное преобразование Фурье (ДПФ) длины n вектора $\mathbf{f} = (f_i)$, $i \in [0, n-1]$, $n \mid (q-1)$, в конечном поле $GF(q)$ есть вектор $\mathbf{F} = (F_j)$,

$$F_j = \sum_{i=0}^{n-1} f_i \alpha^{ij}, \qquad j \in [0, n-1],$$

где α (ядро ДПФ) является элементом порядка n в конечном поле $GF(q)$.

Далее предполагается, что длина n-точечного преобразования Фурье над $GF(2^m)$ есть $n = 2^m - 1$. Произвольный вектор $\mathbf{f} = (f_i)$, $i \in [0, n-1]$, свяжем с многочленом $f(x) = \sum_{i=0}^{n-1} f_i x^i$ и получим $F_j = f(\alpha^j)$. Поле вычисления преобразования Фурье есть конечное поле $GF(2^m)$, а α — примитивный элемент поля $GF(2^m)$. Все логарифмы вычисляются по основанию 2.

Алгоритм Герцеля—Блейхута. Рассмотрим модификацию [2, 3] алгоритма для вычисления ДПФ над конечными полями [4, 5].

Алгоритм Герцеля—Блейхута состоит из двух шагов. На первом шаге выполняется деление с остатком многочлена $f(x)$ на каждый минимальный многочлен $M_k(x)$:

$$\begin{cases} f(x) = M_k(x)\, q_k(x) + r_k(x), \\ \deg r_k(x) < \deg M_k(x) = m_k, \\ k \in [0, l-1], \end{cases}$$

где $r_k(x) = \sum_{j=0}^{m_k-1} r_{j,k} x^j$, l — число двоичных классов сопряженности.

На втором шаге выполняется вычисление значений $r_k(x)$ во всех элементах конечного поля:

$$\begin{cases} F_i = f(\alpha^i) = r_k(\alpha^i) = \sum_{j=0}^{m_k-1} r_{j,k} \alpha^{ij}, \\ i \in [0, n-1], \end{cases}$$

где элемент α^i — корень минимального многочлена $M_k(x)$.

Алгоритм Герцеля—Блейхута принадлежит к классу полубыстрых и имеет сложность порядка $n \log n$ операций умножения и порядка n^2 операций сложения над элементами поля $GF(2^m)$ [2].

Модификация первого шага алгоритма Герцеля—Блейхута. В работе [6] предложен способ улучшения первого шага алгоритма Герцеля—Блейхута, в ней показано, что асимптотическая сложность этого шага составляет $O(n\ (\log n)^2 \log \log n)$ операций над элементами поля $GF(2^m)$.

Построим дерево делителей. На самом нижнем уровне находятся l минимальных многочленов. Предположим, что l есть степень числа 2, иначе дополним множество минимальных многочленов до степени числа 2 фиктивными многочленами, равными единице. На следующем уровне располагаются $l/2$ произведений пар минимальных многочленов. Далее на

каждом уровне располагаются произведения пар многочленов из предыдущего уровня. В корне дерева находится двучлен $x^{2^m-1}-1$. Алгоритм состоит в последовательном вычислении остатков от деления, начиная с исходного многочлена $f(x)$, на все делители из каждого уровня дерева сверху вниз. Известно, например [7], что сложность деления многочлена степени $2s$ на многочлен степени s имеет порядок $D(s)=O(s\ \log s\ \log\log s)$ операций. Из очевидного неравенства $pD(s/p)\le D(s)$ следует, что для каждого уровня дерева сложность вычисления всех остатков от делений не превышает $D(n)$. Число уровней в дереве делителей есть $\log\ l=O\left(\log\ \frac{n}{m}\right)=O(\log\ n)$. Тогда общее число операций имеет порядок $D(n)\ \log\ l=O(n\ (\log n)^2\ \log\log n)$. Заметим, что приведенная оценка сложности алгоритма явно завышена.

Модификация второго шага алгоритма Герцеля—Блейхута. Предложим вариант улучшения второго шага алгоритма Герцеля—Блейхута. Из работ [8, 9] следует, что второй шаг алгоритма можно свести к вычислению l m-точечных циклических сверток. Конструктивный метод построения циклических сверток для длин $m=2^i$, $i\ge 0,$ имеющий сложность порядка $\frac{1}{2}\ m\log m$ операций умножения и $m\log m$ операций сложения, введен автором настоящей статьи. Таким образом, верхняя оценка асимптотической сложности второго шага алгоритма имеет порядок $O(l\ m^2)=O\left(\frac{n}{m}\ m^2\right)=O(n\ \log n)$ операций сложения и умножения над элементами поля $GF(2^m)$.

Заключение. В работе показано, что модификация алгоритма Герцеля—Блейхута с общей сложностью порядка $O(n\ (\log n)^2\ \log\log n)$ операций над элементами поля $GF(2^m)$ относится скорее к классу быстрых алгоритмов вычисления ДПФ, чем к классу полубыстрых алгоритмов.

Автор выражает признательность фонду имени Александра фон Гумбольдта (Германия) за многолетнюю поддержку научных исследований.

СПИСОК ЛИТЕРАТУРЫ

1. *Blahut R. E.* Algebraic Codes on Lines, Planes, and Curves: An Engineering Approach. Cambridge, UK: Cambridge University Press, 2008. 543 p.
2. *Блейхут Р.* Теория и практика кодов, контролирующих ошибки. М.: Мир, 1986. 576 с.
3. *Blahut R. E.* Fast Algorithms for Signal Processing. Cambridge, UK: Cambridge University Press, 2010. 453 p.
4. *Goertzel G.* An algorithm for the evaluation of finite trigonometric series // The American Mathematical Monthly. 1958. Vol. 65, N 1. P. 34—35.
5. *Блейхут Р.* Быстрые алгоритмы цифровой обработки сигналов. М.: Мир, 1989. 448 с.
6. *Trifonov P.* On the additive complexity of the cyclotomic FFT algorithm // Proc. of the IEEE Information Theory Workshop. Lausanne, Switzerland, 2012. P. 537—541.
7. *von zur Gathen J., Gerhard J.* Modern computer algebra. Cambridge, UK: Cambridge University Press, 1999.
8. *Трифонов П. В., Федоренко С. В.* Метод быстрого вычисления преобразования Фурье над конечным полем // Проблемы передачи информации. 2003. Т. 39, № 3. С. 3—10.
9. *Fedorenko S. V.* The discrete Fourier transform over a finite field with reduced multiplicative complexity // Proc. of the IEEE Intern. Symp. on Information Theory. St. Petersburg, 2011. P. 1200—1204.

Сведения об авторе

Сергей Валентинович Федоренко — д-р техн. наук, профессор; Санкт-Петербургский государственный университет аэрокосмического приборостроения, кафедра безопасности информационных систем; E-mail: sfedorenko@ieee.org

Рекомендована кафедрой
№ 51 безопасности информационных систем

Поступила в редакцию
01.02.13 г.

УДК 621.391

А. И. Акмалходжаев, А. В. Козлов

НОВЫЙ АЛГОРИТМ СПИСОЧНОГО ДЕКОДИРОВАНИЯ ТУРБОКОДОВ

Рассматривается метод параллельного списочного турбодекодирования, в рамках которого предложен оконный списочный декодер сверточного кода с мягким выходом. Предложенный алгоритм позволяет добиться выигрыша на словах не только малой, но и большой длины.

Ключевые слова: *турбокоды, турбодекодирование, списочное декодирование.*

Введение. Декодирование турбокода — это итеративный процесс, в ходе которого два декодера сверточного кода с мягким выходом обмениваются значениями оценок внешних вероятностей [1—3]. Обычно достаточно 8—10 итераций для того, чтобы изменения оценок декодированных символов стали незначительными, дальнейшее итерирование декодера практически не приводит к уменьшению вероятности ошибки. Одним из способов снижения вероятности ошибки является использование списочного декодирования.

В настоящей работе рассматривается новый метод списочного декодирования турбокодов, основанный на списочном декодере сверточного кода с мягким выходом. Каждый мягкий выход является последовательностью априорных вероятностей, которые подаются на вход независимых турбодекодеров (рис. 1). Предложенный метод обеспечивает сходимость разных декодеров к различным кодовым словам, из которых затем выбирается подходящее. Список декодированных слов с мягкими решениями может быть сгенерирован с использованием первого, второго или обоих сверточных кодов.

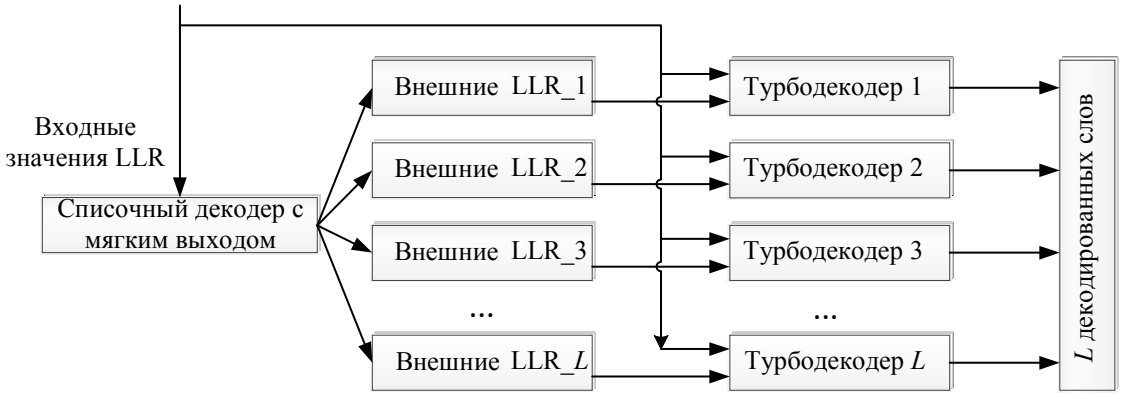


Рис. 1

Впервые подход с использованием списочного декодирования с мягким выходом был рассмотрен в работе [4], в рамках этого подхода был предложен алгоритм декодирования сверточного кода. Однако его использование давало выигрыш лишь на малых длинах, в то время как на больших длинах выигрыш был незначителен. Предложенный в настоящей рабо-

те оконный алгоритм списочного декодирования сверточного кода с мягким выходом позволяет достичь выигрыша и на больших длинах.

Оконный списочный декодер сверточного кода с мягким выходом. Оконный алгоритм строит на участках решетки (окнах) мягкие списки размером L, которые в дальнейшем используются при получении априорных вероятностей для всего информационного слова. Для получения такого списка в предложенном алгоритме используется оконный списочный декодер Витерби и оконный MAP-декодер. Так как в текущем окне не известны начальные и конечные состояния пути, для оконного алгоритма Витерби вводят понятие суффикса (рис. 2). Известно, что если длина суффикса N_{suff} равна 4—5 длинам кодового ограничения сверточного кода, то выжившие пути в конце суффикса, полученные с помощью алгоритма Витерби, с большой вероятностью имеют общий корень в конце окна (N_{win}). Таким образом, суффикс позволяет найти состояние в конце окна, в то время как начальные состояния равновероятны. Пусть t — номер начальной секции окна. Тогда оконный списочный алгоритм Витерби выглядит следующим образом.

1. Выполним параллельный списочный алгоритм Витерби [5, 6] на участке решетки от секции t до $t + N_{\text{win}} + N_{\text{suff}}$. В результате работы этого алгоритма получим для каждого состояния окна и суффикса L лучших путей.

2. Найдем путь с наибольшей конечной метрикой в секции $t + N_{\text{win}} + N_{\text{suff}}$. Пусть S_t — его начальное состояние в окне, а $S_{t+N_{\text{win}}}$ — конечное.

3. Из состояния $S_{t+N_{\text{win}}}$ выполним обратный проход по решетке в окне для оставшегося $L-1$ пути.

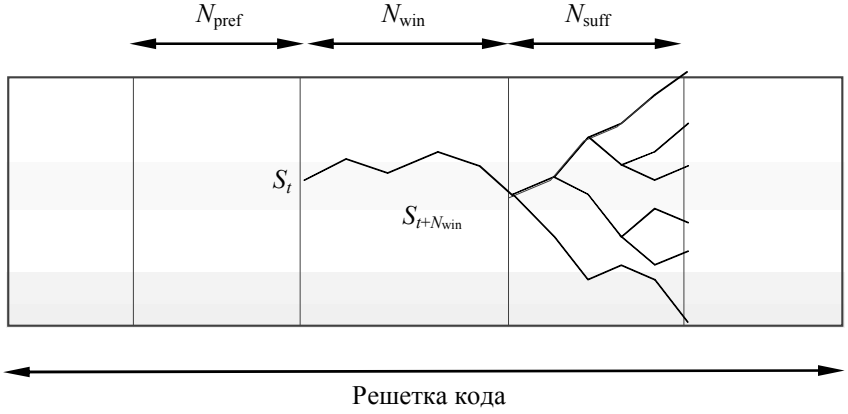


Рис. 2

В результате работы оконного списочного алгоритма получаются L путей в окне, которые могут начинаться в произвольном состоянии решетки, но заканчиваются в состоянии $S_{t+N_{\text{win}}}$.

Поскольку в MAP-алгоритме выполняется два прохода по решетке для нахождения прямых и обратных метрик, в оконном варианте помимо суффикса вводят префикс, который служит для более корректного вычисления метрик в окне (рис. 2), т.е. в оконном MAP [7] алгоритме расчет метрик начинается в секции $t - N_{\text{pref}}$ и заканчивается в секции $t + N_{\text{win}} + N_{\text{suff}}$, а начальные и конечные состояния равновероятны.

Используя полученные пути в окне и оконный MAP-алгоритм, можно получить список мягких решений, выполнив следующие шаги.

1. Найдем с помощью списочного оконного алгоритма Витерби L путей в решетке.

2. Определим первый элемент списка как результат работы алгоритма MAP в окне.

3. Обозначим как Γ_l все ребра, которые принадлежат l-му пути. Для нахождения l-го элемента списка:

— исключим в окне все ребра, которые принадлежат $l-1$ лучшему пути, но не принадлежат оставшимся $L-1$ путям, т.е. исключим все ребра из множества $\left(\bigcup_{i=1}^{l-1}\Gamma_i - \bigcup_{i=1}^{l-1}\left(\Gamma_l \bigcap \Gamma_i\right)\right)$;

— выполним MAP-алгоритм в окне с исключенными ребрами. Выходные надежности алгоритма и будут искомым элементом списка.

Удаление из решетки ребра лучших путей, которые будут учтены в соответствующих элементах списка, позволит рассмотреть менее вероятные решения. Это обеспечит схождение последующих процессов турбодекодирования к другим кодовым словам, среди которых, возможно, будет правильное.

Стоит отметить, что помимо MAP-алгоритма можно использовать его подоптимальные варианты, такие как Max-Log-MAP или Scaled-Max-Log-MAP [8].

Списочный декодер турбокода. Для того чтобы найти мягкое решение для всего информационного слова, решетка сверточного кода разбивается на равные отрезки. В каждом из отрезков с помощью описанного алгоритма находится список мягких решений, из которых в дальнейшем формируется мягкое решение для всего слова. Однако при разбиении слова на N окон с длиной списка L в каждом окне, при полном переборе элементов списка в каждом окне, общий размер списка равен L^N. Экспоненциальное увеличение размера списка не позволяет использовать полный перебор при нахождении общего списка, поэтому был предложен следующий подход к его уменьшению.

Рассмотрим окно j с длиной списка $L=2$. Вычислим евклидово расстояние между первым и вторым элементами списка:

$$\varepsilon_j = \sum_{i=1}^{N_{win}} \left(E_{1,j}^i - E_{2,j}^i\right)^2,$$

где $E_{1,j}$ и $E_{2,j}$ — первый и второй элементы списка соответственно.

Чем больше евклидово расстояние между векторами, тем с большей вероятностью соответствующие процессы турбодекодирования сойдутся к различным словам. Таким образом, в каждом окне вычисляется евклидово расстояние между элементами списка и оставляются лишь элементы с наибольшим расстоянием. В случае $L=2$ уменьшение размера списка в окне приведет к тому, что останется лишь его первый элемент и размер общего списка сократится в 2 раза.

Результаты моделирования. Предложенный метод анализировался путем моделирования (рис. 3) на примере турбокода LTE [9].

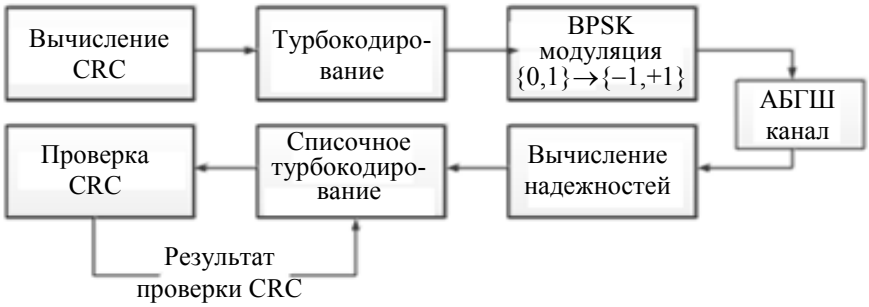


Рис. 3

Как видно из рисунка, информационное слово содержит код CRC, который используется для выбора правильного слова из списка. В качестве CRC используется полином CRC_B из стандарта 3GPP LTE [9].

Для вычисления списка мягких решений использовался первый компонентный код турбокода. Моделирование производилось для информационного слова длиной 512, в качестве

алгоритма декодирования турбокода и генерации списка был выбран алгоритм Scaled-Max-Log-MAP с весовым коэффициентом 0,75. Решетка сверточного кода была разделена на 8 окон по 64 секции в каждом. Размер списка был выбран равным 2, т.е. общий размер списка — 256. При моделировании учитывалась вероятность ошибки на информационное слово (FER).

Из результатов моделирования видно (рис. 4), что предложенный метод по сравнению с алгоритмом Scaled-Max-Log-MAP (кривая *1*) дает выигрыш порядка 0,19 дБ для полного списка. Кривые *2*—*5* характеризуют результаты моделирования для списочного декодера с уменьшенным размером списка: 16 (*2*), 32 (*3*), 64 (*4*) и 256 (*5*) слов. Заметное уменьшение длины списка лишь незначительно снижает производительность декодера — так, для списка длины 16 выигрыш равен 0,13 дБ.

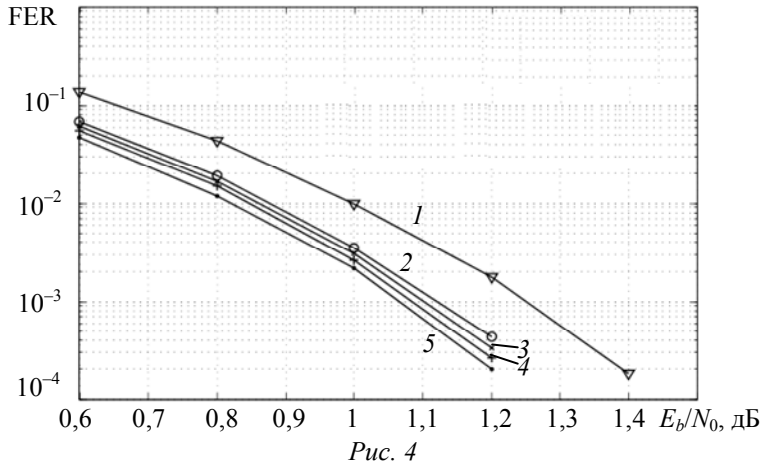


Рис. 4

Заключение. В настоящей работе рассмотрен новый метод списочного декодирования турбокодов, в рамках которого был предложен оконный алгоритм списочного декодирования сверточного кода с мягким выходом. Предложенный метод позволяет добиться выигрыша по сравнению с алгоритмом Scaled-Max-Log-MAP при длине информационного слова 512 вплоть до 0,19 дБ на полном списке. Также рассмотрен подход к уменьшению списка мягких решений на основе расстояния Евклида между элементами списка. Было показано, что при значительном уменьшении списка производительность декодера снизилась незначительно. На списках размером 16 и 32 выигрыш составляет 0,13 и 0,15 дБ соответственно.

СПИСОК ЛИТЕРАТУРЫ

1. *Козлов А. В.* Декодирование LDPC-кодов в дискретном канале flash-памяти // ИУС. 2007. № 5(30). С. 31—35.

2. *Белоголовый А. В., Крук Е. А.* Многопороговое декодирование кодов с низкой плотностью проверок на четность // ИУС. 2005. № 1(14). С. 25—31.

3. *Berrou C., Glavieux A., Thitimajshima P.* Near Shannon limit error-correcting coding: turbo codes // Proc. IEEE Intern. Conf. on Communications. Geneva, Switzerland, 1993. P. 1064—1070.

4. *Акмалходжаев А. И., Козлов А. В.* Списочное декодирование турбо кодов // СПИСОК-2012. Матер. Межвуз. науч. конф. по проблемам информатики. 2012. С. 194—199.

5. *Nill C., Sundberg C.-E. W.* List and Soft Symbol Output Viterbi Algorithms: Extensions and Comparisons // IEEE Transactions on Communications. 1995. Vol. 43, N 2. P. 277—287.

6. *Narayanan K. R., Stuber G. L.* List Decoding of Turbo Codes // IEEE Transactions on Communications. 1998. Vol. 46, N 6. P. 754—762.

7. *Bahl L., Cocke J., Jelinek F., Raviv J.* Optimal decoding of linear codes for minimizing symbol error rate // IEEE Transactions on Information Theory. 1974. Vol. 20. P. 284—287.

8. *Claussen H., Karimi H. R., Mulgrew B.* Improved max-log-map turbo decoding by maximization of mutual information transfer // EURASIP J. on Applied Signal Processing. 2005. P. 820—827.

9. 3GPP LTE TS 36.212 V8.3.0: “Evolved Universal Terrestrial Radio Access (E-UTRA); Multiplexing and channel coding”.

Сведения об авторах

Акмал Илхомович Акмалходжаев — Санкт-Петербургский государственный университет аэрокосмического приборостроения, кафедра безопасности информационных систем; программист; E-mail: Akmal.ilh@gmail.com

Александр Владимирович Козлов — Санкт-Петербургский государственный университет аэрокосмического приборостроения, кафедра безопасности информационных систем; ведущий программист; E-mail: akozlov@vu.spb.ru

Рекомендована кафедрой
№ 51 безопасности информационных систем

Поступила в редакцию
01.02.13 г.

УДК 004.056.2

М. О. Алексеев

НОВАЯ КОНСТРУКЦИЯ СИСТЕМАТИЧЕСКОГО НАДЕЖНОГО КОДА

Предложена конструкция систематического надежного кода. Представлена новая нелинейная функция для вычисления проверочных символов кода. Проанализирована надежность кода при обнаружении однонаправленных ошибок.

Ключевые слова: *нелинейная функция, надежный код, однонаправленные ошибки, показательная функция.*

Введение. Появление криптоатак, ориентированных на особенности реализации криптографических алгоритмов, требует разработки методов проектирования защищенных архитектур вычислительных устройств. Такие криптоатаки, получившие название „атаки по сторонним каналам“, основаны на сборе и анализе информации о физических особенностях криптографических модулей (как аппаратных, так и программных) [1, 2].

Одну из основных угроз для криптографических модулей представляют помехи, индуцируемые злоумышленником. Анализ работы устройства в условиях помех предоставляет атакующему дополнительную информацию, которая может быть использована для успешного взлома шифра [3].

Дублирование оборудования с последующим сравнением результатов его работы не обеспечивает надежной защиты от атак с привнесением помех. Если злоумышленник способен возбуждать помехи с достаточно высоким пространственным и временным разрешением, то наложение одинаковых помех на оба экземпляра атакуемого блока (исходного и дублирующего) приведет к необнаруживаемой ошибке на выходе устройства. Очевидно, что даже многократного дублирования защищаемого блока недостаточно в такой ситуации.

Линейные помехоустойчивые коды, часто применяемые в аппаратных схемах для контроля ошибок, также не обеспечивают необходимый уровень защиты устройства. Если злоумышленник способен контролировать возникающие ошибки, то, генерируя помехи, приводящие к любой из $q^k - 1$ необнаруживаемых ошибок, соответствующих ненулевым кодовым словам, он обеспечивает ошибочный выход атакуемого блока вне зависимости от поступающих данных.

Надежные коды. Обеспечить защиту от описанной модели атаки позволяют нелинейные коды. Коды, названные надежными, обеспечивают обнаружение любой ошибки с заданной вероятностью. В настоящей работе приведено лишь определение надежных кодов; более подробно эти коды приведены в работах [4—6].

Пусть $C \in GF(p^n)$ является (n, M)-кодом, где $M = |C|$.

Код C называется надежным по отношению к его вероятности обнаружения ошибки, если вероятность $Q(e)$ необнаружения ошибки e меньше единицы для всех ненулевых e:

$$Q(e) = \frac{|\{w \mid w \in C, w+e \in C\}|}{|C|} < 1,\ e \neq 0,$$

где $w, e \in GF(p^n)$.

Через R обозначается мощность максимального пересечения кода C и его сдвигов $C+e$, $e \in GF(p^n)$, $e \neq 0$. Другими словами, R — максимальное число кодовых слов кода C, при наложении на которые фиксированной ошибки $e \neq 0$ получаются кодовые слова. Очевидно, что в этом случае ошибка не может быть обнаружена. Отсюда следует, что вероятность обнаружения ошибки P_{det} ограничена снизу выражением $P_{\text{det}} \geq 1 - R/M$, т.е. любая ошибка может быть обнаружена с вероятностью не ниже $1 - R/M$.

Над полем с характеристикой $p > 2$ может быть построен код, у которого $R = 1$. В случае, когда $p = 2$ (наиболее востребовано с точки зрения реализации), минимальным возможным параметром является $R = 2$ [4].

На практике наиболее удобно использовать систематические коды, так как при защите аппаратных блоков требуется высокая скорость обработки данных.

Согласно теореме 2 из работы [5], конкатенация информационной $x \in GF(2^k)$ и проверочной $y = f(x)$, $y \in GF(2^r)$ части образует кодовые слова $(x \mid y = f(x))$ надежного систематического кода, параметры которого определяются следующим образом: $R = 2^k P_f$, $n = k + r$, $|M| = 2^k$. Параметр P_f определяет степень нелинейности функции.

Надежные коды используются как для защиты криптографических модулей, так и для защиты систем хранения. Избыточность, необходимая для защиты аппаратных схем, заключается в дублировании оборудования и добавлении блоков вычисления проверочных символов. В случае проектирования защищенного модуля памяти размер требуемой памяти увеличивается в n/k раз.

Нелинейная показательная функция. Согласно статье [7], функция $f(x) = u^x \bmod p$ (где x — элемент абелевой группы $G = \{0, ..., p-1\}$, p — простое число, а u — элемент порядка q из поля $GF(p)$) является разностно $\left(\frac{p-1}{q} + 1\right)$-равномерным отображением.

Исследуем степень нелинейности этой функции. Пусть $a,\ b \in G$ и $a \neq 0$. Тогда уравнение

$$u^{(x+a) \bmod p} - u^x = b \tag{1}$$

эквивалентно

$$\begin{cases} u^{x+a} - u^x = b \text{ и } 0 \leq x \leq p-a-1 \\ \text{или} \\ u^{x+a-p} - u^x = b \text{ и } p-a \leq x \leq p-1. \end{cases} \tag{2}$$

Из уникальности решения x уравнения

$$u^{x+a} - u^x = b$$

по модулю q следует, что первое уравнение (2) имеет не более $\left\lceil \frac{p-a}{q} \right\rceil$ корней в G, второе — не более $\left\lceil \frac{a}{q} \right\rceil$. Следовательно, уравнение (1) имеет не более

$$\left\lceil \frac{p-a}{q} \right\rceil + \left\lceil \frac{a}{q} \right\rceil = \frac{p-1}{q} + 1$$

решений в G.

Выбрав в качестве u примитивный элемент поля $GF(p)$, можно получить из (1) уравнение вида $f(x+a)-f(x)=b$, которое имеет не более двух корней. Оно аналогично проверочному выражению надежных кодов. С помощью этого соотношения определяется наличие ошибок.

Стоит отметить, что при использовании в качестве u примитивного элемента поля $f(x)=u^x \bmod p$ становится почти совершенно нелинейной функцией с $P_f = 2/p$.

Таким образом, конкатенацией информационной x и проверочной части $y=u^x \bmod p$ получаем систематический надежный код со следующими параметрами: $k=\lceil \log_2 p \rceil$, $r=k$, $n=2k$, $R=2$.

Однонаправленные атаки. Известные 2-надежные коды в качестве совершенно нелинейных используют степенные функции и функцию инвертирования в поле [6]. Эти коды являются надежными с заданной вероятностью обнаружения ошибок при аддитивной модели помехи.

Однако не всегда ошибки в устройстве могут быть описаны аддитивной моделью. Как показывает практика, для flash-памяти, оптических дисков и сетей характерна достаточно большая разница между вероятностями переходов $0 \to 1$ и $1 \to 0$ [8]. Зачастую используется допущение, что в таких системах возможен только один тип переходов. Подобные ошибки получили название асимметричных.

Исследования показали, что для некоторых систем хранения (LSI/VLSI ROM и RAM) характерны однонаправленные ошибки, отличающиеся от асимметричных тем, что оба перехода $0 \to 1$ и $1 \to 0$ возможны, но в каждом отдельном слове встречается только один тип перехода — один тип асимметричной ошибки. Математически такая ошибка может быть представлена как побитовая конъюнкция/дизъюнкция кодового слова c и некоторого вектора w, состоящего из нулей и единиц: переход $0 \to 1$ — $c \vee w$; переход $1 \to 0$ — $c \wedge w$.

При индуцировании помех криптоаналитиком (искусственном происхождении ошибки) также возможны асимметричные и однонаправленные модели ошибок. Возможность осуществлять переход всех битов в 0 позволяет криптоаналитику успешно внедрять необнаруживаемые ошибки даже при использовании существующих надежных кодов.

Рассмотрим пример. Для защиты блока памяти используется 2-надежный код $(x \mid y = x^3)$ над полем $GF(p^n)$. Допустим, злоумышленник осуществил атаку, которая привела к переходу $0 \to 0$, $1 \to 0$ для всех битов кодового слова. Тогда проверочное уравнение $f(x \wedge 0) = f(x) \wedge 0$ при $f(x)=x^3$ будет выполняться при любых x и атака не будет обнаружена. Аналогична ситуация и для функции инвертирования в поле, так как она доопределяется тем, что $0^{-1}=0$ [5].

Предлагаемая конструкция кода обеспечивает защиту даже при однонаправленных ошибках. Это обеспечивается тем, что в общем случае $u^0 \neq 0$ и $u^{p-1} \neq p-1$.

Наиболее эффективным сценарием криптоатаки на данный надежный код представляется приведение данных к кодовым словам наименьшего или наибольшего веса Хемминга (в зависимости от типа перехода ошибки). Например, наименьшим весом обладает слово $(0 \mid u^0 = 1)$. Злоумышленник может обнулить все биты информационной части кодового слова, а у проверочной части оставить нетронутым только младший бит. Далее, в зависимости от значения младшего бита выполняется (1) или не выполняется (0) проверочное соотношение. Таким образом, вероятность необнаружения ошибки при однонаправленной атаке ограничена сверху значением 0,5 (при равномерном распределении сообщений). Тут необходимо отме-

тить, что для успешного проведения большинства типов атак с привнесением ошибок требуется внедрение заданного количества необнаруженных ошибок. В такой ситуации вероятность необнаружения ошибки убывает экспоненциально с ростом числа атак.

Таким образом, предлагаемый код обеспечивает надежную защиту не только от ошибок и атак, описываемых аддитивной моделью, но и от воздействий, описываемых моделью однонаправленных ошибок.

Практическая значимость. Очевидно, что процедуры кодирования и декодирования предлагаемого кода обладают более высокой вычислительной сложностью, нежели существующие кодовые конструкции. Однако если криптографический модуль использует алгоритм Диффи—Хеллмана для генерации секретного ключа между двумя устройствами, то модули, выполняющие возведение в степень по модулю простого числа, могут быть использованы и для процедур кодирования и декодирования предлагаемого кода. Более того, в обоих случаях требуется возведение фиксированного основания в степень, значение которой является переменной величиной. Поэтому могут быть применены эффективные алгоритмы возведения в степень по модулю простого числа, например, метод Евклида для фиксированного основания [9].

Также возможно эффективное использование данного надежного кода в криптографических модулях, использующих возведение в степень при шифровании и дешифровании, примерами являются шифры RSA и Эль-Гамаля, а также электронные цифровые подписи на их основе. Использование уже реализованных в устройстве блоков сводит аппаратные затраты к минимуму.

СПИСОК ЛИТЕРАТУРЫ

1. *Беззатеев С. В., Литвинов М. Ю., Трояновский Б. К.* Использование помехоустойчивых кодов для шифрации видеоинформации // ИУС. 2007. №5(30). С. 23—26.

2. *Zhou Y., Feng D.* Side-channel Attacks: Ten Years After Its Publication and the Impacts on Cryptographic Module Security Testing. 2005 [Электронный ресурс]: <http://eprint.iacr.org/2005/388/>.

3. *Biham E., Shamir A.* Differential Cryptanalysis of DES-like Cryptosystems. The Weizmann Institute of Science, Department of Applied Mathematics, 1990.

4. *Akdemir K. D., Wang Z., Karpovsky M. G., Sunar B.* Design of Cryptographic Devices Resilient to Fault Injection Attacks Using Nonlinear Robust Codes // Fault Analysis in Cryptography. 2011.

5. *Kulikowski K., Karpovsky M. G.* Robust Correction of Repeating Errors by Nonlinear Codes // Communications, IET. 2011. Vol. 5, N 4. P. 2317—2327.

6. *Karpovsky M. G., Kulikowski K., Wang Z.* On-line self error detection with equal protection against all errors // Int. J. of Highly Reliable Electronic System Design. 2008.

7. *Nyberg K.* Differently uniform mappings for cryptography // Eurocrypt 1993. Lecture Notes in Computer Science. 1994. Vol. 765. P. 55—64.

8. *Ahlswede R., Aydinian H., Khachatrian L.* Unidirectional error control codes and related combinatorial problems // Proc. 8th Intern. Workshop Algebr. Combin. Coding Theory (ACCT-8). St. Petersburg, 2002. P. 6—9.

9. *Menezes A., van Oorschot P., Vanstone S.* Handbook of Applied Cryptography. CRC Press, 1996.

Сведения об авторе

Максим Олегович Алексеев — аспирант; Санкт-Петербургский государственный университет аэрокосмического приборостроения, кафедра аэрокосмических компьютерных технологий; E-mail: alexeevmo@gmail.com

Рекомендована кафедрой
№ 51 безопасности информационных систем

Поступила в редакцию
01.02.13 г.

БЕСПРОВОДНЫЕ СЕТИ СВЯЗИ

УДК 004.75

Е. А. Бакин, К. Н. Смирнов

МЕТОД ОЦЕНКИ ТОПОЛОГИИ БЕСПРОВОДНОЙ СЕТИ С ПРИМЕНЕНИЕМ АПРИОРНОЙ ИНФОРМАЦИИ О РАСПОЛОЖЕНИИ УСТРОЙСТВ

Рассматриваются методы оценки коэффициентов передачи канала между устройствами сенсорной сети. Приведена статистическая модель взаимного расположения устройств, для нее предложен метод оценки коэффициентов передачи по максимуму апостериорной плотности вероятности. Проведено сравнение стандартных методов оценки с предложенным.

Ключевые слова: *сенсорная сеть, коэффициент передачи канала, максимум апостериорной плотности, RSSI.*

Введение. В настоящее время задача контроля параметров объектов, распределенных на обширной территории, весьма распространена во многих областях жизнедеятельности. Такой контроль подразумевает измерение некоторого набора физических величин, характеризующих состояние объекта, и передачу полученных данных на пункт сбора информации. В решении этой задачи широко используются так называемые сенсорные сети [1—4].

Сенсорная сеть состоит из множества датчиков, называемых сенсорами, и пункта сбора информации, называемого базовой станцией (БС). Все устройства сенсорной сети связаны между собой радиолиниями. Сенсоры предназначены для регистрации измеряемого параметра и передачи полученной информации на БС. Как правило, каждый сенсор состоит из датчика, вычислительного устройства и маломощного приемопередатчика [5]. Назначением БС является сбор информации с сенсоров и управление сетью. Для эффективного управления сетью базовой станции необходима информация о топологии сети, а именно о том, между какими сенсорами может быть установлена надежная связь [6].

Параметром, характеризующим надежность связи между двумя сенсорами a и b, может являться коэффициент передачи канала $g_{a,b}$. В этом случае топология сенсорной сети полностью определяется матрицей коэффициентов передачи

$$\mathrm{G} = \begin{bmatrix} g_{1,1} & g_{1,2} & \cdots & g_{1,N} \\ g_{2,1} & g_{2,2} & \cdots & g_{2,N} \\ \vdots & \vdots & \ddots & \vdots \\ g_{N,1} & g_{N,2} & \cdots & g_{N,N} \end{bmatrix}, \qquad (1)$$

где N — число сенсоров в сети.

Топология сенсорной сети, как правило, изменяется во времени. Таким образом, для поддержания работоспособности сети необходима периодическая оценка текущей топологии. Обычно с этой целью устройства сети обмениваются набором тестовых сообщений, по которым

оценивается качество связи между парами устройств [7]. Чем больше тестовых сообщений, тем точней результат оценки, однако тем выше накладные расходы на проведение данной процедуры. В настоящей работе предлагается алгоритм оценки топологии сети, использующий дополнительную информацию о статистической взаимосвязи между координатами устройств и позволяющий повысить точность оценки без увеличения числа тестовых сигналов.

Оценка коэффициентов передачи канала при помощи тестового сигнала. Для оценки коэффициентов передачи, как правило, используется следующая процедура, инициируемая базовой станцией [8]. Каждый сенсор сети по очереди передает в эфир тестовый сигнал с известной структурой, мощностью $P_{\text{прд}}$ и длительностью τ. Время начала и окончания выхода в эфир каждого из сенсоров регламентировано и каждый из сенсоров обладает информацией о времени выхода в эфир всех остальных сенсоров сети. Как правило, приемный тракт устройств сенсорной сети включает в себя индикатор мощности входного сигнала — так называемый RSSI [9]. Работу идеализированного устройства RSSI можно описать следующим образом.

Зная время передачи сигнала τ и мощность передатчика $P_{\text{прд}}$, можно определить энергию излученного сигнала $E_{\text{прд}} = P_{\text{прд}}\tau$. Энергия сигнала на входе приемника будет равна $E_{\text{прм}} = g_{a,b}E_{\text{прд}}$. Тогда если тестовый сигнал является узкополосным, справедливо выражение $S_{\text{прм}}(j\omega) = \sqrt{g_{a,b}}S_{\text{прд}}(j\omega)e^{j\omega\Delta t}$, где $S_{\text{прд}}(j\omega)$ — спектр переданного (излученного) сигнала, $S_{\text{прм}}(j\omega)$ — спектр принятого сигнала, Δt — задержка на распространение.

Для максимизации отношения сигнал/шум (ОСШ) при приеме сигнала применяется согласованный фильтр, комплексная частотная характеристика которого равна $K_{\text{сф}}(j\omega) = kS^*(j\omega)$, где * — знак комплексного сопряжения, а k — коэффициент, зависящий от конструктивных особенностей фильтра, $S(j\omega)$ — спектральная функция сигнала, с которым согласован фильтр. Спектральная функция сигнала на выходе согласованного фильтра будет равна

$$S_{\text{в.сф}}(j\omega) = \sqrt{g_{a,b}}S_{\text{прд}}(j\omega)e^{j\omega\Delta t}kS^*_{\text{прд}}(j\omega) = \sqrt{g_{a,b}}k\left|S_{\text{прд}}(j\omega)\right|^2 e^{j\omega\Delta t}.$$

Далее для устранения неоднозначности начальной фазы принятого сигнала выделяется модуль его огибающий (например, при помощи квадратурного детектора). Тогда при $\Delta t \ll t$ через интервал времени τ после начала приема на выходе квадратурного детектора будет наблюдаться максимальное значение выходного сигнала оптимального фильтра: $s_{\max} = \sqrt{g_{a,b}}kE_{\text{прд}}$.

Так как одновременно с полезным сигналом на согласованный фильтр поступают собственные тепловые шумы приемника, окончательная формула для выходного сигнала в момент времени τ имеет вид $s_{\text{в.сф}} = \left|s_{\max}e^{j\omega\Delta t} + n\right| = \left|\sqrt{g_{a,b}}kE_{\text{прд}}e^{j\omega\Delta t} + n\right|$, где n — комплексная гауссова случайная величина с нулевым математическим ожиданием и дисперсией D_n, зависящей от коэффициента шума приемника, коэффициента усиления приемного тракта и т. д.

Таким образом, измеряя уровень сигнала в моменты времени $t_m = t_0 + m\tau$ ($m = \overline{1,N}$, t_0 — время начала процедуры), каждый сенсор i может определить коэффициент передачи канала между собой и сенсором m через выражения (2), (3):

$$\xi = \frac{s_{\text{в.сф}}(t_m)}{kP_{\text{прд}}\tau} = \left|\sqrt{g_{i,m}}e^{j\omega\Delta t} + \eta\right|, \tag{2}$$

$$g_{i,m} \approx \xi^2, \tag{3}$$

где ξ — нормированный сигнал на выходе детектора, η — гауссова случайная величина с дисперсией $D = \dfrac{D_n}{k^2 E_{\text{прд}}^2}$.

Для описания предлагаемого алгоритма оценки коэффициента передачи приведем используемую в работе систему допущений.

Для узкополосных систем зависимость коэффициента передачи от расстояния описывает расширенная модель Окумура-Хата [10—12]:

$$g_{i,j} = \frac{\alpha}{d_{i,j}^{\beta}}, \tag{4}$$

где $d_{i,j}$ — расстояние между сенсорами i и j, α и β — коэффициенты, характеризующие параметры среды распространения сигнала.

Согласно принятой в работе модели, сенсоры сети случайным образом размещены на площади $S = a^2$, так что их координаты являются независимыми случайными величинами (СВ) с равномерно распределенной на интервале $[0, a]$ плотностью вероятности [13].

Оценка коэффициента передачи канала на основе максимума апостериорной плотности вероятности. Для повышения точности оценки коэффициента передачи канала воспользуемся методом максимума апостериорной плотности вероятности. В данном методе учитывается дополнительная информация о взаимном расположении сенсоров.

Поскольку коэффициент передачи канала оценивается по формуле (1), можно вычислить его априорную плотность вероятности. Для этого сначала найдем плотность вероятности (ПВ) расстояния между сенсорами. Расстояние между сенсорами составит

$$d_{i,j} = \sqrt{\left(x_i - x_j\right)^2 + \left(y_i - y_j\right)^2},$$

где x_i, x_j, y_i, y_j — координаты сенсоров на плоскости.

Найдем поэтапно ПВ расстояния: сначала — закон распределения разности координат, затем — квадрат этой разности; затем — распределение суммы квадратов и наконец — распределение квадратного корня получившейся случайной величины.

ПВ разности координат $\Delta x = x_i - x_j$ представляет собой известное распределение Симпсона:

$$f_{\Delta x}(x) = \begin{cases} \dfrac{a + x}{a^2}, & x \in [-a, 0); \\ \dfrac{a - x}{a^2}, & x \in [0, a]; \\ 0, & x \notin [-a, a]. \end{cases}$$

Найдем распределение СВ Δx^2. Так как Δx распределена на интервале $[-a, a]$, а функция возведения в квадрат не является монотонной на нем, то необходимо разбить интервал на участки монотонности $[-a, 0)$ и $[0, a]$ и вычислить ПВ Δx^2 на одном из отрезков. Результирующая ПВ Δx^2 будет равна удвоенному значению ПВ, вычисленной для одного из отрезков (поскольку $y = x^2$ симметрична относительно оси ординат):

$$f_{\Delta x^2}(x) = \begin{cases} \dfrac{1}{a\sqrt{x}} - \dfrac{1}{a^2}, & x \in \left[0, a^2\right]; \\ 0, & x \notin \left[0, a^2\right]. \end{cases}$$

Приведенные выражения справедливы как для координаты x, так и для y.

Найдем плотность вероятности суммы $\Delta x^2 + \Delta y^2$. Поскольку Δx^2 и Δy^2 независимы, то для нахождения закона распределения их суммы необходимо провести композицию законов распределения: $f_\Sigma(z) = \int\limits_{-\infty}^{\infty} f_{\Delta x^2}(x) f_{\Delta y^2}(z-x)\,dx$.

Плотность вероятности суммы $\Delta x^2 + \Delta y^2$ будет равна

$$f_\Sigma(z) = \begin{cases} \dfrac{z}{a^4} - \dfrac{4\sqrt{z}}{a^3} + \dfrac{\pi}{a^2}, & z \in \left[0, a^2\right]; \\ \dfrac{2\arcsin\left(\dfrac{2a^2 - z}{z}\right) - 3}{a^2} + \dfrac{4\sqrt{z - a^2}}{a^3} - \dfrac{z - a^2}{a^4}, & z \in \left(a^2, 2a^2\right]; \\ 0, & z \notin \left[0, 2a^2\right]. \end{cases}$$

И наконец, найдем плотность вероятности расстояния между сенсорами:

$$f_d(x) = \begin{cases} \left(\dfrac{x^2}{a^4} - \dfrac{4x}{a^3} + \dfrac{\pi}{a^2}\right) 2x, & x \in \left[0, a\right]; \\ \left(\dfrac{2\arcsin\left(\dfrac{2a^2 - x^2}{x^2}\right) - 3}{a^2} + \dfrac{4\sqrt{x^2 - a^2}}{a^3} - \dfrac{x^2 - a^2}{a^4}\right) 2d, & x \in \left(a, \sqrt{2}a\right]; \\ 0, & x \notin \left[0, \sqrt{2}a\right]. \end{cases}$$

Теперь, зная значение ПВ для d и выражение, связывающее его с коэффициентом передачи канала (1), можно найти априорную плотность вероятности для коэффициента передачи g:

$$f(g) = \begin{cases} 2\gamma\left(\dfrac{2\arcsin\left(\dfrac{2a^2 - \gamma^2}{\gamma^2}\right) - 3}{a^2} + \dfrac{4\sqrt{\gamma^2 - a^2}}{a^3} - \dfrac{\gamma^2 - a^2}{a^4}\right)\left|\psi'(g)\right|, & g \in \left[\dfrac{\alpha}{\left(\sqrt{2}a\right)^\beta}, \dfrac{\alpha}{a^\beta}\right]; \\ \left(\dfrac{2\gamma^3}{a^4} - \dfrac{8\gamma^2}{a^3} + \dfrac{2\pi\gamma}{a^2}\right)\left|\psi'(g)\right|, & g \in \left(\dfrac{\alpha}{a^\beta}, \infty\right); \\ 0, & g \in \left(-\infty, \dfrac{\alpha}{\left(\sqrt{2}a\right)^\beta}\right), \end{cases}$$

где $\left|\psi'(g)\right| = -\dfrac{\sqrt[\beta]{\alpha}}{\beta} g^{\frac{-(1+\beta)}{\beta}}$ — производная по g от функции, обратной (4), а $\gamma = \sqrt[\beta]{\dfrac{\alpha}{g}}$.

Используя формулу Бейеса, можно определить апостериорную плотность вероятности для оцениваемого параметра g как

$$f\left(g\left|\xi\right.\right)=\frac{f\left(g\right)f\left(\xi\left|g\right.\right)}{f(\xi)},$$

где $f(g)$ — априорная плотность вероятности параметра g; $f\left(\xi\left|g\right.\right)$ — условная плотность вероятности ξ.

Значение $f\left(\xi\left|g\right.\right)$ подчиняется гауссову закону:

$$f\left(\xi\left|g\right.\right)=\frac{1}{\sqrt{2\pi D}}\exp\left\{-\frac{\left(\xi-\sqrt{g}\right)^2}{2D}\right\}.$$

Искомая оценка коэффициента передачи канала равна абсциссе максимума апостериорной плотности вероятности (рис. 1):

$$\hat{g}=\arg\left\{\max f\left(g\left|\xi\right.\right)\right\}=\arg\left\{\max\left[f\left(g\right)f\left(\xi\left|g\right.\right)\right]\right\}. \qquad (5)$$

В силу одномодовости апостериорной плотности вероятности ее максимум может быть найден численно.

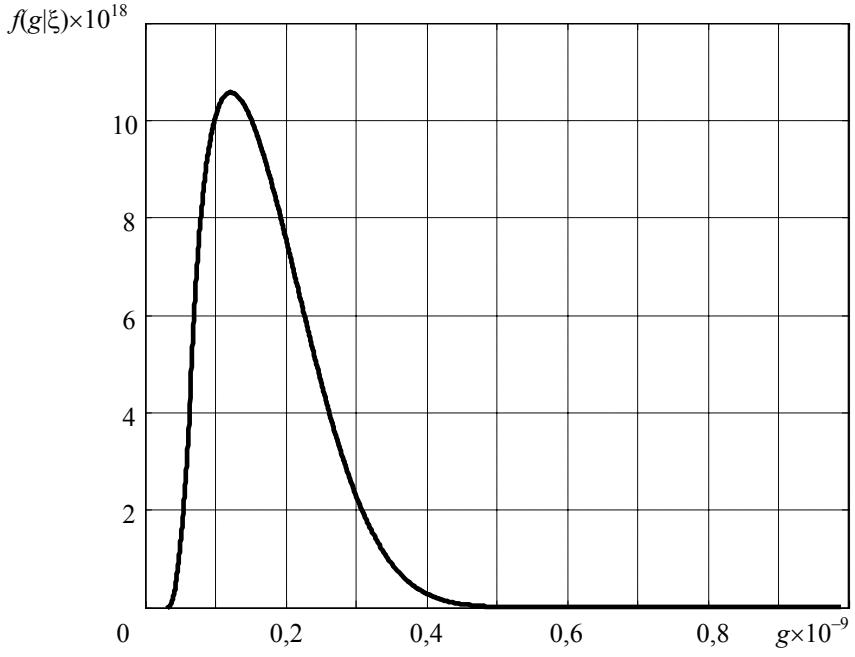


Рис. 1

Анализ эффективности предложенного алгоритма. Сравнение приведенных методов производилось путем имитационного моделирования с использованием работ [14, 15]. При моделировании были использованы следующие типовые значения параметров: a = 1000 м, $P_{\text{прд}}$ = 6 мВт, τ = 1 мс, $\alpha = 9{,}9\cdot10^{-5}$ (соответствует работе с изотропными антеннами на частоте 2,4 ГГц), β = 3 [16].

Были получены зависимости (*1* — стандартный, *2* — предлагаемый алгоритм): относительной ошибки оценки параметра от длины тестового сигнала (рис. 2), относительной ошибки оцениваемого параметра от расстояния между сенсорами (рис. 3), зависимость дисперсии полученной оценки (3) от дисперсии шума на выходе согласованного фильтра (2) (рис. 4).

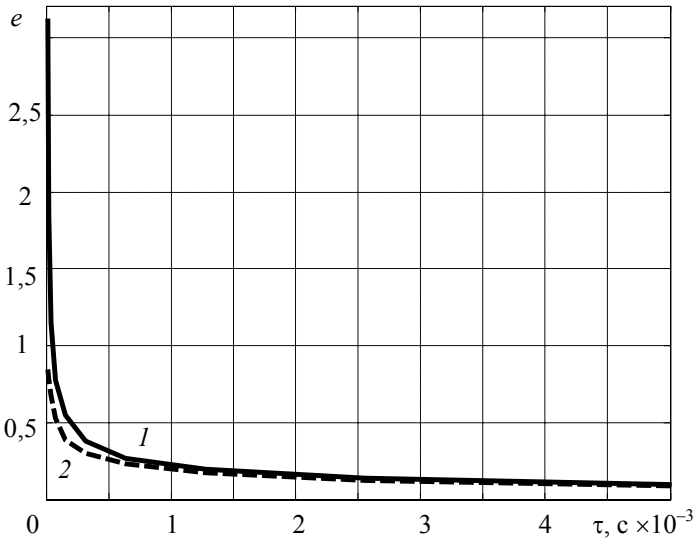


Рис. 2

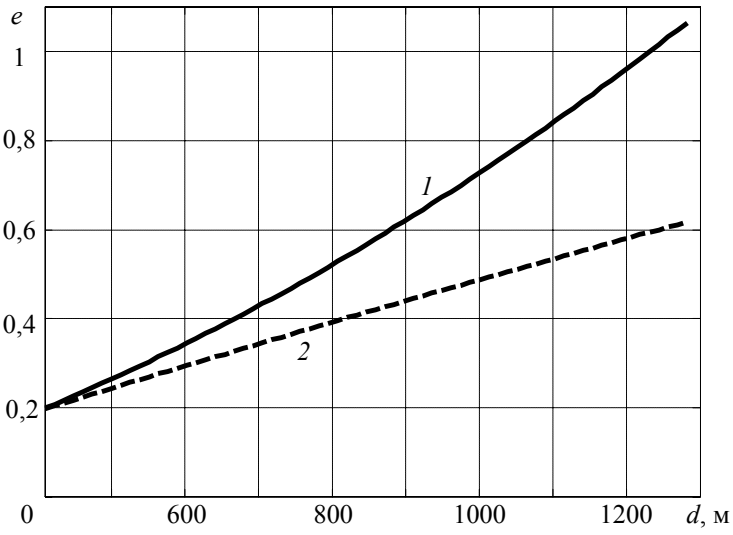


Рис. 3

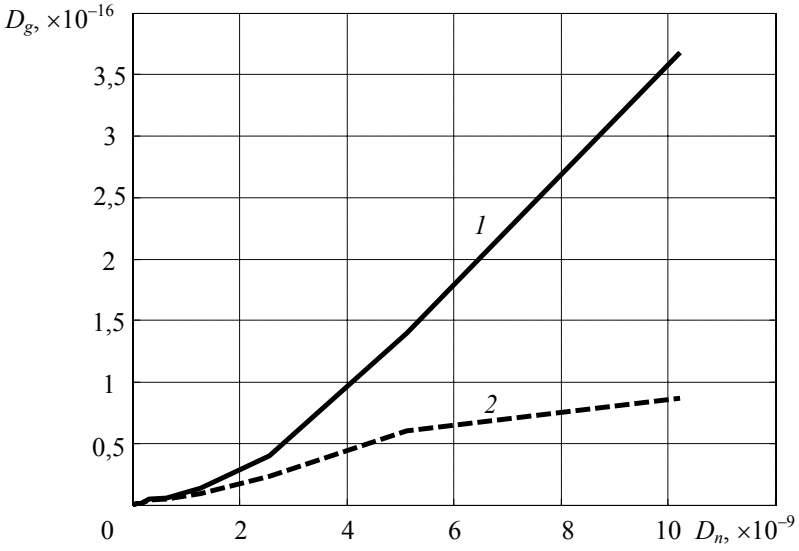


Рис. 4

Заключение. В настоящей работе представлены два способа оценки коэффициента передачи канала g — стандартный по сигналу RSSI и метод оценки по максимуму апостериорной плотности вероятности. Теоретически получены априорные и апостериорные плотности вероятности оцениваемого параметра. Серия вычислительных экспериментов показала, что предложенный метод оценки дает меньшую дисперсию и позволяет существенно снизить относительную ошибку оценки коэффициента передачи канала.

СПИСОК ЛИТЕРАТУРЫ

1. *Минеев А. Н., Минеев В. Н., Архипов Д. А., Агеев С. В.* Беспроводные сенсорные системы обнаружения пожаров на промышленных предприятиях России // Интернет-журнал „Технологии техносферной безопасности“. 2012. Февраль.
2. *Ларцов С. В., Столяров В. Е., Карюк М. В.* Применение беспроводной оперативной системы сбора информации на территориально распределенных объектах // Перспективные технологии в средствах передачи информации. 2009. С. 89—93.
3. *Вишневский В., Гайкович Г.* Беспроводные сенсорные сети в системах промышленной автоматики // Связь и телекоммуникации. 2008. № 1. С. 106—110.
4. *Шепета А. П., Евсеев Г. С., Бакин Е. А.* Нижняя граница длительности периода сбора информации в сенсорной сети // ИУС. 2011. № 6(55). С. 64—67.
5. *Karl H., Willi A.* Protocols and architectures for wireless sensor networks. Wiley-Interscience, 2005. 526 p.
6. *Labrador M. A., Wightman P. M.* Topology Control in Wireless Sensor Networks. Springer, 2009. 412 p.
7. *Andrews J. G., Ghosh A., Muhamed R.* Fundamentals of WiMAX: Understanding Broadband Wireless Networking. Prentice Hall PTR, 2007. 530 p.
8. *Santi P.* Topology control in wireless ad hoc and sensor networks. Wiley-Interscience, 2005. 280 p.
9. CC1111F32: True System-on-Chip with Low Power RF Transceiver and 8051 MCU. 110 p.
10. *Bose A., Foh C. H.* A Practical Path Loss Model For Indoor WiFi Positioning Enhancement // Proc. of ICICS'07. 2007.
11. *Somarriba O.* Evaluation of heuristic algorithms for scheduling, routing and power allocation in traffic sensitive spatial TDMA wireless ad hoc networks // 6th Intern. ICST Symp. on Modeling and Optimization. 2008. P. 566—571.
12. *Christophides F., Friderikos V.* Iterative hybrid graph and interference aware scheduling algorithm for STDMA networks // Electronic letters. 2008. Vol. 44. P. 558—559.
13. *Onat F. A., Stojmenovic I., Yanikomeroglu H.* Generating grandom graphs for simulation of wireless adhoc, actuator, sensor, and wireless networks // Pervasive and Mobile Computing. 2008. Vol. 4. P. 597—615.
14. *Levenberg K.* A method for the solution of certain problems in least squares // Quart. Appl. Math. 1944. Vol. 2. P. 164—168.
15. *Marquardt D.* An algorithm for least — squares estimation of nonlinear parameters // SIAM J. Appl. Math. 1963. Vol. 11. P. 431—441.
16. *Lee W. C. Y.* Mobile cellular telecommunications, Analog and Digital systems. NY: McGraw-Hill, 1995. 664 p.

Сведения об авторах

Евгений Александрович Бакин — Санкт-Петербургский государственный университет аэрокосмического приборостроения, кафедра моделирования вычислительных и электронных систем; ассистент; E-mail: jenyb@vu.spb.ru

Константин Николаевич Смирнов — аспирант; Санкт-Петербургский государственный университет аэрокосмического приборостроения, кафедра моделирования вычислительных и электронных систем; E-mail: kossmir@gmail.com

Рекомендована кафедрой
№ 51 безопасности информационных систем

Поступила в редакцию
01.02.13 г.

УДК 004.728.3.057.4

М. А. Гранкин, Е. В. Пустовалов, А. М. Тюрликов

АНАЛИЗ ПРОЦЕДУРЫ ПОГАШЕНИЯ ИНТЕРФЕРЕНЦИИ В OFDM-СИСТЕМЕ СО СЛУЧАЙНЫМ МНОЖЕСТВЕННЫМ ДОСТУПОМ

Рассматривается процедура погашения интерференции в централизованной сети, в которой на физическом уровне используется OFDM, а на уровне управления доступом к среде — случайный множественный доступ. Вычислена вероятность ошибки при погашении интерференции. Получена зависимость скорости алгоритмов множественного доступа от отношения сигнал/шум в канале.

Ключевые слова: *OFDM, погашение интерференции, случайный множественный доступ.*

Введение. Передача данных с ортогональным частотным разделением (Orthogonal Frequency Division Multiplexing, OFDM) [1] является одной из популярных технологий, используемых в современных системах связи, таких как IEEE 802.11, IEEE 802.16. В большинстве систем связи с OFDM используют частотно-временное разделение абонентов с динамическим расписанием. Тем не менее, в системах связи с большим числом абонентов и относительно небольшим трафиком, например, системах типа „машина-к-машине“ (Machine-Type-Communications, MTC), более эффективно использование случайного множественного доступа (СМД) [2].

В системах с СМД возможно возникновение ситуации, при которой два и более абонентов одновременно используют одни и те же частотно-временные ресурсы канала. В этом случае сигналы пользователей интерферируют друг с другом, в результате ни одно из переданных сообщений не может быть успешно принято. Такое событие называется *конфликтом.* В традиционных алгоритмах СМД (АЛОХА [3], древовидные алгоритмы [4, 5] и др.) конфликт разрешается тем, что все его участники повторно посылают свои сообщения через случайный промежуток времени, определяемый алгоритмом. Однако в современных беспроводных сетях можно уменьшить количество повторных передач. Это достигается следующим образом. Сигнал, принятый во время конфликта, сохраняется в буфере на приемной стороне. После того как один из участников конфликта повторно передал свое сообщение, и оно было успешно принято, этот сигнал вычитается из суммы сигналов, хранящейся в буфере, после чего декодируется сообщение второго абонента. Данная процедура называется *последовательным погашением интерференции* (Successive Interference Cancellation, SIC). Использование процедуры SIC в современных беспроводных сетях требует определения способа ее реализации на физическом уровне сети. Кроме того, необходима разработка новых алгоритмов СМД с учетом процедуры SIC на физическом уровне. Последняя задача успешно решалась в ряде работ [6—9]. В частности, в [9] был предложен древовидный алгоритм с погашением интерференции, устойчивый к возможным ошибкам в процедуре SIC, и была найдена скорость алгоритма как функция от вероятности ошибки на физическом уровне. Тем не менее конкретная схема погашения интерференции на физическом уровне не была рассмотрена, и неясно, как предложенная вероятностная модель, используемая для расчета скорости алгоритма, связана с реальными характеристиками канала связи, такими как частотная селективность канала и дисперсия шума.

В настоящей работе рассматривается процедура погашения интерференции на физическом уровне централизованной системы связи с OFDM. Исследуется влияние характеристик канала связи на величину ошибки в процедуре погашения интерференции и соответственно — на характеристики алгоритма СМД с погашением интерференции.

Модель системы. Будем рассматривать централизованную систему множественного доступа, все абоненты которой передают свои сообщения единому получателю — центральной станции (ЦС). Время дискретно и разбито на кадры, равные времени передачи одного сообщения. В конце каждого кадра ЦС уведомляет абонентов о том, какие сообщения были успешно приняты в данном кадре. На основе этой информации абоненты принимают решения о повторной передаче своих сообщений.

Передача сообщений в системе ведется с помощью ортогонального частотного разделения с кодированием (COFDM) [1]. В начало каждого OFDM-пакета добавляется преамбула, состоящая из последовательности во временной области с хорошими автокорреляционными свойствами (служит для детектирования сигнала) и последовательности $\mathbf{X}_{\text{пр}}$ в частотной области (служит для оценки канала). Будем также полагать, что каждое сообщение пользователя содержит контрольную сумму, которая при наличии ошибок в пакете на выходе декодера позволяет гарантированно их обнаружить.

Рассмотрим низкочастотную модель приема и передачи в OFDM, т.е. до цифро-аналогового преобразования в передатчике и после аналого-цифрового преобразования в приемнике. Передатчик OFDM условно будем обозначать Tx; стандартный OFDM-приемник — Rx. Будем полагать, что прохождение сигнала абонента через радиочасть передатчика, радиоканал и радиочасть приемника описывается эквивалентным низкочастотным линейным фильтром с откликом $\mathbf{h}$ и частотной передаточной функцией $\mathbf{H} = \text{ДПФ}(\mathbf{h})$, где ДПФ — дискретное преобразование Фурье. Пусть в некотором кадре одновременно передаются сигналы от K абонентов. Обозначим через $\mathbf{x}^{(i)}$ сигнал i-го абонента с выхода модуля Tx. Тогда входной сигнал OFDM-приемника представляется следующим выражением

$$\mathbf{y} = \sum_{i=1}^{K} \mathbf{x}^{(i)} * \mathbf{h}^{(i)} + \mathbf{n}, \tag{1}$$

где „*“ обозначает операцию свертки; $\mathbf{h}^{(i)}$ — отклик канала, через который проходит сигнал i-го абонента; $\mathbf{n}$ — вектор комплексного аддитивного белого гауссова шума (АБГШ) с дисперсией σ^2. Каждый элемент n_k вектора $\mathbf{n}$ является случайной комплексной величиной, действительная и мнимая части которой имеют гауссово распределение с нулевым математическим ожиданием и дисперсией $\sigma^2/2$ (такие величины будем называть комплексными гауссовыми величинами с нулевым математическим ожиданием и дисперсией σ^2).

Алгоритм оценки частотной передаточной функции канала. Для выполнения процедуры погашения интерференции приемнику нужно иметь оценку передаточной функции канала, которую выполним по преамбуле. На вход алгоритма подается сигнал $\mathbf{y}_{\text{пр}}$, который соответствует принятой из канала преамбуле. После удаления циклического префикса и перевода в частотную область с помощью быстрого преобразования Фурье (БПФ) получим вектор $\mathbf{Y}_{\text{пр}}$ длиной N (N — длина преобразования Фурье). Оценку канала выполним, разделив каждый элемент вектора $\mathbf{Y}_{\text{пр}}$ на известные значения вектора преамбулы $\mathbf{X}_{\text{пр}}$

$$\hat{H}_k = \frac{Y_{\text{пр},k}}{X_{\text{пр},k}}, \ \forall k = 0, ..., N-1.$$

Введем в обозначение ошибку в оценке канала:

$$\varepsilon_k \triangleq \hat{H}_k - H_k. \tag{2}$$

Можно показать, что для рассмотренного алгоритма оценки канала параметр ε_k является случайной комплексной гауссовой величиной с нулевым математическим ожиданием и дисперсией σ^2.

Будем полагать, что приемнику известна максимально возможная длительность отклика канала $L < N$. Тогда точность оценки передаточной функции канала можно повысить благодаря следующей процедуре:

1) перевести вектор $\hat{\mathbf{H}}'$ во временную область с помощью обратного БПФ. Получить вектор $\hat{\mathbf{h}}'$;

2) построить вектор $\hat{\mathbf{h}}$, обнулив последние $N - L$ элементов

$$\hat{h}_k = \begin{cases} \hat{h}_k', & 0 < k \le L\ -1, \\ 0, & L\ \ge k < N; \end{cases}$$

3) получить окончательные значения вектора $\hat{\mathbf{H}}$, переведя вектор $\hat{\mathbf{h}}$ в частотную область с помощью БПФ.

После выполнения этой процедуры дисперсия ошибки ε_k уменьшится в L/N раз.

Алгоритм работы центральной станции с погашением интерференции. Схема приемника ЦС с погашением интерференции приведена на рис. 1. Сигнал $\mathbf{y}$ с выхода АЦП поступает на вход стандартного OFDM-приемника Rx, который осуществляет обнаружение сигнала, оценку отклика канала, демодуляцию и декодирование. Если детектор в модуле Rx не обнаружил преамбулу, то ЦС определяет событие как „пусто“ и на этом обработка сигнала $\mathbf{y}$ заканчивается. Если детектор обнаружил преамбулу, то проверяется контрольная сумма для двоичного вектора $\hat{\mathbf{m}}^{(1)}$ на выходе блока Rx. Если контрольная сумма неверна, то ЦС обнаруживает конфликт и сигнал $\mathbf{y}$ записывается в буфер. Заметим, что если в буфере уже хранится некоторый сигнал, то буфер очищается, и на место старого сигнала записывается новый. Таким образом, для каждого кадра в буфере хранится не более одного цифрового сигнала, полученного с выхода АЦП. Наконец, если в векторе $\hat{\mathbf{m}}^{(1)}$ оказалась верная контрольная сумма, то ЦС определяет событие „успех“. Если буфер не пуст, то ЦС запускает процедуру погашения интерференции.

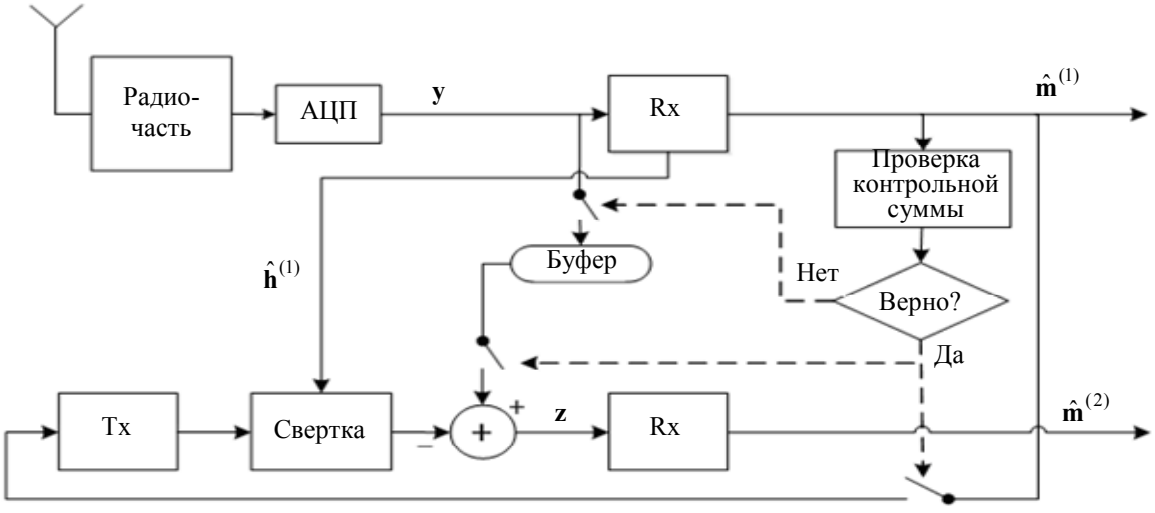


Рис. 1

Рассмотрим реализацию процедуры погашения интерференции. Сообщение $\hat{\mathbf{m}}^{(1)}$ поступает на вход модуля Tx, выполняющего операции кодирования и модуляции, аналогичные тем, которые выполнялись абонентом на передающей стороне. На выходе модуля Tx получается цифровой сигнал $\mathbf{x}^{(1)}$. Далее сигнал $\mathbf{x}^{(1)}$ поступает в цифровой

фильтр, который выполняет свертку входного сигнала с оценкой отклика канала $\hat{\mathbf{h}}^{(1)}$, полученной модулем Rx в текущем кадре. Результат свертки $\mathbf{x}^{(1)}$ и $\hat{\mathbf{h}}^{(1)}$ вычитается из сигнала $\mathbf{y}_{\text{buf}}$, хранящегося в буфере, и полученный сигнал $\mathbf{z}$

$$\mathbf{z} = \mathbf{y}_{\text{buf}} - \mathbf{x}^{(1)} * \mathbf{h}^{(1)}$$

отправляется во второй модуль Rx.

По окончании обработки сигнала $\mathbf{z}$ ЦС проверяет контрольную сумму в векторе $\hat{\mathbf{m}}^{(2)}$ на выходе второго блока Rx. Если контрольная сумма верна, значит, в предыдущем кадре произошел конфликт кратности два и ЦС смогла успешно восстановить сообщение второго абонента в результате погашения интерференции. На находящийся выше уровень отправляются сообщения $\mathbf{m}^{(1)}$ и $\mathbf{m}^{(2)}$, а по каналу обратной связи ЦС передает информацию об успешном приеме двух сообщений. Если контрольная сумма неверна, то либо в буфере хранился сигнал конфликта большей кратности, либо в результате погашения интерференции произошли ошибки, и сообщение второго абонента не было восстановлено. В этом случае на находящийся выше уровень перейдет только сообщение абонента $\mathbf{m}^{(1)}$, о чем ЦС сообщит абонентам по каналу обратной связи.

По окончании процедуры погашения интерференции буфер на ЦС, в котором хранится сигнал $\mathbf{y}$, очищается.

Анализ реализации процедуры погашения интерференции. Пусть в некотором кадре t один абонент передает свое сообщение $\mathbf{m}^{(1)}$. ЦС принимает в этом кадре сигнал $\mathbf{y}_t$:

$$\mathbf{y}_t = \mathbf{x}^{(1)} * \mathbf{h}^{(1)} + \mathbf{n}_t$$

и отправляет его в блок обработки Rx, на выходе которого получается двоичный вектор $\hat{\mathbf{m}}^{(1)}$. Вероятность ошибки на сообщение первого пользователя $p_1 \triangleq P\{\hat{\mathbf{m}}^{(1)} \neq \mathbf{m}^{(1)}\}$ зависит от параметров канала (профиль многолучевого распространения $\mathbf{P_h}$ и дисперсия шума σ^2), параметров помехоустойчивого кода и модуляции, а также от входного распределения символов в сообщении. Будем считать, что параметры кода и модуляции в системе зафиксированы, а сообщения всех пользователей имеют одинаковое равномерное входное распределение на множестве двоичных символов. Введем функцию ошибки $p_e(\mathbf{P_h}, \sigma^2)$, которая определяет вероятность ошибки на сообщение пользователя в зависимости от параметров канала, тогда

$$p_1 \triangleq P\{\hat{\mathbf{m}}^{(1)} \neq \mathbf{m}^{(1)}\} = p_e(\mathbf{P_h}, \sigma^2). \quad (3)$$

Заметим, что в рамках введенной системы обозначений p_1 является вероятностью ложного конфликта.

Пусть теперь в кадре t передают два абонента, а в кадре $t+1$ один из абонентов успешно передал свое сообщение $\mathbf{m}^{(1)}$. Будем полагать, что в процессе приема сигнала не возникло ошибок, и ЦС безошибочно декодировала $\mathbf{m}^{(1)}$. После успешного приема $\mathbf{m}^{(1)}$ ЦС запустит процедуру погашения интерференции и попытается декодировать сообщение $\mathbf{m}^{(2)}$ второго абонента. Найдем вероятность того, что ЦС не сможет успешно декодировать сообщение $\mathbf{m}^{(2)}$ при условии, что $\mathbf{m}^{(1)}$ успешно принято.

Утверждение. Если для цифровой модуляции сигнала в частотной области используется двоичная фазовая манипуляция (Binary Phase Shift Keying, BPSK), то вероятность ошибки в погашении интерференции можно найти с помощью выражения

$$p_2 \triangleq P\{\hat{\mathbf{m}}^{(2)} \neq \mathbf{m}^{(2)} \mid \hat{\mathbf{m}}^{(1)} = \mathbf{m}^{(1)}\} = p_e\left(\mathbf{P_h}, \sigma^2\left(1 + L/N\right)\right). \quad (4)$$

Доказательство. В кадре $t+1$ на вход второго модуля Rx поступает вектор $\mathbf{z}_{t+1}$:

$$\mathbf{z}_{t+1} \triangleq \mathbf{y}_t - \mathbf{x}^{(1)} * \mathbf{h}^{(1)} = \mathbf{x}^{(2)} * \mathbf{h}^{(2)} - \mathbf{x}^{(1)} * (\hat{\mathbf{h}}^{(1)} - \mathbf{h}^{(1)}) + \mathbf{n}_t.$$

После удаления циклического префикса и перевода в частотную область получаем

$$Z_{t+1,k} = X_k^{(2)} H_k^{(2)} - X_k^{(1)} \left(\hat{H}_k^{(1)} - H_k^{(1)} \right) + \eta_{t,k}, \forall k = 0,..., N-1, \qquad (5)$$

где k — номер поднесущей в дискретном преобразовании Фурье; $\mathbf{Z}_{t+1}$, $\mathbf{X}^{(1)}$, $\mathbf{X}^{(2)}$, $\mathbf{H}^{(1)}$, $\mathbf{H}^{(2)}$ и $\boldsymbol{\eta}_{t+1}$ — соответствующие частотные аналоги векторов $\mathbf{z}_{t+1}$, $\mathbf{x}^{(1)}$, $\mathbf{x}^{(2)}$, $\mathbf{h}^{(1)}$, $\mathbf{h}^{(2)}$ и $\mathbf{n}_{t+1}$. Подставив (2) в (5), получим

$$Z_{t+1,k} = X_k^{(2)} H_k^{(2)} - X_k^{(1)} \varepsilon_k^{(1)} + \eta_{t,k}, \forall k = 0, ..., N-1.$$

Введем обозначения

$$\zeta_k \triangleq X_k^{(1)} \varepsilon_k^{(1)}, \qquad (6)$$
$$\gamma_k \triangleq \eta_{t,k} - \zeta_k.$$

Поскольку для модуляции сигнала в цифровой области используется двоичная фазовая манипуляция, а символы в сообщении имеют равномерное распределение, то $X_k^{(1)}$ представляет собой случайную величину, имеющую равномерное распределение на множестве $\{-1, +1\}$. Вычислив плотность произведения случайных величин, получим, что ζ_k — комплексная гауссова величина с нулевым математическим ожиданием и дисперсией $\sigma^2 L / N$. Согласно правилу сложения гауссовых величин, γ_k — комплексная гауссова величина с нулевым математическим ожиданием и дисперсией

$$D[\gamma_k] = \sigma^2 + \sigma^2 L / N = \sigma^2 \left(1 + L / N\right).$$

Таким образом, после погашения интерференции дисперсия шума в сигнале на входе второго модуля Rx повышается в $\left(1 + L / N\right)$ раз. Справедливость (4) доказана. □

Замечание. Если для модуляции данных в частотной области используется модуляция, отличная от двоичной фазовой манипуляции, то распределение величины ζ_k (см. выражение (6)) не является гауссовым. Однако при $E[X_k^{(1)}] = 0$ и $E[|X_k^{(1)}|^2] = 1$, можно считать, что выражение (4) выполняется с высокой точностью.

Из (3) и (4) следует, что, зная функцию $p_e(\mathbf{P}_\mathbf{h}, \sigma^2)$, можно найти вероятность ложного конфликта p_1 и вероятность ошибки в погашении интерференции p_2.

Анализ СМД с погашением интерференции. Выше были рассмотрены алгоритмы физического уровня. На уровне управления доступом к среде (Media Access Control, MAC) каждого абонента работает алгоритм СМД, который, получая от ЦС в конце каждого кадра сигнал обратной связи θ, определяет кадры, в которых абонент должен передавать (повторно передавать) свои сообщения. Сравним работу в рассмотренной выше системе связи трех алгоритмов СМД: простого древовидного, улучшенного древовидного [4] и устойчивого древовидного с погашением интерференции [9]. В качестве меры производительности алгоритмов СМД будем вычислять их скорость — максимальную интенсивность поступления сообщений в систему, при которой система остается стабильной (т.е. обеспечивается конечная задержка сообщений).

В [10] была введена модель СМД с ложными конфликтами и получена скорость простого и улучшенного древовидных алгоритмов как функция от вероятности ложного конфликта p_1. С использованием методики расчета скорости из [11] скорость алгоритма с погашением

интерференции может быть найдена как функция от вероятности ложного конфликта p_1 и вероятности ошибки в процедуре погашения интерференции p_2.

Для нахождения вероятностей p_1 и p_2 найдем значения функции $p_e(\mathbf{P_h}, \sigma^2)$ с помощью имитационного моделирования. Будем рассматривать систему с большим числом абонентов, которые передают на ЦС короткие сообщения, размером 200 бит. В качестве кодово-модуляционной схемы будем использовать сверточный код со скоростью 1/2 и BPSK модуляцию. Размер преобразования Фурье выберем 512, так что одно сообщение передается внутри одного блока OFDM. Профиль канала многолучевого распространения приведен в таблице.

Параметр	Номер луча					
	1	2	3	4	5	6
Задержка, мкс	0	0,15	2,22	3,05	5,86	5,93
Относительное ослабление, дБ	0	13,8	16,2	14,9	13,6	16,4

На рис. 2 приведены графики зависимости скорости R алгоритмов от отношения сигнал/шум (ОСШ) в канале (*1* — простой древовидный алгоритм; *2* — улучшенный древовидный алгоритм; *3* — древовидный алгоритм с погашением интерференции). Видно, что при больших значениях ОСШ (когда вероятность ложного конфликта близка к нулю) скорость алгоритма с погашением интерференции на 13 % выше скорости улучшенного древовидного алгоритма и на 20 % — скорости простого древовидного алгоритма. С другой стороны, при ОСШ меньше 6 дБ алгоритм с погашением интерференции проигрывает простому древовидному алгоритму. Таким образом, оценив уровень ОСШ, центральная станция может принять решение, какой из алгоритмов СМД целесообразно применять в данном канале.

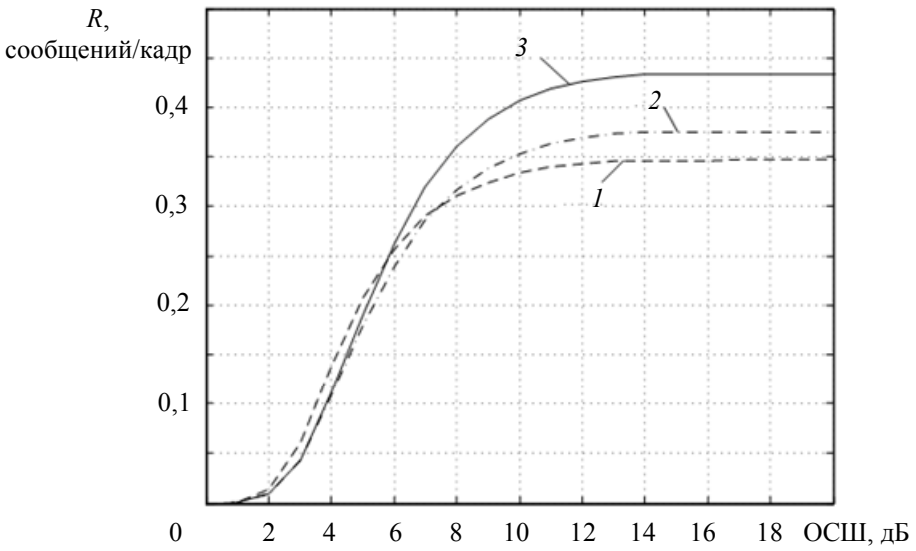


Рис. 2

Заключение. В работе рассмотрена реализация процедуры погашения интерференции на физическом уровне OFDM-системы и получена оценка вероятности ошибки в такой системе. Показано, что, используя полученную вероятность ошибки в расчете скорости древовидных алгоритмов, можно определить, какой из алгоритмов СДМ целесообразнее использовать в конкретном канале.

Заметим, что полученные результаты применимы и в других, близких к OFDM, системах, например, в системе с модуляцией SC-FDMA (Single Carrier Frequency Division Multiple Access), которая используется в восходящем канале стандарта LTE.

СПИСОК ЛИТЕРАТУРЫ

1. *Prasad R.* OFDM for Wireless Communications Systems. Artech House, 2004. 272 p.

2. *Cheng M., Lin G., Wei H., Hsu A.* Overload control for machine-type-communications in LTE-advanced system // IEEE Communications Magazine. 2012. Vol. 50, N 6. P. 38—45.

3. *Abramson N.* The ALOHA system — another alternative for computer communications // Proc. AFIPS Conf. 1970. Vol. 36. P. 295—298.

4. *Цыбаков Б. С., Михайлов В. А.* Свободный синхронный доступ пакетов в широковещательный канал с обратной связью // Проблемы передачи информации. 1978. Т. 14, № 4. С. 32—59.

5. *Capetanakis J.* Tree algorithms for packet broadcast channels // IEEE Transact. on Information Theory. 1979. Vol. 25, N 4. P. 505—515.

6. *Винель А. В., Тюрликов А. М., Федоров К. А.* Использование последовательного погашения интерференции при организации случайного множественного доступа в централизованных сетях // ИУС. 2009. № 2(39). С. 46—55.

7. *Yu Y., Giannakis G. B.* High-throughput random access using successive interference cancellation in a tree algorithm // IEEE Transact. on Information Theory. 2007. Vol. 53, N 12. P. 4628—4639.

8. *Houdt B. V., Peeters G.* FCFS tree algorithms with interference cancellation and single signal memory requirements // Proc. of Intern. Conf. on Telecommunications ICT'08. 2008. P. 1—6.

9. *Андреев С. Д., Пустовалов Е. В., Тюрликов А. М.* Древовидный алгоритм разрешения конфликта, устойчивый к неполному погашению интерференции // Автоматика и телемеханика. 2009. Т. 70, № 3. С. 78—96.

10. *Евсеев Г. С., Ермолаев Н. Г.* Оценки характеристик разрешения конфликтов в канале со свободным доступом и шумом // Проблемы передачи информации. 1982. Т. 18, № 2. С. 101—105.

11. *Евсеев Г. С., Тюрликов А. М.* Взаимосвязь характеристик блокированных стек-алгоритмов случайного множественного доступа // Проблемы передачи информации. 2007. Т. 43, № 4. С. 83—92.

Сведения об авторах

Максим Андреевич Гранкин — аспирант; Санкт-Петербургский государственный университет аэрокосмического приборостроения, кафедра инфокоммуникационных систем; E-mail: m.grankin@vu.spb.ru

Евгений Васильевич Пустовалов — Санкт-Петербургский государственный университет аэрокосмического приборостроения, Институт компьютерной безопасности вычислительных систем и сетей; научный сотрудник; E-mail: eugeny@vu.spb.ru

Андрей Михайлович Тюрликов — д-р техн. наук, доцент; Санкт-Петербургский государственный университет аэрокосмического приборостроения, кафедра инфокоммуникационных систем; E-mail: turlikov@vu.spb.ru

Рекомендована кафедрой
№ 51 безопасности информационных систем

Поступила в редакцию
01.02.13 г.

УДК 004.75

К. Б. Гурнов, Г. С. Евсеев

СИНТЕЗ ОПТИМАЛЬНОГО ПРАВИЛА ПРИЕМА СИГНАЛА НА ФОНЕ ПЕРЕКРЕСТНЫХ ПОМЕХ В СИСТЕМЕ WCAN

Предложен новый алгоритм приема сигналов на основе вычисления максимума функции правдоподобия для системы беспроводной связи между чипами, приводятся аналитические выкладки для расчета вероятности ошибки на бит. Представлены результаты моделирования.

Ключевые слова: *беспроводная связь между чипами, сверхширокополосная связь, позиционная импульсная модуляция, максимум функции правдоподобия, вероятность ошибки.*

Введение. Необходимость разработки принципиально новых технологий связи обусловлена, прежде всего, появлением сложных систем, которые могут включать большое количество плат и микросхем. Такие системы требуют все больших скоростей передачи информации, при этом обмен информации по проводным линиям связи может быть затруднен или вовсе невозможен.

Беспроводная связь между чипами (wireless chip area network, WCAN) [1—3] в настоящее время позволяет обеспечить требуемую скорость и помехоустойчивость передачи информации. Для связи между чипами широко используется диапазон, выделенный для ультраширокополосных сигналов (UWB). Он позволяет достичь высокой помехозащищенности и адаптивности к реальной эфирной обстановке благодаря низкому (шумоподобному) уровню сигнала, экономичному использованию частотного ресурса, сложности перехвата и постановки прицельных помех.

В системах данного типа широко используются различные схемы модуляции (BPSK, DPSK, PPM и т.д.). Поскольку одним из основных требований для трансивера является дешевизна и простота, то схема модуляции PPM (pulse position modulation) [4—7] является наиболее привлекательной.

Цель настоящей работы — построение модели приемника для стандарта беспроводной связи UWB с использованием PPM-модуляции.

Модель системы с синхронным множественным доступом в канал. Рассматривается система, абоненты которой обмениваются двоичными данными по общему каналу связи. Для передачи двоичных символов используется кодово-импульсная модуляция. При этом для передачи одного бита используется посылка в канал N импульсов, информация о передаваемом символе заключена в задержках между импульсами.

Предполагается, что в системе установлена полная синхронизация, т.е.

— время работы представляется в виде последовательности интервалов (слотов), каждый из которых имеет длительность $2Tc$ (Tc — длительность импульса);

— M последовательных слотов образуют фрейм;

— N последовательных фреймов образуют гиперфрейм;

— границы всех слотов, фреймов и гиперфреймов считаются совмещенными у всех приемников и передатчиков.

Для передачи одного символа используется гиперфрейм. При этом в каждом из N фреймов гиперфрейма случайным образом выбирается слот и в нем — полуслот (правый или левый). При передаче символа „0“ импульсы передаются в выбранных полуслотах, а при передаче „1“ — в смежных полуслотах выбранных слотов. Из этого следует, что выбор полуслотов определяется либо сгенерированной случайной двоичной последовательностью длины N

при передаче символа „0“, либо инверсией этой последовательности при передаче „1“. Предполагается, что такой механизм обеспечивает равновероятный выбор положения импульса в полуслотах фрейма, а также независимый выбор положения импульсов в разных фреймах гиперфрейма.

Приемник, синхронизированный с передатчиком, может быть выполнен в виде фильтра, согласованного с сигналом. При этом спустя время *Tc* от начала импульса (в конце полуслота) на выходе приемника формируется значение, равное энергии импульса. Будем полагать, что значения энергии импульсов, поступающих от разных передатчиков, на входе каждого приемника одинаковы. В этом случае можно считать, что на выходе приемника появляется нормированное значение, равное числу импульсов, принятых в текущем полуслоте. Предполагается, что приемнику известны номера работающего с ним передатчика и слотов, выбранных для передачи импульсов (это может быть обеспечено, например, синхронным запуском двух копий псевдослучайного датчика в передатчике и приемнике). Кроме того, считается известной двоичная последовательность длины *N*, определяющая выбор полуслотов для передачи импульсов. Поскольку передаваемый символ неизвестен, положение импульсов полезного сигнала остается неопределенным, потому что может задаваться либо этой последовательностью, либо ее инверсией.

В подобной системе единственым источником ошибок при приеме двоичного символа являются импульсы „чужих“ передатчиков, попавшие в слоты, анализируемые приемником. Заметим, что если хотя бы в одном из *N* анализируемых слотов импульсы присутствуют только в одном полуслоте, возможно точно определить значение переданного символа. На этом основана работа OR-приемника, описанного в монографии [1].

Постановка задачи. Из описания системы следует, что на решение приемника влияют только импульсы, расположенные в слотах, выбранных для передачи полезного сигнала. Принятие решений на приемной стороне в этом случае обеспечивает метод статистической теории решений. Очевидно, что апостериорные вероятности передачи „0“ или „1“ одинаковы. Решение при этом принимается путем вычисления функции правдоподобия и сравнения двух гипотез: что наиболее вероятно, появление „1“ или „0“.

Без ограничения общности можно считать, что при передаче „0“ все импульсы полезного сигнала содержатся в правом полуслоте, а при „1“ — в левом. Обозначим через x_i и y_i ($i = 1, ..., N$) число принятых импульсов соответственно в левом и правом полуслотах анализируемого слота в *i*-м фрейме гиперфрейма. В отсутствие перекрестных помех либо $x_i = 1$, $y_i = 0$ ($i = 1..N$), либо наоборот. Если в канале работают *K*–1 „чужих“ передатчиков, то x_i, y_i могут принимать значения от нуля до *K* (рис. 1).

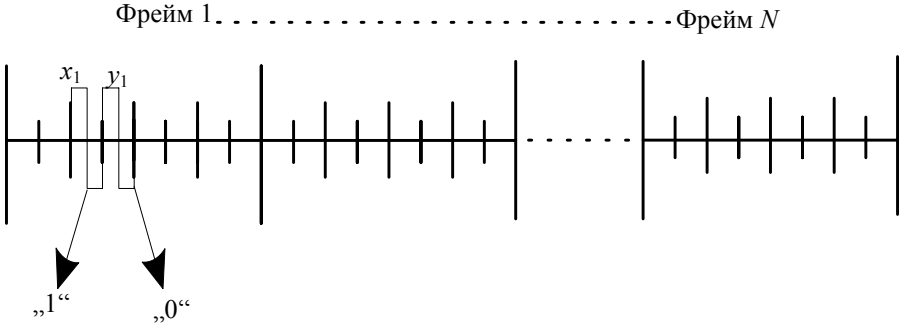


Рис. 1

Вычислим вероятность образования пар (x_i, y_i) при передаче символов „1“ $P(x_i, y_i / "1") = P(x_i - 1, y_i)$ и „0“ $P(x_i, y_i / "0") = P(x_i, y_i - 1)$ в одном фрейме

$$P(x_i, y_i / "1") = P(x_i - 1, y_i) = C_{K-1}^{x_i+y_i-1} \left(\frac{1}{M}\right)^{x_i+y_i-1} \left(\frac{M}{M-1}\right)^{K-1-(x_i+y_i-1)} C_{x_i+y_i-1}^{x_i-1} \left(\frac{1}{2}\right)^{x_i+y_i-1},$$

$$P(x_i, y_i / "0") = P(x_i, y_i - 1) = C_{K-1}^{x_i+y_i-1} \left(\frac{1}{M}\right)^{x_i+y_i-1} \left(\frac{M}{M-1}\right)^{K-1-(x_i+y_i-1)} C_{x_i+y_i-1}^{y_i-1} \left(\frac{1}{2}\right)^{x_i+y_i-1}.$$

Вычитание единицы означает, что учитываются сигналы только от других (мешающих) абонентов, $C_{K-1}^{x_i+y_i-1}$ — число комбинаций, при которых $(K-1)$ мешающих сигналов попадают в правый полуслот, $\left(\frac{1}{M}\right)^{x_i+y_i-1}$ — вероятность того, что абонент передавал сообщение в левом полуслоте одного из M слотов, $\left(\frac{M}{M-1}\right)^{K-1-(x_i+y_i-1)}$ — вероятность того, что ни один из $K-1$ абонентов не передавал сообщений в заданном слоте, $C_{x_i+y_i-1}^{x_i-1}$ — число комбинаций, при которых $(K-1)$ мешающих сигналов попадают в левый полуслот, $\left(\frac{1}{2}\right)^{x_i+y_i-1}$ — вероятность попадания мешающих сигналов в левый полуслот заданного слота.

Так как искажения переданного бита в разных фреймах статистически независимы, то воспользуемся теоремой умножения вероятностей:

$$P(x_1, y_1, ..., x_N, y_N / z) = \prod_{i=1}^{N} P(x_i, y_{i,N} / z), \quad z = „0“, „1“.$$

Принимая решение, необходимо сравнить полученные вероятности для символов „0“ и „1“.

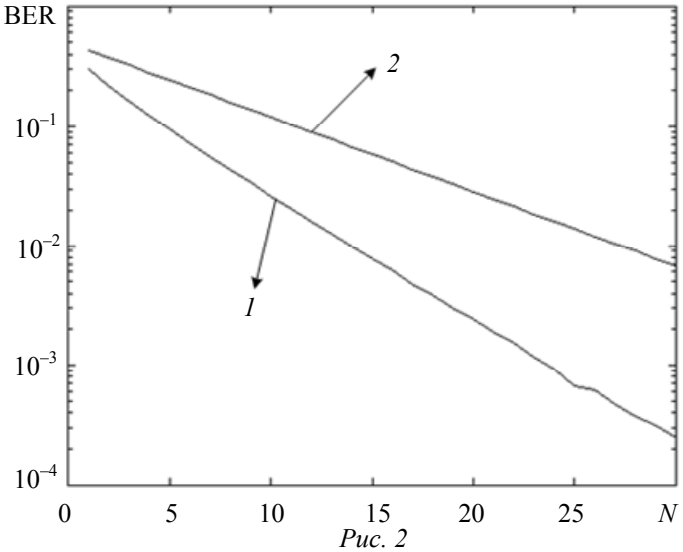


Рис. 2

$$\prod_{i=1}^{N} P(x_i, y_i / "1") \geq \prod_{i=1}^{N} P(x_i, y_i / "0").$$

После сокращения одинаковых сомножителей получим выражение

$$\prod_{i=1}^{N} C_{x_i+y_i-1}^{x_i-1} \geq \prod_{i=1}^{N} C_{x_i+y_i-1}^{y_i-1},$$

$$\prod_{i=1}^{N} x_i \geq \prod_{i=1}^{N} y_i.$$

Для оценки качества работы предлагаемого алгоритма было проведено моделирование. При этом производилось сравнение алгоритма оптимального приема (*1*) и алгоритма, используемого в OR-приемнике (*2*), по BER — вероятности ошибки на бит (рис. 2) для K=2, M=8.

Заключение. Результаты моделирования показали эффективность предложенного алгоритма, обеспечивающего выигрыш по вероятности ошибки на бит над OR-приемником. Для рассматриваемой системы, в которой K=2, M=8, моделированием получено, что выигрыш по вероятности ошибки на бит составляет практически два порядка.

СПИСОК ЛИТЕРАТУРЫ

1. *Zigangirov K. Sh.* Theory of code division multiple access communication. John Wiley & Sons, 2004. 400 p.
2. *Favi E., Charbon C.* Techniques for fully integrated intra-/inter-chip optical communication // Design Automation Conf. 2008. P. 343—344.
3. *Ando H., Kameda S., Iwata A.* Principal component analysis-based object detection/recognition chip for wireless interconnected three-dimensional integration // Jap. J. of Appl. Phys. 2008. Vol. 47. P. 2746—2748.
4. *Carusone T.* Future chip-to-chip interconnect technologies // CMOS Emerging Technologies Spring Conf. 2009. P. 156—158.
5. *Agdam M. K.* A low-power high-speed 4-bit adc for ds-uwb communications // IEEE Computer Society Annual Symp. on VLSI. 2007. P. 506—507.
6. *Moore S. S. B., Sellathamby C., Iniewski K.* Chip to chip communications for terabit transmission rates // IEEE Asia Pacific Conf. on Circuits and Systems. 2008. P. 1558—1561.
7. *Прокис Дж.* Цифровая связь. М.: Радио и связь, 2000. 798 с.

Сведения об авторах

Константин Борисович Гурнов — Санкт-Петербургский государственный университет аэрокосмического приборостроения, кафедра моделирования вычислительных и электронных систем; ассистент; E-mail: kocta4212@mail.ru

Григорий Сергеевич Евсеев — канд. техн. наук, доцент; Санкт-Петербургский государственный университет аэрокосмического приборостроения, кафедра моделирования вычислительных и электронных систем; E-mail: egs@vu.spb.ru

Рекомендована кафедрой
№ 51 безопасности информационных систем

Поступила в редакцию
01.02.13 г.

УДК 519.711.4

Е. А. Крук, Д. А. Маличенко

РАСЧЕТ ЗАДЕРЖКИ ПРИ ИСПОЛЬЗОВАНИИ КОДИРОВАНИЯ НА ТРАНСПОРТНОМ УРОВНЕ СЕТИ ПЕРЕДАЧИ ДАННЫХ

Рассматривается задача определения выигрыша от использования кодирования на транспортном уровне сети передачи данных. Рассчитана задержка кодированных сообщений с учетом неэкспоненциального характера задержки входящих в сообщения пакетов.

Ключевые слова: *транспортное кодирование, коды, исправляющие ошибки.*

Введение. Для уменьшения средней задержки передачи сообщений в сетях с коммутацией пакетов Г. А. Кабатянский и Е. А. Крук [1, 2] предложили метод транспортного кодирования, или кодирования на транспортном уровне сети.

При кодировании на транспортном уровне пакеты, из которых состоит подготовленное к передаче сообщение, рассматриваются как символы некоторого алфавита, а само сообщение — как вектор над этим алфавитом. Вектор-сообщение кодируется с помощью некоторого помехоустойчивого кода, в результате чего к сообщению добавляются избыточные символы — пакеты и получается кодированное сообщение.

При передаче кодированных сообщений возрастает нагрузка на сеть, что ведет к увеличению среднего времени задержки при передаче пакетов, входящих в сообщение. Однако для восстановления сообщения узлу-адресату в силу свойств помехоустойчивого кода не требуются все переданные пакеты. Сообщение может быть восстановлено по их части, что позволяет при сборке сообщения не ждать некоторых „задержавшихся“ пакетов. Таким образом,

использование транспортного кодирования приводит к двум противоположным эффектам — негативному, состоящему в увеличении среднего времени передачи пакетов, и позитивному, связанному с облегчением правил приема сообщений. При довольно общих ограничениях на организацию сети суммарное влияние указанных эффектов приводит к уменьшению средней задержки сообщений в сети.

Транспортное кодирование рассматривалось в значительном числе публикаций [3—11]. В настоящей статье выполнен расчет условий использования кодирования на транспортном уровне сети.

Модель сети. Рассмотрим модель сети передачи данных с коммутацией пакетов. Сеть имеет M каналов, емкость i-го канала равна C_i. Будем считать, что каналы сети абсолютно надежны, если всегда выполняется следующее неравенство

$$P_{\text{ош}} < P_{\text{ош.д}}, \tag{1}$$

где $P_{\text{ош}}$ — вероятность получения узлом-адресатом искаженного сообщения, $P_{\text{ош.д}}$ — допустимая вероятность ошибки при получении адресатом сообщения. Все узлы сети предполагаются абсолютно надежными и выполняющими операции по коммутации пакетов. Считается, что время обработки пакета в узле пренебрежимо мало. Время передачи пакета по каналу имеет экспоненциальное распределение с математическим ожиданием $1/\mu$. Если канал занят, пакет встает в очередь. Каждое сообщение, поступающее в сеть, разбивается на K одинаковых пакетов. Длина каждого пакета составляет s бит. Трафик, поступающий в сеть от внешних источников, образует пуассоновский процесс с интенсивностью γ (пакетов в секунду). Обозначим через λ_i среднее число пакетов, проходящих по i-му каналу в секунду, тогда полный трафик сети равен

$$\lambda = \sum_{i=1}^{M} \lambda_i .$$

Определить закон распределения времени задержки пакета в сети довольно сложно. Интервал времени между последовательными моментами поступления двух пакетов в канал не может быть меньше времени передачи первого из них по указанному каналу. Таким образом, задержки пакетов в сети являются зависимыми величинами. Однако если пакеты, передающиеся по одному каналу, пришли из разных каналов или если пакеты, пришедшие по одному каналу, отправляются по разным каналам, можно предположить, что эта зависимость уменьшится. Как показал Клейнрок [12, 13], для сетей со средней связанностью задержки пакетов можно считать независимыми случайными величинами. В этом случае i-й канал можно представить в виде системы массового обслуживания с потоком интенсивностью λ_i, на входе распределенным по пуассоновскому закону, и временем обслуживания, распределенным по показательному закону со средним $\dfrac{1}{\mu C_i}$.

В реальной сети закон распределения времени задержки пакета, очевидно, зависит от топологии сети, процедуры маршрутизации и т.д. Однако известно, что для многих реальных сетей закон распределения времени задержки пакета близок к экспоненциальному [12, 13]. Тогда можно предположить, что время задержки пакета в сети распределено экспоненциально с математическим ожиданием [12]:

$$\overline{t}(\lambda, \mu) = \sum_{i=1}^{M} \frac{\lambda_i}{\gamma} \frac{1}{\mu C_i - \lambda_i} . \tag{2}$$

Если рассмотреть случай, когда все M каналов имеют одинаковую пропускную способность, а внешний трафик равномерно распределяется между каналами (так что интенсив-

ности потоков пакетов для всех каналов одинаковы), то выражение (2) можно записать следующим образом:

$$\overline{t}(\lambda,\mu)=\sum_{i=1}^{M}\frac{\overline{l}}{\mu C}\frac{1}{1-\rho}, \tag{3}$$

где $\overline{l}=\dfrac{\lambda}{\gamma}$ — средняя длина пути, проходимого пакетом по сети, $\rho=\dfrac{\lambda}{\mu C}$ — загрузка сети, $C=\sum_{i=1}^{M}C_i$ — суммарная емкость каналов сети. Значение загрузки сети в данном случае совпадает с $\rho_i=\dfrac{\lambda_i}{\mu C_i}$ — загрузкой канала сети. Заметим, что для сетей средней и большой связанности с достаточно большим числом узлов значение ρ_i стремится к ρ.

Транспортное кодирование при экспоненциальной задержке пакетов. Рассмотрим модель сети с абсолютно надежными каналами, т.е. в предположении, что для каналов сети справедливо неравенство (1). В дополнение к сформулированной выше модели сети предположим, что время задержки пакета имеет экспоненциальное распределение, а его математическое ожидание $\overline{t}$ является функцией от λ и μ и определяется формулой (3). Такое предположение, по-видимому, справедливо для сетей с малой загрузкой.

Время задержки некодированного сообщения в сети T определяется максимальным временем задержки среди K пакетов данного сообщения

$$T=\max\{t_1,...,t_K\}, \tag{4}$$

где t_i — задержка i-го пакета сообщения. Таким образом, время задержки сообщения равно времени задержки пакета, пришедшего последним. Если переобозначить задержки пакетов сообщения в порядке возрастания $t_{1:K}\le t_{2:K}\le...\le t_{K:K}$, то $T=t_{K:K}$. В этом случае задержка кодированного сообщения T_{cod} будет равна

$$T_{\text{cod}}=t_{K:N}.$$

Воспользовавшись аппаратом ранговых статистик [14], математическое ожидание времени задержки i-го пришедшего пакета (при общем числе пакетов N) можно записать следующим образом:

$$M[t_{i:N}]=NC_{N-1}^{i-1}\int_0^1 P^{-1}(u)u^{i-1}[1-u]^{N-i}du, \tag{5}$$

где $P(t)$ — функция распределения времени задержки пакета в сети, $P^{-1}(u)$ — функция, обратная к $P(t)$. Для случая экспоненциального распределения времени задержки пакета в сети с использованием стандартного аппарата ранговых статистик формулу (5) можно переписать в следующем виде:

$$M[t_{i:N}]=\overline{t}(\lambda,\mu)\sum_{j=N-i+1}^{N}j^{-1}, \tag{6}$$

где $\overline{t}(\lambda,\mu)$ — среднее время задержки пакета в сети. Тогда среднюю задержку в сети некодированного сообщения $\overline{T}_1$ можно записать как

$$\overline{T}_1=M[t_{i:K}]=\overline{t}(\lambda,\mu)\sum_{j=1}^{K}j^{-1}, \tag{7}$$

где $\overline{t}(\lambda,\mu)$ определяется равенством (3). Сумму в правой части равенства (7) можно представить следующим образом [15]:

$$\sum_{j=1}^{K} j^{-1} = \varepsilon + \ln K + \frac{1}{2K} - \sum_{i=2}^{\infty} \frac{A_i}{K(K+1)...(K+i-1)}, \tag{8}$$

где $\varepsilon = 0,577...$ — постоянная Эйлера,

$$A_i = \frac{1}{i}\int_0^1 x(1-x)(2-x)(3-x)...(i-1-x)dx.$$

Отсюда получим оценку средней задержки некодированного сообщения:

$$\overline{T}_1 \geq (\varepsilon + \ln K)\overline{t}(\lambda,\mu). \tag{9}$$

Среднюю задержку кодированного сообщения $\overline{T}_2$ для заданного N, в соответствии с (6), можно записать следующим образом:

$$\overline{T}_2 = M[t_{K:N}] = \min_R \left\{ \overline{t}(\lambda / R,\mu) \sum_{j=N-K+1}^{N} j^{-1} \right\}, \tag{10}$$

где $\overline{t}(\lambda/R,\mu)$ — среднее время задержки пакета при трафике, возросшем в результате использования кодированных сообщений в $1/R$ раз. Отсюда с учетом (8) получим

$$\overline{T}_2 \leq \min_R \left\{ \overline{t}(\lambda / R,\mu) \ln\left(\frac{1}{1-R}\right) \right\}. \tag{11}$$

Среднюю задержку пакета при трафике, возросшем в $1/R$ раз, можно в соответствии с (3) записать как

$$\overline{t}(\lambda / R,\mu) = \frac{\overline{l}}{\mu C}\frac{R}{R-\rho}. \tag{12}$$

Минимизируя (11) по R, получим

$$\overline{T}_2 \leq \frac{\overline{l}}{\mu C}\frac{4\rho}{(1-\rho)^2}. \tag{13}$$

Выигрыш при использовании кодирования на транспортном уровне сети может быть получен в случае:

$$\overline{T}_1 - \overline{T}_2 > 0. \tag{14}$$

Подставив (8) и (13) в (14), получим условие выигрыша от использования кодирования

$$\varepsilon + \ln K > \frac{4\rho}{1-\rho}, \tag{15}$$

откуда видно, что применение кодирования на транспортном уровне сети, например при $K = 7$, выгодно при умеренной загрузке сети $\rho < 0,4$. В этом случае при загрузке $\rho = 0,3$ средняя задержка сообщения при использовании кодирования уменьшается более чем в 1,5 раза. Очевидно, что с увеличением K диапазон загрузок сети, пригодных для использования кодирования, увеличивается. Расчеты по точным формулам показывают, что введение кодирования на транспортном уровне сети снижает среднюю задержку сообщения практически при любых значениях начальной загрузки сети, хотя выигрыш уменьшается с ростом ρ.

Транспортное кодирование при неэкспоненциальных моделях задержки. Выше для расчета задержки сообщения использовалась экспоненциальная модель задержки пакета. Далее расчет выполним с помощью программы имитационного моделирования. Программа моделирует ожидание пакетов в очереди и передачу по каналу. Каждый отдельный канал пред-

ставляет собой систему массового обслуживания. Имитационная модель задается следующими параметрами:

1) топология сети, представленная с помощью матрицы смежности;

2) матрица интенсивностей потока;

3) матрица емкостей каналов;

4) таблица маршрутизации.

Распределение задержки пакетов обусловлено только самой имитационной моделью. Так же, как и ранее, будут рассматриваться сети, вся нагрузка по передаче пакетов в которых распределяется равномерно по всей сети, т.е. все каналы одинаково загружены. Чтобы задать такую сеть для программы имитационного моделирования, сделаем одно дополнительное допущение. Будем считать, что трафик между каждой парой узлов „источник—получатель“ одинаков и параметры маршрутов (длина и количество) также одинаковы. Тогда зададим только одну пару узлов „источник—получатель“ с числом маршрутов, равным длине сообщения. Чтобы учесть увеличение загрузки сети, например, при использовании транспортного кодирования, будем пропорционально увеличивать загрузку на каждом канале. В случае использования транспортного кодирования загрузка каналов возрастет в R раз по сравнению со случаем без кодирования, где R — скорость используемого кода. Емкость всех каналов положим равной единице.

На рис. 1 представлены зависимости выигрыша T_1/T_2 от скорости кода при k=8. Выигрыш рассчитан с использованием экспоненциальной модели задержки пакета и с помощью имитационной модели (цифры со штрихом) для разной длины путей (*а* — 1, *б* — 3) между отправителем и получателем сообщений при разных значениях загрузки сети ρ (*1*, *1′* — 0,2; *2*, *2′* — 0,4; *3*, *3′* — 0,6).

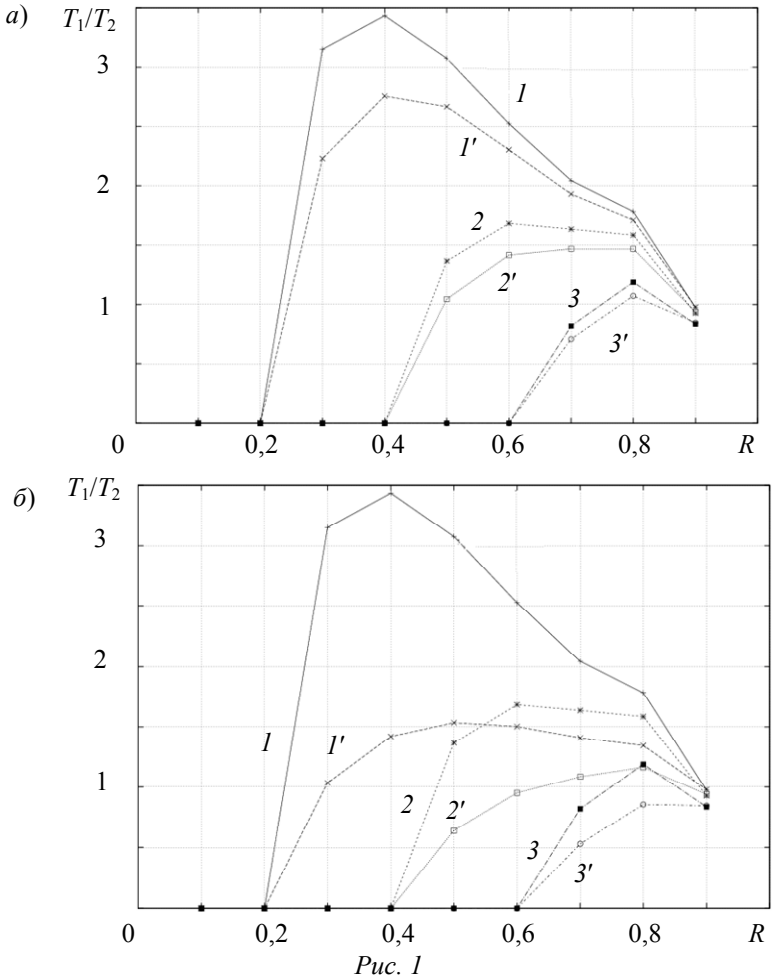


Рис. 1

Из рисунка видно, что с увеличением путей возрастает погрешность расчета, связанная с допущением об экспоненциальной задержке пакетов. Для иллюстрации этого факта гистограммы экспоненциального распределения (*1*) и полученного имитационным моделированием распределения (*2*) при длине пути 3 приведены на рис. 2.

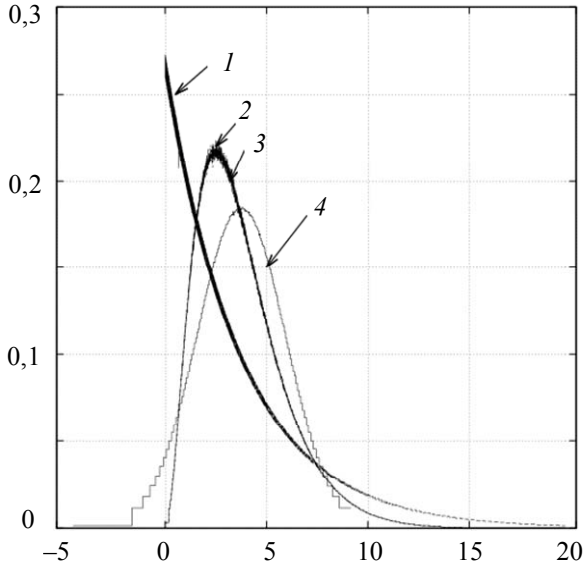


Рис. 2

Из рисунка видно, что распределения сильно различаются по форме. Дисперсии распределений также различны. Рассмотрим причины изменения. С увеличением длины маршрута до трех каждый пакет на пути от источника до получателя сообщения должен пройти три системы массового обслуживания. Таким образом, задержка пакета представляет собой сумму как минимум трех случайных величин, распределенных по одному и тому же экспоненциальному закону. Точное количество случайных величин в сумме зависит от размера очереди в каждой системе массового обслуживания, т.е. от загрузки сети. Известно, что сумма r случайных величин, распределенных по одному и тому же экспоненциальному закону, распределена по закону Эрланга. На рис. 2 также приведены распределения Эрланга 3-го порядка (*3*) и нормального распределения (*4*). Математические ожидания всех четырех распределений одинаковы. Дисперсия нормального закона распределения задана такой же, как у распределения, полученного с помощью имитационной модели. В остальных распределениях дисперсия рассчитывается по уже заданным параметрам.

Значение выигрыша от кодирования, рассчитанное с использованием экспоненциального распределения (рис. 1, *б*), существенно больше значения, полученного с помощью имитационного моделирования. В качестве альтернативы экспоненциальному закону распределения для расчета задержки сообщения рассмотрим закон распределения Эрланга и нормальный закон.

На рис. 3 представлен выигрыш от кодирования в зависимости от скорости кода, рассчитанный с помощью этих двух законов распределения (*2* — имитационная модель). Видно, что оценки выигрыша от кодирования, основанные на эрланговом распределении задержки пакета (*3*) и на нормальном распределении точнее соответствующей оценки, основанной на экспоненциальном законе распределения (*1*).

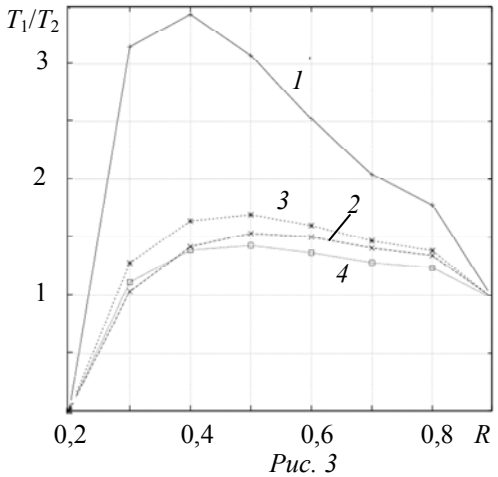


Рис. 3

Выводы. Сравнение значений выигрыша от использования кодирования на транспортном уровне сети передачи, полученных в результате расчетов и имитационного моделирования, показали, что:

— существует широкий набор параметров сети, для которых использование транспортного кодирования обеспечивает выигрыш по средней задержке сообщений;

— принятая в работах [1, 2] для аналитических расчетов модель, основанная на экспоненциальном характере задержки пакетов сети, имеет ограниченные пределы использования. Во многих случаях более точные результаты дает использование моделей, предполагающих, что задержка пакетов распределена по закону Эрланга или нормальному закону;

— подбор закона распределения задержки пакетов для проведения аналитических расчетов требует учета длины путей, проходимых пакетами в сети.

СПИСОК ЛИТЕРАТУРЫ

1. *Кабатянский Г. А., Крук Е. А.* Кодирование уменьшает задержку // X Всесоюз. школа-семинар по вычислительным сетям. Ч. 2. М.-Тбилиси, 1985. С. 23—26.
2. *Кабатянский Г. А., Крук Е. А.* Об избыточном кодировании на транспортном уровне сети передачи данных // Помехоустойчивое кодирование и надежность ЭВМ. М.: Наука, 1987. С. 143—150.
3. *Vvedenskaya N. D.* Large Queuing System where Messages are Transmitted via Several Routes // Problems of Information Transmission. 1998. Vol. 34, N 2. P. 180—189.
4. *Krouk E., Semenov S.* Application of Coding at the Network Transport Level to Decrease the Message Delay // Proc. of 3rd Intern. Symp. on Communication Systems Networks and Digital Signal Processing. Staffordshire University, UK, 2002. P. 109—112.
5. *Крук Е. А., Прохорова В. Б.* Расчет вероятностных характеристик для дискретных каналов с памятью // ИУС. 2007. № 5(30). С. 56—57.
6. *Башун В. В., Сергеев А. В.* Модель и протокол передачи видеоданных в реальном времени по беспроводному каналу // ИУС. 2007. № 6(31). С. 20—27.
7. *Alon N., Luby M.* A linear time erasure codes with nearly optimal recovery // IEEE Trans. on Inf. Theory. 1996. Vol. 42, N 6. P. 1732—1736.
8. *Luby M., Mitzenmacher M., Shokrollahi M. A., Spielman D. A., Stemann V.* Practical loss-resilient codes // Proc. of the 29th Ann. Symp. Theory of Computing. 1997. Vol. 42, N 6. P. 150—159.
9. *Luby M.* LT Codes // Proc. of the 43rd Annual IEEE Symp. on Foundations of Comp. Science. 2002.
10. *Krouk E. E., Semenov S.* Transmission of a Message During Limited Time with the Help of Transport Coding // Proc. of ICETE 2005. Intern. Conf. on E-business and Telecommunication Networks. 2005. P. 88—93.
11. *Kabatiansky G., Krouk E., Semenov S.* Error Correcting Coding and Security for Data Networks. Analysis of the Superchannel Concept. Wiley, 2005. 288 p.
12. *Клейнрок Л.* Вычислительные системы с очередями. М.: Мир, 1979. 600 с.
13. *Клейнрок Л.* Коммуникационные сети. Стохастические потоки и задержки сообщений. М.: Наука, 1970. 256 с.
14. *Дэйвид Г.* Порядковые статистики. М.: Наука, 1979. 340 с.
15. *Градштейн И. С., Рыжик И. Р.* Таблицы интегралов, сумм, рядов и произведений. М., 1963. 1100 с.

Сведения об авторах

Евгений Аврамович Крук — д-р техн. наук, профессор; Санкт-Петербургский государственный университет аэрокосмического приборостроения, кафедра безопасности информационных систем; E-mail: ekrouk@vu.spb.ru

Дмитрий Александрович Маличенко — Санкт-Петербургский государственный университет аэрокосмического приборостроения, кафедра безопасности информационных систем; ассистент; E-mail: dml@vu.spb.ru

Рекомендована кафедрой
№ 51 безопасности информационных систем

Поступила в редакцию
01.02.13 г.

УДК 004.728.3.057.4

Е. В. Пустовалов, А. М. Тюрликов

АНАЛИЗ РЕЖИМОВ ЭНЕРГОСБЕРЕЖЕНИЯ МОБИЛЬНОГО ПОЛЬЗОВАТЕЛЬСКОГО УСТРОЙСТВА

Рассматриваются различные режимы энергосбережения для мобильного абонентского устройства, основанные на его периодическом отключении. На основе известной модели входного потока проведена оценка энергопотребления устройства и средней задержки сообщений.

Ключевые слова: *энергосбережение, мобильное устройство, режим ожидания, входной поток со всплесками.*

Введение. На сегодняшний день наблюдается стремительный рост программно-аппаратных возможностей мобильных пользовательских устройств и, как следствие, их повышенное энергопотребление. Таким образом, важной задачей является поиск алгоритмов снижения энергопотребления и продления времени непрерывной работы мобильного устройства. Один из путей решения задачи — оптимизация работы устройства в перерывах между сеансами приема данных. Как правило, в современных мобильных устройствах периоды приема данных перемежаются с периодами ожидания. В литературе такой тип трафика называют „поток со всплесками“ [1]. Во время ожидания можно отказаться от непрерывного мониторинга канала связи, отключив приемопередатчик на определенное время. Однако поскольку приемник, как правило, не может определить длительность паузы, он должен периодически включаться на короткое время для мониторинга канала, чтобы иметь возможность оперативно получать сообщения от базовой станции. Такой режим работы назовем „режимом ожидания“. В том или ином виде режим ожидания реализован в большинстве стандартов связи третьего и четвертого поколений, таких как HSPA, WiMAX и LTE [2, 3].

При анализе режимов энергосбережения, основанных на периодическом отключении приемопередатчика, помимо величины энергопотребления необходимо учитывать требования к качеству обслуживания, которые определяются задержкой сообщения. Поступившее на базовую станцию во время режима ожидания новое сообщение не может быть принято пользователем до тех пор, пока его приемопередатчик не включится для мониторинга канала. Это приводит к следующему эффекту: чем реже приемник „просыпается“ в режиме ожидания, тем меньше энергии он потребляет, но тем больше задержка нового сообщения. Таким образом, встает оптимизационная задача: подобрать параметры режима энергосбережения так, чтобы минимизировать энергопотребление устройства при заданных ограничениях на качество обслуживания. В настоящей работе рассматривается такой показатель качества обслуживания, как средняя задержка.

Очевидно, что решение поставленной оптимизационной задачи зависит от характера трафика и алгоритма функционирования устройства в режиме ожидания. В настоящей работе анализируются энергопотребление и средняя задержка для типового режима энергосбережения с несколькими циклами ожидания, а также модели входного потока со всплесками.

Режимы энергосбережения. Рассмотрим простейший режим энергосбережения, проиллюстрированный на рис. 1. После окончания приема очередной порции данных запускается таймер с интервалом (тайм-аутом) T_1. Если по истечении T_1 не пришло новых сообщений, то устройство переходит в режим ожидания. В режиме ожидания все время функционирования разбито на циклы ожидания длиной L. Устройство выполняет мониторинг канала в течение B единиц времени в начале каждого цикла ожидания. При поступлении в цикле ожидания

на базовую станцию сообщений для пользователя данные сохраняются в буфере до начала следующего цикла, после чего устройство включается и принимает очередную порцию данных. По окончании приема данных описанная схема повторяется. Данный режим энергосбережения характеризуется набором из трех параметров (T_1, L, B).

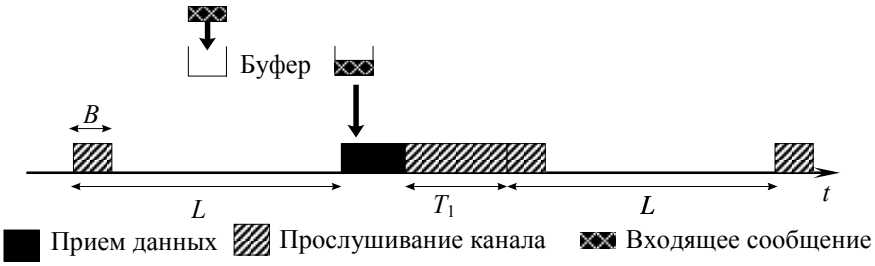


Рис. 1

Для повышения гибкости настройки параметров энергосбережения в современных стандартах мобильной связи предусмотрен так называемый режим с короткими и длинными циклами (рис. 2). По истечении времени T_1 система переходит в режим ожидания с параметрами L_1 и B_1. Одновременно с переходом в режим ожидания с короткими циклами запускается таймер с T_2. По истечении T_2 устройство переходит в режим ожидания с длинными циклами с параметрами L_2 ($L_2 > L_1$) и B_2 ($B_2 \le B_1$). Работа устройства в коротких и длинных циклах ожидания аналогична работе в простом режиме.

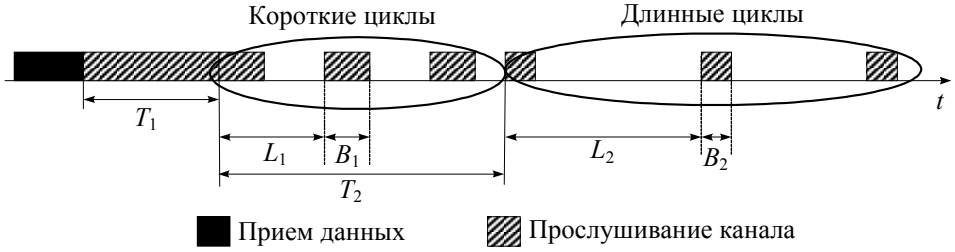


Рис. 2

Заметим, что при $L_2 = L_1$ и $B_2 = B_1$ режим с двумя типами циклов сводится к простому режиму энергосбережения. Кроме того, существуют другие возможные сценарии функционирования устройства в состоянии энергосбережения, однако в настоящей работе анализируется режим с короткими и длинными циклами, поскольку именно он используется в современных сетях связи третьего и четвертого поколений 3GPP HSPA и 3GPP LTE [2].

Модель входного потока. Для анализа описанных режимов энергосбережения необходимо задать модель трафика. Как правило, трафик реального устройства имеет сложный характер, в нем присутствует несколько потоков от различных приложений. Для упрощения анализа реальный трафик пользователя аппроксимируют одной из математических моделей, параметры которой рассчитываются на основе параметров реального трафика. Дальнейший анализ режимов энергосбережения проводится на модели входного потока со всплесками [4], которая является одной из стандартных моделей тестирования производительности систем связи, основанных на стандартах 3GPP.

Модель потока со всплесками описывается двумя параметрами: средним размером порции данных (всплеска) $\overline{s}$ и средней интенсивностью их поступления λ. Размер конкретной порции данных и временной интервал между ними являются случайными величинами. Интервалы между поступлениями данных распределены по экспоненциальному закону с параметром λ. Закон распределения размера порции данных может быть произвольным с математическим ожиданием $\overline{s}$, например, логнормальным. Интервал времени до прихода в систему новых данных отсчитывается от момента окончания приема предыдущей порции, таким образом, в каждый момент времени в буфере может находиться не более одной порции данных.

Скорость приема данных будем считать постоянной и равной R. Таким образом, математическое ожидание времени приема порции данных ($\overline{t}_{rx}$) равно

$$\overline{t}_{rx} \triangleq E\left[t_{rx}\right] = \frac{\overline{s}}{R}.$$

Анализ режима энергосбережения. При работе в режиме ожидания мобильное устройство может находиться в одном из двух состояний: „off“, в котором приемопередатчик выключен, и „on“, в котором устройство выполняет мониторинг канала или принимает данные. Пусть ζ_{on} — энергопотребление устройства в состоянии „on“, а ζ_{off} — в состоянии „off“ ($\zeta_{\text{off}} << \zeta_{\text{on}}$). Тогда общее среднее энергопотребление устройства равно

$$P = \eta_{\text{on}}\zeta_{\text{on}} + \eta_{\text{off}}\zeta_{\text{off}}, \qquad (1)$$

где η_{on} и η_{off} — доля времени нахождения устройства в состоянии „on“ и „off“. Поскольку конкретные значения констант ζ_{on} и ζ_{off} устанавливает производитель оборудования, то при анализе ограничимся вычислением величин η_{on} и η_{off}.

Определим долю времени, в течение которого приемник находится в состоянии „off“, следующим образом:

$$\eta_{\text{off}} \triangleq \lim_{T\to\infty} \frac{T_{\text{off}}(T)}{T},$$

где T — общее время работы системы; $T_{\text{off}}(T)$ — время, в течение которого абонентское устройство находится в состоянии „off“. Доля времени пребывания в состоянии „on“ может быть найдена исходя из условия нормировки

$$\eta_{\text{on}} + \eta_{\text{off}} = 1.$$

Обозначим промежуток времени: от момента начала приема текущей порции данных до момента начала приема следующей t_{cyc}. В заданном входном потоке последующая порция данных может поступить в систему только после окончания приема очередной, таким образом, поведение системы с момента начала приема нового сообщения не зависит от поведения системы в предыдущие моменты времени. Такой процесс называется регенеративным, а интервал t_{cyc} — циклом регенерации [5, 6]. Используя теорию регенеративного анализа, величину η_{off} можно вычислить по формуле

$$\eta_{\text{off}} = \frac{\mathrm{E}\left[t_{\text{off}}\right]}{\mathrm{E}\left[t_{\text{cyc}}\right]}, \qquad (2)$$

где t_{off} — время нахождения устройства в состоянии „off“ в цикле регенерации.

Напомним, что в режиме ожидания абонент слушает канал только B единиц времени в течение цикла длительности L. Пусть t_{drx1} и t_{drx2} — время нахождения в режиме с короткими и длинными циклами в интервале t_{cyc}, тогда

$$t_{\text{off}} = t_{drx1}\frac{L_1 - B_1}{L_1} + t_{drx2}\frac{L_2 - B_2}{L_2},$$

а математическое ожидание

$$\mathrm{E}\left[t_{\text{off}}\right] = \mathrm{E}\left[t_{drx1}\right]\frac{L_1 - B_1}{L_1} + \mathrm{E}\left[t_{drx2}\right]\frac{L_2 - B_2}{L_2}. \qquad (3)$$

Покажем, как найти математические ожидания t_{drx1}, t_{drx2} и t_{cyc}. В любом цикле регенерации возможно, что новые данные придут

1) до начала циклов ожидания (т.е. до истечения времени T_1). Поскольку время между приходом данных имеет экспоненциальное распределение, то вероятность возникновения такого события

$$p_1 = P(t < T_1) = 1 - e^{-\lambda T_1};$$

2) в течение коротких циклов ожидания (т.е. после истечения T_1, но до истечения T_2). Вероятность такого события

$$p_2 = P(T_1 < t < T_1 + T_2) = P(t > T_1) - P(t > T_1 + T_2) = e^{-\lambda T_1} - e^{-\lambda(T_1+T_2)};$$

3) в течение длинных циклов ожидания (т.е. по истечении T_2). Вероятность события

$$p_3 = P(t > T_1 + T_2) = e^{-\lambda(T_1+T_2)}.$$

Найдем величину $\mathrm{E}\left[t_{drx1}\right]$. В первом случае устройство не перейдет ни в один из режимов ожидания и

$$\mathrm{E}\left[t_{drx1} \mid t < T_1\right] = 0.$$

В третьем случае устройство пробудет в режиме ожидания с короткими циклами в течение T_2, после чего перейдет в режим с длинными циклами и

$$\mathrm{E}\left[t_{drx1} \mid t > T_1 + T_2\right] = T_2.$$

Рассмотрим подробно второй случай. Устройство находится в режиме с короткими циклами ожидания до начала приема новой порции данных, тогда

$$\mathrm{E}\left[t_{drx1} \mid T_1 < t < T_1 + T_2\right] = \mathrm{E}\left[t - T_1 \mid T_1 < t < T_1 + T_2\right] + \mathrm{E}\left[d \mid T_1 < t < T_1 + T_2\right], \tag{4}$$

где d — время от момента поступления новых данных в систему до момента начала их приема. Параметр d далее будем называть начальной задержкой. В силу отсутствия последействия у экспоненциального распределения (отсутствие памяти) [7] имеем

$$\mathrm{E}\left[t - T_1 \mid T_1 < t < T_1 + T\right] = \mathrm{E}\left[t \mid t < T_2\right].$$

Обозначим через $f(t)$ плотность экспоненциального распределения, тогда

$$\mathrm{E}\left[t \mid t < T_2\right] = \int_0^{T_2} t f(t \mid t < T_2) dt = \int_0^{T_2} t \frac{f(t)}{P(t < T_2)} dt = \frac{\int_0^{T_2} t\lambda e^{-\lambda t} dt}{1 - e^{-\lambda T_2}} = \frac{-e^{\lambda T_2}(T_2 + 1/\lambda) + 1/\lambda}{1 - e^{-\lambda T_2}}. \tag{5}$$

Найдем $\mathrm{E}\left[d \mid T_1 < t < T_1 + T_2\right]$. Пусть k — случайная величина ($0 \le k \le L_1$), определяемая моментом поступления нового сообщения в цикле регенерации длины L_1. Тогда задержка от момента поступления до момента приема равна

$$d = \begin{cases} 0, & \text{если } k \le B_1, \\ L_1 - k, & \text{если } k > B_1. \end{cases} \tag{6}$$

Заметим: если время прихода сообщения имеет экспоненциальное распределение, то на интервале фиксированной длины это время имеет равномерное распределение, согласно свойству простейшего потока событий [7]. Таким образом, введенная выше случайная величина k имеет равномерное распределение. Опустив промежуточные выкладки, согласно (6), получим

$$\overline{d}_1 \triangleq \mathrm{E}\left[d \mid T_1 < t < T_1 + T_2\right] = \frac{L_1}{2} - B_1 + \frac{B_1^2}{2L_1}. \tag{7}$$

Аналогично для случая, когда новое сообщение прибудет в течение длинного цикла ожидания

$$\bar{d}_2 \triangleq \mathrm{E}\left[d \mid t > T_1 + T_2\right] = \frac{L_2}{2} - B_2 + \frac{{B_2}^2}{2L_2}.$$

Подставив (5) и (7) в (4), получим

$$\mathrm{E}\left[t_{drx1} \mid T_1 < t < T_1 + T_2\right] = \frac{-e^{-\lambda T_2}(T_2 + 1/\lambda) + 1/\lambda}{1 - e^{-\lambda T_2}} + \bar{d}_1,$$

и безусловное математическое ожидание

$$\mathrm{E}\left[t_{drx1}\right] = \left(\frac{-e^{-\lambda T_2}(T_2 + 1/\lambda) + 1/\lambda}{1 - e^{-\lambda T_2}} + \bar{d}_1\right)\left(e^{-\lambda T_1} - e^{-\lambda(T_1+T_2)}\right) + T_2 e^{-\lambda(T_1+T_2)}. \quad (8)$$

Аналогичным образом рассчитаем

$$\mathrm{E}\left[t_{drx2}\right] = \left(\frac{1}{\lambda} + \bar{d}_2\right)e^{-\lambda(T_1+T_2)}. \quad (9)$$

Средняя начальная задержка находится по формуле

$$\bar{d} \triangleq \mathrm{E}\left[d\right] = \bar{d}_1\left(e^{-\lambda T_1} - e^{-\lambda(T_1+T_2)}\right) + \bar{d}_2 e^{-\lambda(T_1+T_2)}. \quad (10)$$

Осталось найти среднюю длительность цикла регенерации, состоящего из времени приема данных, времени до поступления новой порции данных, начальной задержки нового сообщения. Тогда математическое ожидание t_{cyc} равно

$$\mathrm{E}\left[t_{\text{cyc}}\right] = \mathrm{E}\left[t_{rx}\right] + \mathrm{E}\left[t\right] + \mathrm{E}\left[d\right] = \bar{t}_{rx} + \frac{1}{\lambda} + \bar{d}. \quad (11)$$

Подставив (8) и (9) в (3), а (3) и (11) — в (2), окончательно получим долю времени, которую устройство проводит с выключенным приемопередатчиком.

Численные результаты. Заметим, что функции средней начальной задержки (10) и времени в энергосберегающих режимах (8) и (9) нелинейно зависят от параметров режима ожидания (L_1, B_1, T_1, L_2, B_2 и T_2). Это приводит к тому, что в общем случае при отсутствии ограничений на эти параметры нахождение оптимальных значений может быть непростой задачей. В реальных системах связи, как правило, задан набор возможных значений данных параметров, и решение оптимизационной задачи можно свести к перебору.

Ниже приведен типовой набор параметров трафика и режимов ожидания мобильного абонентского устройства.

Параметры трафика

Средний размер порции данных $\bar{s}$	10 КБ
Среднее время между поступлением данных $1/\lambda$	2 с
Скорость приема данных R	12,5 КБ/с

Параметры режимов энергосбережения

L_1	80 / 160 / 320 мс
B_1	10 мс
t_1	100 / 200 / 400 / 800 мс
L_2	640 / 1280 / 2560 / 5120 мс
B_2	2 / 4 / 6 / 8 / 10 мс
T_2	0,5 / 1 / 2 / 5 с

На рис. 3 приведена зависимость доли времени в состоянии „on“ от ограничения на среднюю задержку. Каждая точка на графике соответствует значению η_{on} при оптимальных параметрах режима ожидания, т.е. таких, для которых η_{on} минимально при заданном огра-

ничении на $\overline{d}$. Поскольку, согласно (1), энергопотребление устройства пропорционально величине η_{on} , точки на графике соответствуют минимальному значению энергопотребления.

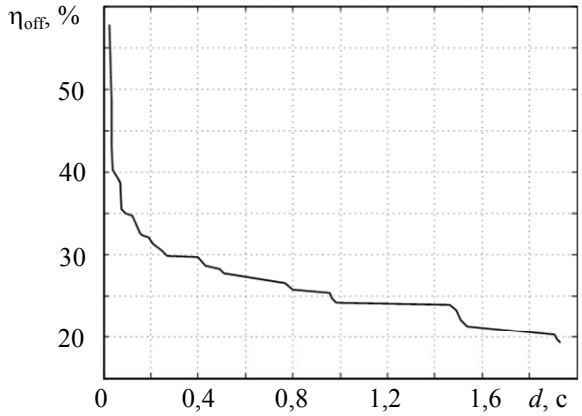


Рис. 3

Заключение. В работе рассмотрены типовые режимы энергосбережения мобильного пользовательского устройства, основанные на периодическом отключении приемопередатчика, а также описана методика оценки средней начальной задержки и энергопотребления. Показано, что, используя данную методику, можно подбирать оптимальные параметры режимов ожидания с учетом ограничения средней начальной задержки.

Отметим, что предложенная методика базируется на простой математической модели входного потока. Реальные потоки сложны, однако с той или иной степенью точности могут быть аппроксимированы рассмотренной моделью. Кроме того, описанный способ анализа применим и для более сложных систем с большим числом состояний. Критерием применимости методики является условие, при котором функционирование системы можно разбить на циклы регенерации.

СПИСОК ЛИТЕРАТУРЫ

1. *Kresch E., Kulkarni S.* A poisson based bursty model of internet traffic // Proc. of IEEE 11th Intern. Conf. on Computer and Information Technology. 2011. P. 255—260.
2. *Dahlman E., Parkvall S., Skold J., Beming P.* 3G evolution: HSPA and LTE for mobile broadband. Elsevier Ltd., 2008. 648 p.
3. *Ergen M.* Mobile broadband — including WiMAX and LTE. NY: Springer, 2009. 540 p.
4. CDMA2000 evaluation methodology. Version 1.0 (Revision 0). 3GPP2, 2004.
5. *Крэйн М., Лемуан О.* Введение в регенеративный метод анализа моделей. М.: Наука, 1982. 104 с.
6. *Анисимов А. В., Тюрликов А. М.* Анализ влияния изменения характеристик потока на энергозатраты мобильной станции // ИУС. 2010. № 6(49). С. 62—69.
7. *Феллер В.* Введение в теорию вероятностей и ее приложения. М.: Мир, 1967. Т. 2. 752 с.

Сведения об авторах

Евгений Васильевич Пустовалов — Санкт-Петербургский государственный университет аэрокосмического приборостроения, Институт компьютерной безопасности вычислительных систем и сетей; научный сотрудник; E-mail: eugeny@vu.spb.ru

Андрей Михайлович Тюрликов — д-р техн. наук, доцент; Санкт-Петербургский государственный университет аэрокосмического приборостроения, кафедра инфокоммуникационных систем; E-mail: turlikov@vu.spb.ru

Рекомендована кафедрой
№ 51 безопасности информационных систем

Поступила в редакцию
01.02.13 г.

УДК 004.056

Д. А. Ковалев, С. В. Беззатеев

ЗАЩИТА ПРОТОКОЛОВ УЛЬТРАЛЕГКОЙ АУТЕНТИФИКАЦИИ ОТ АТАК НА LSB

Предложен подход к улучшению версии протокола взаимной аутентификации LMAP++ путем замены стандартной операции сложения по модулю 2^m на операцию сложения по модулю 2^m–1 и использованием только простейших арифметических операций. Проведено сравнение сложности предложенной версии со сложностью известных методов повышения надежности протокола LMAP++.

Ключевые слова: *RFID, ультралегкие протоколы, LMAP++, аутентификация.*

Введение. Ультралегкие протоколы аутентификации для RFID построены на простейших арифметических операциях. Такие протоколы предназначены для сфер, требующих массового использования RFID-меток.

Ультралегкая RFID-метка имеет существенные ограничения по вычислительным возможностям и памяти, поэтому такие распространенные криптографические решения по обеспечению безопасности, как RSA, DES, AES, не могут быть реализованы в криптографических функциях, используемых в ультралегких протоколах, в них применяется следующий набор операций [1]:

— $\oplus$ XOR — поразрядная операция ИСКЛЮЧАЮЩЕГО ИЛИ,

— $\vee$ OR — поразрядное логическое ИЛИ,

— $\wedge$ AND — поразрядное логическое И,

— + — сложение m-битных чисел с игнорированием переполнения (сложение по модулю 2^m).

Несмотря на существенные ограничения по вычислительным возможностям, к безопасности ультралегких RFID-меток предъявляются достаточно высокие требования:

— анонимность метки,

— взаимная аутентификация между RFID-считывателем и меткой при минимальном числе сообщений, которыми они обмениваются.

В ультралегких протоколах можно выделить следующие основные этапы.

1. Считыватель посылает некоторую, инициализирующую протокол, команду метке. На этот запрос RFID-метка всегда отвечает своим динамическим идентификатором.

2. Считыватель находит в базе ключи и статический идентификатор метки по полученному динамическому идентификатору. Далее считыватель генерирует случайные числа и использует их и ключ метки для создания сообщения, которое на следующем шаге будет использоваться для взаимной аутентификации.

3. Считыватель и метка обмениваются сообщениями аутентификации.

4. Обновляются ключи и динамический идентификатор на считывателе и метке.

В 2006 г. P. Peris-Lopez предложил несколько ультралегких протоколов взаимной аутентификации — LMAP [2], EMAP [1], M2AP [3], но в них было обнаружено множество уязвимостей [4, 5]. В 2007 г. Li и Wang предложили улучшенную версию протокола LMAP: SLMAP, в которой также были найдены слабые места [6, 7]. В 2008 г. Tieyan Li улучшил свой протокол и назвал его LMAP++ [8], улучшенная версия также имела недостатки [9, 10].

Основные уязвимости протоколов аутентификации ультралегких радиочастотных идентификаторов. Большинство атак на ультралегкие протоколы используют идентичность операции сложения по модулю 2^m и операции XOR ($\oplus$) для наименее значимых битов (LSB)

$$[a+b]_0 = a_0 \oplus b_0,$$
$$[a-b]_0 = a_0 \oplus b_0.$$

Для представления старших битов используется следующая формула:

$$[a+b]_i = a_i \oplus b_i \oplus s(a,b,i-1),$$
$$[a-b]_i = a_i \oplus b_i \oplus t(a,b,i-1),$$

где $0 \le i < m$, а $s(a,b,i) = ([a]_i \wedge [b]_i) \vee ([a]_i \oplus [b]_i \wedge s(a,b,i-1))$ определяет, происходит ли перенос единицы в старший бит при сложении a_i и b_i, $s(a,b,i) = 1$ означает наличие переноса единицы из младших битов в старшие.

Аналогичным образом определяется параметр $t(a,b,i)$ — заем единицы из старших битов при вычитании a_i из b_i.

На такой особенности соотношения операций арифметического сложения и сложения по модулю два построено большинство атак на ультралегкие протоколы. Эти атаки приводят к рассинхронизации информации, хранящейся на считывателе и метке, раскрытию секретной информации о метке, а также к возможности отслеживать метку даже после ее успешной аутентификации на считывателе.

Способы противодействия атакам, использующим уязвимости LSB. Для предотвращения проведения атак, построенных на уязвимости LSB, в некоторых протоколах предлагается использовать следующие операции. В протоколе ULAP [11], Gossamer [12] предлагается использовать легкую хэш-функцию MixBits. В ULAP динамический идентификатор передается не в открытом виде, а в виде хэш-функции от него. Для этого считыватель генерирует случайное число и отсылает его метке вместе с сообщением, которое служит командой инициализации протокола. Метка отвечает значением IDS_{ULAP} (рис. 1), вычисляемым по алгоритму:

```
IDS_ULAP=IDS;
for(i=0;i<32;i++)
{
  IDS_ULAP = (IDS_ULAP >>1) + IDS_ULAP + IDS_ULAP +n;
}
```

где IDSULAP >>1 — сдвиг вектора IDSULAP на 1 бит вправо.

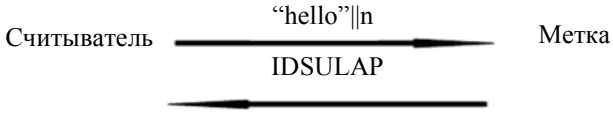


Рис. 1

В протоколах UMA-RFID [13], SASI [14], SULMA [15] при создании сообщений для взаимной аутентификации используется операция Rot(**x**,**y**), т.е. циклический сдвиг влево вектора **x**, на wt(**y**) позиций, где wt — вес Хемминга.

В протоколе RAPP [16] при создании сообщений используется операция перестановки Per(**x**,**y**) битов в векторе **x** в соответствии со значениями битов в векторе **y**.

Перестановка Per(**x**,**y**) выполняется следующим образом. Предположим, что **x** и **y** — два 96-битных числа, где

$$x = x_0 x_2 ... x_{95},\ x_i \in \{0,1\},\ i = 0,1,2,...,95,$$
$$y = y_0 y_2 ... y_{95},\ y_i \in \{0,1\},\ i = 0,1,2,...,95,$$

и вес Хемминга вектора **y** равен m ($0 \le m \le 95$), при

$$y_{k_1} = y_{k_2} = ... = y_{k_m} = 1, y_{k_m} = y_{k_{m+1}} = ... = y_{k_{95}} = 0,$$

где $0 \le k_1 < k_2 < ... < k_m \le 95$ и $0 \le k_{m+1} < k_{m+2} < ... < k_{95} \le 95$. Тогда перестановка Per(**x**,**y**)= $= x_{k_1}\ x_{k_2}\ ...\ x_{k_m}\ x_{k_{95}}\ ...\ x_{k_{m+2}}\ x_{k_{m+1}}$.

В протоколе EMAP [1] при обновлении ключей и динамического идентификатора метки используется операция Fp(**a**) при m=96, вектор **a** будет разбит на 24 блока по 4 бита, и для каждого блока будет вычисляться бит четности.

Пусть $\mathbf{a} = a_0, a_1, a_2, \ldots, a_{95}$, тогда

$$\mathrm{Fp}(\mathbf{a}) = (a_0 \oplus a_1 \oplus a_2 \oplus a_3, a_4 \oplus a_5 \oplus a_6 \oplus a_7, \ldots, a_{92} \oplus a_{93} \oplus a_{94} \oplus a_{95}).$$

Использование операции сложения по модулю 2^m–1. Для устранения возможности проведения атак, построенных на уязвимости LSB, предлагается заменить операцию сложения по модулю 2^m на операцию сложения по модулю 2^m–1. Реализовать эту операцию можно с помощью элементарных арифметических операций и архитектуры сумматора (рис. 2).

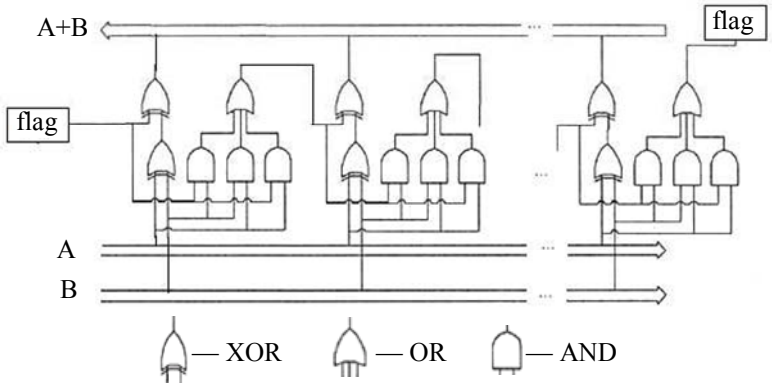


Рис. 2

Сложение по модулю 2^m –1 для чисел A и B можно провести за 5 шагов.

Шаг 1. C' =A+B mod 2^m, flag=1 если A+B > 2^m–1 и flag=0 — в противном случае.

Шаг 2. C'=C'+0+flag mod 2^m.

Шаг 3. D=C mod 2^m.

Шаг 4. D=D+1 mod 2^m, flag=1, если D=2^m–1, и flag=0 — в противном случае.

Шаг 5. C=C'+0+flag mod 2^m.

Таким образом, результатом сложения чисел A и B по модулю 2^m–1 будет число C.

При использовании операции сложения по модулю 2^m–1 исключаются уязвимости, существовавшие ранее вследствие идентичности операций сложения по модулю 2^m и XOR для LSB, так как равенства $[a+b]_0 = a_0 \oplus b_0$ и $[a-b]_0 = a_0 \oplus b_0$ не выполняются для операций арифметического сложения и вычитания по модулю 2^m–1.

В таблице сравниваются параметры операций, использовавшихся для предотвращения атаки по LSB.

Операции	Сложность в логических вентилях при m=96
MixBits	8120
Rot (**x**,**y**)	480
Permutation	~45794
Fp	468
Сложение по mod 2^m–1	173

Выводы. Предложена операция, предотвращающая атаки LSB, которая менее требовательна к вычислительным возможностям RFID-метки, чем предлагавшиеся ранее операции.

СПИСОК ЛИТЕРАТУРЫ

1. *Peris-Lopez P., Hernandez-Castro J. C., Estevez-Tapiador J. M., Ribagorda A.* EMAP: An Efficient Mutual Authentication Protocol for Low-cost RFID Tags // OTM Federated Conf. and Workshop: IS Workshop (IS'06). Montpellier, France: Springer-Verlag, 2006. Vol. 4277 of LNCS. P. 352—361.

2. *Peris-Lopez P., Hernandez-Castro J. C., Estevez-Tapiador J. M., Ribagorda A.* LMAP: A Real Lightweight Mutual Authentication Protocol for Low-cost RFID tags // Workshop on RFID Security (RFIDSec'06). Graz Austria, 2006.

3. *Peris-Lopez P., Hernandez-Castro J. C., Estevez-Tapiador J. M., Ribagorda A.* M2AP: A Minimalist mutual authentication protocol for low-cost RFID tags // 3rd Intern. Conf. on Ubiquitous Intelligence and Computing (UIC'06). 2006. Vol. 4159. P. 912—923.

4. *Barasz M., Boros B., Ligeti P., Loja K., Nagy D. A.* Breaking LMAP // Proc of RFIDSec. 2007. P. 11—16.

5. *Li T., Wang G., Deng R. H.* SecurityAnalysisona Family of Ultra-lightweight RFID Authentication Protocols // J. of Software. 2008. Vol. 3. P. 1—10.

6. *Safkhani M., Bagheri N., Naderi M., Sanadhya S. K.* Security Analysis of LMAP++, an RFID Authentication Protocol // 6th Intern. Conf. Internet Technology and Secured Transactions. 2011. P. 689—694.

7. *Hernandez-Castro J. C., Tapiador J. E., Peris-Lopez P., Clark J. A., Talbi E.* Metaheuristic Traceability Attack against SLMAP, an RFID Lightweight Authentication Protocol // Intern. J. Foundations of Computer Science. 2009. P. 543—553.

8. *Li T.* Employing Lightweight Primitiveson Low-Cost RFID Tags for Authentication // Vehicular Technology Conf. 2008. P. 770—776.

9. *Wangand S.-H., Zhang W.-W.* Passive Attack on RFID LMAP++ Authentication protocol // CANS. 2009. P. 185—193.

10. *Hernandez-Castro J. C., Tapiador J. E., Peris-Lopez P., Clark J. A., Talbi E.* Metaheuristic Traceability Attackagainst SLMAP, an RFID Lightweight Authentication Protocol // IPDPS'09. Proc. of the 2009 IEEE Intern. Symp. Parallel & Distributed Processing. 2009. P. 1—5.

11. *Tanenbaum A. S.* Structured Computer Organization. 2001.

12. *Barasz M., Boros B., Ligeti P., Loja K., Nagy D. A.* Breaking EMAP // SecureComm. 2007. P. 514—517.

13. *Li T., Wang G.* Security Analysis of Two UltraLightweight RFID Authentication Protocols // IFIPSEC'07. 2007. P. 109—120.

14. *Yu H.* SASI: A New Ultralightweight RFID Authentication Protocol Providing Strong Authentication and Strong Integrity // Dependable and Secure Computing. IEEE Transact. on Date of Publication. 2007.

15. *Kianersi M., Gardeshi M., Arjmand M.*SULMA: A Secure Ultra Light-Weight Mutual Authentication Protocol for Lowcost RFID Tags // Intern. J. of UbiComp. 2011. Vol. 2. P. 17.

16. *Peris-Lopez P., Hernandez-Castro J. C., Tapiador J. M. E., Ribagorda A.* Advances in Ultralightweight Cryptography for Low-cost RFID Tags: Gossamer Protocol // Workshop on Information Security Applications. 2008. Vol. 5379. P. 56—68.

Сведения об авторах

Данил Александрович Ковалев — аспирант; Санкт-Петербургский государственный университет аэрокосмического приборостроения, кафедра технологий защиты информации; E-mail: iostreamawm@gmail.com

Сергей Валентинович Беззатеев — д-р техн. наук, доцент; Санкт-Петербургский государственный университет аэрокосмического приборостроения, кафедра технологий защиты информации; заведующий кафедрой; E-mail: bsv@aanet.ru

Рекомендована кафедрой
№ 51 безопасности информационных систем

Поступила в редакцию
01.02.13 г.

ОБРАБОТКА ВИДЕОИНФОРМАЦИИ

УДК 004.627

А. И. Веселов, М. Р. Гильмутдинов, Б. С. Филиппов

МЕТОД ГЕНЕРАЦИИ СТОРОННЕЙ ИНФОРМАЦИИ ДЛЯ СИСТЕМ РАСПРЕДЕЛЕННОГО КОДИРОВАНИЯ ВИДЕОИСТОЧНИКОВ

На примере эталонной реализации кодека Discover описаны основные методы распределенного кодирования видеоисточников, проанализированы их преимущества и недостатки. Предложен новый метод генерации сторонней информации, основанный на иерархической оценке движения. Продемонстрирована эффективность кодека, использующего предложенный метод.

Ключевые слова: *сжатие видеофайлов, распределенное кодирование, временная (межкадровая) интерполяция видеоданных, оценка движения.*

Введение. Распределенное кодирование видеоданных (Distributed Video Coding, DVC) является сравнительно новым подходом к сжатию видеоисточника. Несмотря на то что теоретические предпосылки DVC были получены еще в 1970-е гг. [1, 2], активные исследования в данном направлении начались только в конце 1990-х гг. Это связано в основном с тем, что до недавнего времени распределенное кодирование рассматривалось как задача, не имеющая реального практического применения. Развитие технологий мобильной передачи данных привело к формированию новых требований к кодеру, учитывающих особенности мобильных видеоисточников: ограниченный, зачастую трудновосполняемый, объем аккумуляторной батареи и сравнительно малые вычислительные возможности мобильных устройств. Эти особенности накладывают существенные ограничения на допустимую сложность процедуры сжатия видеоданных на стороне мобильного передатчика. Кроме того, следует отметить, что описанные ограничения не принимались в расчет при разработке современных стандартов сжатия видеоданных ITU-T H.26x и ISO/IEC MPEG [3]. В связи с этим разработка подходов к сжатию видеоданных, учитывающих описанные выше особенности, является актуальной задачей.

Для решения этой задачи во многих работах в качестве перспективной технологии указывается DVC, поскольку в ее архитектуре заложено снижение сложности кодирования при сохранении степени сжатия. Основная сложность при этом переносится со стороны кодера на декодер: наиболее вычислительно сложная операция устранения временной избыточности, связанная с формированием ошибок предсказания на стороне кодера, заменяется процедурой интерполяции (или экстраполяции) кадров на стороне декодера. Блок, отвечающий за предсказание кадров на стороне декодера, принято называть блоком *генерации сторонней информации*. Ошибки, которые могут быть внесены в кадры в процессе интерполяции, исправляются с помощью проверочных битов некоторого помехоустойчивого кода, досылаемых кодером по запросам от декодера. Степень сжатия определяется количеством проверочных битов.

Из сказанного выше следует, что на эффективность устранения временной избыточности на стороне декодера и в конечном итоге — на сжатие будут влиять следующие факторы:

— точность метода генерации сторонней информации;

— эффективность исправления ошибок предсказания.

В настоящей статье рассматривается задача генерации сторонней информации, проанализирован метод генерации сторонней информации, используемый в эталонной реализации DVC кодека Discover [4], предложен подход, использующий более точную процедуру оценки движения.

Метод генерации сторонней информации, используемый в кодеке Discover. Наиболее популярным методом генерации сторонней информации является временная интерполяция кадров. В основе алгоритмов интерполяции лежат процедуры оценки и компенсации движения, позволяющие определить координаты одинаковых объектов на базовых кадрах и рассчитать положение этих объектов на промежуточном кадре. В кодеке Discover используется блоковая оценка движения [5], реализуемая в два этапа (рис. 1).

Рис. 1

Перед оцениванием движения базовые кадры подвергаются низкочастотной фильтрации с целью подавления шумов и увеличения точности последующего поиска. После однонаправленной оценки выполняется уточняющая *билатеральная* [6, 7] оценка с меньшим радиусом поиска, по завершении которой каждой координате на интерполированном кадре будет поставлен в соответствие вектор движения, т.е. на интерполированном кадре не будет участков с „коллизиями“ и „дырами“, которые возможны после первого шага [6]. Следующим шагом алгоритма является пространственное сглаживание множества векторов, объединенных в так называемое *векторное поле*. Для этого используется взвешенная медианная фильтрация. Для блока с координатами $\mathbf{p}_i = \begin{pmatrix} p^x \\ p^y \end{pmatrix}$ (под координатами блока понимаются координаты верхнего левого угла блока по вертикали p^y и по горизонтали p^x) и вектором $\mathbf{mv}_i = \begin{pmatrix} mv^x \\ mv^y \end{pmatrix}$ эта операция определена как:

$$\mathbf{mv}'_i = \arg \max_{\mathbf{mv} \in \{\mathbf{mv}_1, \ldots, \mathbf{mv}_N\}} \left[w_j \left(\sum_{j=1}^{N} \left| \left\| \mathbf{mv}_i - \mathbf{mv}_j \right\|_L - \left\| \mathbf{mv} - \mathbf{mv}_j \right\|_L \right| \right) \right],$$

где $\|\cdot\|_L$ — норма вектора, $\mathbf{mv}'_i$ — результат фильтрации, $\{\mathbf{mv}_1, \ldots, \mathbf{mv}_N\}$ — множество „связанных“ с $\mathbf{mv}_i$ векторов, в это множество входят векторы соседних блоков, а также вектор для блока с координатой $\mathbf{p}_i$ в предыдущем интерполированном кадре; w_j — весовые коэффициенты, определяемые как:

$$w_j = \frac{MSE(\mathbf{mv}_i, \mathbf{p}_i)}{MSE(\mathbf{mv}_j, \mathbf{p}_i)},$$

где $MSE(\mathbf{mv}, \mathbf{p})$ — оператор расчета среднего квадратического отклонения при применении вектора $\mathbf{mv}$ к блоку с координатой $\mathbf{p}$.

Полученное сглаженное билатеральное векторное поле используется на последнем шаге алгоритма для компенсации движения и формирования интерполированного кадра:

$$\tilde{F}^t(\mathbf{p}_i) = \frac{1}{2}\left[F^{t-1}(\mathbf{p}_i - \alpha\mathbf{mv}) + F^{t+1}(\mathbf{p}_i + (1-\alpha)\mathbf{mv}) \right],$$

где через $\tilde{F}^t(\mathbf{p}_i)$ обозначена интенсивность пиксела, находящегося на позиции $\mathbf{p}_i$ в интерполированном кадре $\tilde{F}^t$.

Метод генерации сторонней информации, основанный на иерархической оценке движения. Одним из существенных недостатков применяемого в Discover метода генерации сторонней информации является то, что в нем используется обычная блоковая оценка движения с полным перебором всех возможных векторов движения в некотором множестве. Учет корреляции векторов соседних блоков осуществляется только при медианной фильтрации векторного поля, но не используется в самой процедуре оценки движения. Такой подход в большинстве случаев неудобен для оценки так называемого *истинного движения* (*True Motion*) объектов [8], которое является определяющим фактором при интерполяции кадров.

Рассмотрим предлагаемый метод генерации сторонней информации, основанный на процедуре иерархической оценки движения. Эта процедура показывает хорошие результаты при решении схожей задачи — интерполяции кадров в алгоритмах преобразования кадровой скорости [9, 10]. Метод основан на постепенном уточнении векторов движения (начиная от оценки глобального смещения в рамках всего кадра и заканчивая оценкой локальных смещений объектов) посредством *иерархической* обработки кадров, использующей совокупность кадров различного разрешения [11]. Альтернативным способом является изменение размеров блоков при оценке движения с сохранением разрешения кадров. Такой подход учитывает корреляцию векторов и позволяет более точно оценивать истинное движение объектов, чем реализованный в Discover метод.

При оценке истинного движения также используется многоэтапный поиск: на начальном этапе осуществляется обычная блоковая билатеральная оценка движения, затем полученная оценка уточняется за счет использования векторов смежных блоков [8]. Поскольку при оценке движения реальный объект в кадре разбивается на несколько блоков, использование связей между блоками позволяет исправить ошибки поиска. Перед проведением дополнительного поиска выполняется оценка *надежности векторов движения*, полученных в ходе начального поиска. Надежность вектора — это количественный критерий, характеризующий степень влияния данного вектора на разброс значений векторов в его области [12]. Дополнительное разбиение каждого уровня иерархической оценки позволяет повысить точность оценки истинного движения. В работе [13] показано, что поиск с использованием полного перебора всех возможных векторов движения для блока приводит к появлению ошибок в определении истинного движения. В связи с этим в предложенном методе генерации сторонней информации предлагается использовать подоптимальный поиск, например, *градиентный спуск* [14]. Также предлагаемый алгоритм использует предобработку базовых кадров для выделения регионов со статичными объектами [15]. Эта информация позволяет существенно повысить точность оценки движения. В качестве модуля компенсации движения используется компенсация движения *с перекрытиями* (Overlapped Block Motion Compensation, OBMC), которая позволяет уменьшить блоковые искажения на интерполированном кадре [16]:

$$\tilde{F}^t(\mathbf{p}_i) = \frac{1}{2}\sum_{n=1}^{5} W_n \otimes \left[F^{t-1}(\mathbf{p}_i - \alpha\mathbf{mv}_n) + F^{t+1}(\mathbf{p}_i + (1-\alpha)\mathbf{mv}_n) \right],$$

где $\mathbf{mv}_1$, $\mathbf{mv}_2$, …, $\mathbf{mv}_5$ — вектор текущего блока $\mathbf{p}_i$ и его четырех соседей, W_1, W_2, …, W_5 — матрицы весовых коэффициентов, размер матриц совпадает с размерами блоков

$$\sum_{i=1}^{5} W_i = \mathrm{J},$$

где J — матрица, состоящая из всех единиц.

Окончательная схема предлагаемого метода генерации сторонней информации приведена на рис. 2.

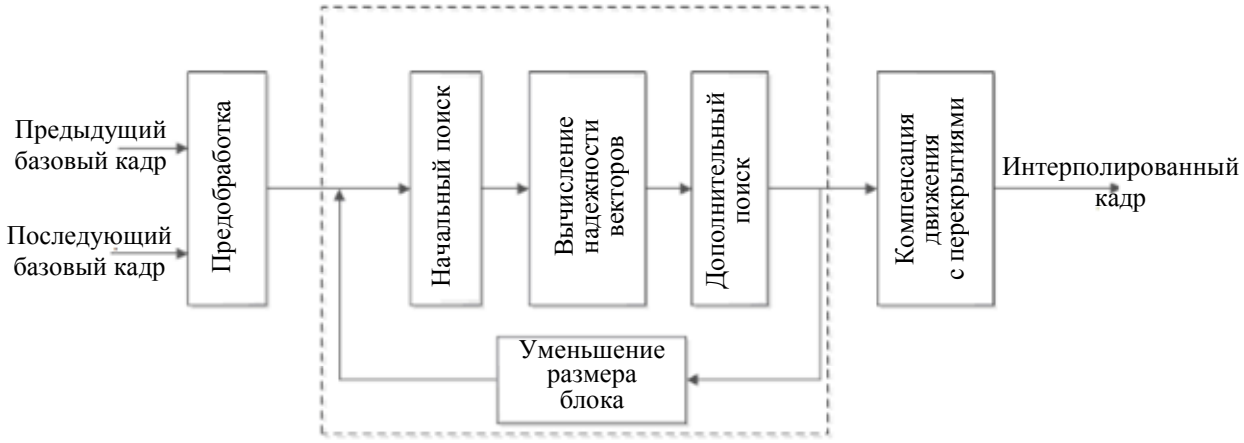


Рис. 2

Для оценки предлагаемого метода генерации сторонней информации был реализован видеокодек, работающий по следующей схеме [17]. Ключевые кадры обрабатываются, как в Discover. По восстановленным ключевым кадрам с помощью предложенного алгоритма генерируется сторонняя информация. Помехоустойчивое кодирование для исправления ошибок в сторонней информации не используется, т.е. промежуточные кадры обрабатываются только на стороне декодера и дополнительные биты от кодера не требуются. Интерполированный кадр выдается в выходной поток в качестве восстановленного кадра. Для оценки предложенной процедуры генерации сторонней информации были построены зависимости „скорость—искажение“ для различных кодеков на последовательностях из стандартного набора тестовых видеоданных [18]. В качестве критерия искажения использовалось усредненное по всем кадрам пиковое отношение сигнал/шум для яркостной компоненты (PSNR, Peak Signal-to-Noise Ratio). Скорость (Bitrate) рассчитывалась как среднее число килобитов, передаваемых в секунду. Частота следования кадров для тестовых видеопоследовательностей составляла 15 кадров в секунду, формат QCIF. В качестве сравниваемых кодеков были использованы (рис. 3):

— кодек стандарта H.264, режим Intra;

— кодек стандарта H.264, режим Inter;

— кодек стандарта H.264, режим Inter No Motion;

— кодек Discover;

— реализованный кодек (SUAI DVC).

Кодек H.264 Intra обрабатывает все кадры как ключевые. Остальные кодеки используют режим IBIB, т.е. каждый второй кадр обрабатывался как ключевой. В H.264 Inter предсказание осуществляется на кодере. Для H.264 Inter No Motion в качестве ошибки предсказания используется разница между базовым кадром и кодируемым.

На всех последовательностях, кроме Soccer, которая имеет низкую межкадровую корреляцию, SUAI DVC выигрывает у Discover в среднем на 0,5—1 дБ. При этом оба кодека проигрывают на всех последовательностях кодеку H.264 Inter (со сложным кодером). Если сравнивать кодеры низкой сложности, то в целом производительность DVC кодеков

приблизительно на том же уровне, что у H.264 Inter No Motion и, как правило, выше, чем у H.264 Intra.

В текущей версии кодека исправление ошибок предсказания не реализовано и, как следствие, дополнительные биты со стороны кодера для неключевых кадров не передаются. Это объясняет отсутствие по кодеку SUAI DVC для больших значений Y-PSNR.

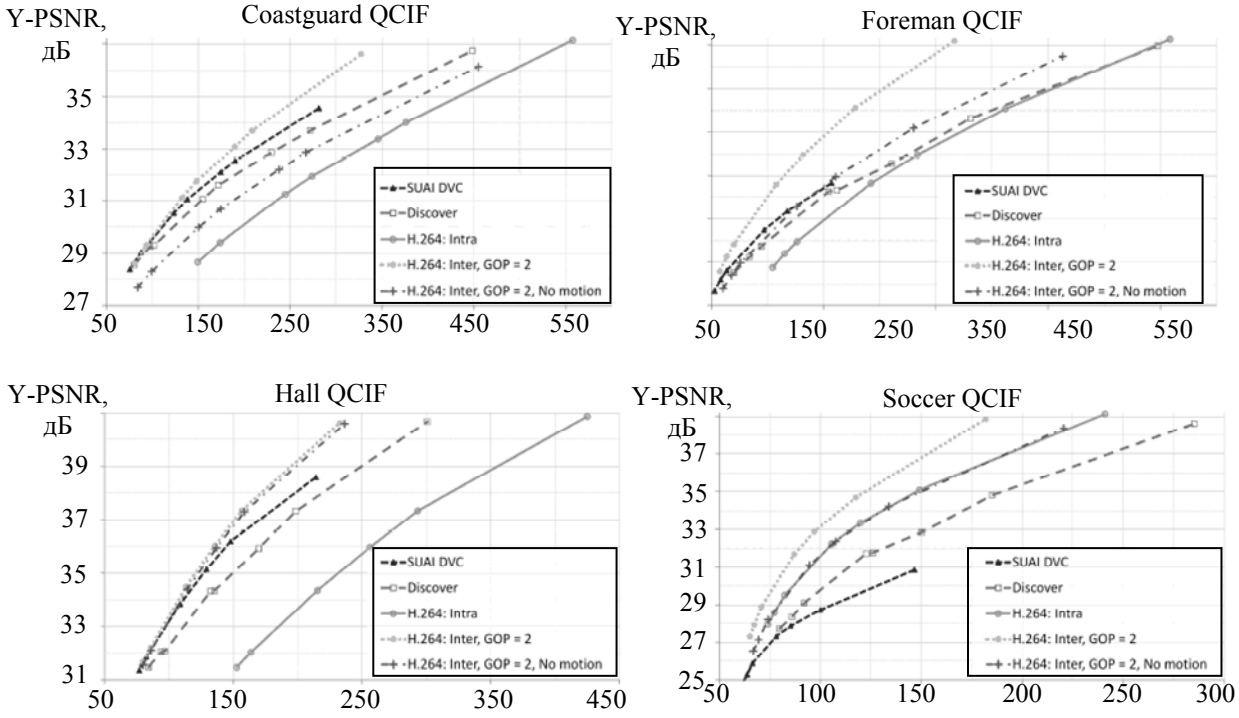


Рис. 3

Заключение. В работе приведено описание основных методов, используемых при распределенном кодировании видеоданных. Выделены наиболее значимые для этого подхода задачи и описаны способы их решения в эталонной реализации кодека Discover. Предложен новый более сложный метод генерации сторонней информации на стороне декодера, проведена его предварительная оценка. Реализован новый кодек, использующий предложенный метод. Показано, что для тестовых видеопоследовательностей с высокой межкадровой корреляцией реализованный кодек превосходит Discover в среднем на 0,5—1 дБ по критерию „скорость—искажение“. Таким образом, использование предложенного метода генерации сторонней информации позволяет повысить производительность DVC кодека без увеличения сложности кодирования.

СПИСОК ЛИТЕРАТУРЫ

1. *Wolf J. K., Slepian D.* Noiseless Coding of Correlated Information Sources // IEEE Transact. on Information Theory. 1973. Vol. 19, N 4. P. 471—480.

2. *Ziv J., Wyner A. D.* The Rate-Distortion Function for Source Coding with Side Information at the Decoder // IEEE Transact. on Information Theory. 1976. Vol. 22. P. 1—10.

3. Advanced video coding for generic audiovisual services. Recommendation ITU-T H.264 ISO/IEC 14496-10. 2003. 732 p.

4. DISCOVER project page [Электронный ресурс]: <www.discoverdvc.org>.

5. *Pereira F., Ascenso J., Brites C.* Improving Frame Interpolation with Spatial Motion Smoothing for Pixel Domain Distributed Video Coding // Proc. of 5th EURASIP Conf. on Speech and Image Processing, Multimedia Communications and Services. 2005. P. 252—257.

6. *Choi B.-T., Lee S.-H., Ko S.-J.* New Frame Rate Up-Conversion Using Bi-Directional Motion Estimation // IEEE Transact. on Consumer Electronics. 2000. Vol. 46. P. 603—609.

7. *Марковский С. Г., Тюрликов А. М.* Использование идентификаторов абонентов для резервирования канала множественного доступа // ИУС. 2008. № 2(33). С. 28—35.

8. *de Haan G.* et al. True Motion Estimation with 3-D Recursive Search Block-Matching // IEEE Transact. on Circuits and Systems for Video Technology. 1993. Vol. 3. P. 368—379.

9. *Lee Y.-L., Nguyen T.* Method and Architecture Design for Motion Com- pensated Frame Interpolation in High-Definition Video Processing // IEEE Intern. Symp. on Circuits and Systems (ISCAS). 2009. P. 1633—1636.

10. *Jeon B.-W., Lee G.-I., Lee S.-H., Park R.-H.* Coarse-to-fine Frame Interpolation for Frame Rate Up-Conversion Using Pyramid Structure // IEEE Transact. on Consumer Electronics. 2003. Vol. 49, N 3. P. 499—508.

11. *Houlding D., Vaisey J.* Pyramid Decompositions and Hierarchical Motion Compensation // Digital Video Compression: Algorithms and Technologies. Proc. of SPIE. 1995. Vol. 2419. P. 201—209.

12. *Huang A.-M., Nguyen T.* Correlation-Based Motion Vector Processing with Adaptive Interpolation Scheme for Motion-Compensated Frame Interpolation // IEEE Transact. on Image Proc. 2009. Vol. 18, N 4. P. 740—752.

13. *Braspenning R., De Haan G.* True Motion Estimation using Feature Correspondences // Proc. SPIE. Visual Communications and Image Proc. 2004. Vol. 5308. P. 396—407.

14. *Сэломон Д.* Сжатие данных, изображений и звука. М.: Техносфера, 2004. 368 с.

15. *Yu L., Heindlmaier M.* Optical Flow, Bilateral Filtering, Confidence Information and Motion Compensated Interpolation — a unifying approach. Technical report. Technische Universitat Munchen Institute for Data Processing. 2008. 99 p.

16. *Orchard M. T., Sullivan G. J.* Overlapped Block Motion Compensation: An Estimation-Theoretic Approach // IEEE Transact. on Image Processing. 1994. Vol. 3, N 5. P. 693—699.

17. *Gilmutdinov M., Veselov A., Filippov B.* Analysis of Side Information Generation Impact on Distributed Video Coding Performance // IEEE Proc. of XIII Intern. Symp. on Problems of Redundancy in Information and Control System. 2012. P. 26—31.

18. Набор тестовых видеопоследовательностей [Электронный ресурс]: <http://media.xiph.org/video/derf/>.

Сведения об авторах

Антон Игоревич Веселов — аспирант; Санкт-Петербургский государственный университет аэрокосмического приборостроения, кафедра инфокоммуникационных систем; E-mail: anton.veselov@gmail.com

Марат Равилевич Гильмутдинов — канд. техн. наук, доцент; Санкт-Петербургский государственный университет аэрокосмического приборостроения, кафедра инфокоммуникационных систем; E-mail: mgilmutdinov@gmail.com

Борис Сергеевич Филиппов — аспирант; Санкт-Петербургский государственный университет аэрокосмического приборостроения, кафедра инфокоммуникационных систем; E-mail: FilippovBoris@gmail.com

Рекомендована кафедрой
№ 51 безопасности информационных систем

Поступила в редакцию
01.02.13 г.

УДК 004.932

А. В. Афанасьева, Д. О. Иванов, Д. А. Рыжов

АЛГОРИТМ ВСТАВКИ ЦИФРОВЫХ ВОДЯНЫХ ЗНАКОВ ПРИ ИСПОЛЬЗОВАНИИ СТАНДАРТА H.264

Предложен алгоритм вставки цифровых водяных знаков (ЦВЗ) в видеопоток, закодированный по стандарту H.264. Описан способ согласования алгоритма извлечения ЦВЗ с антикоалиционными кодами.

Ключевые слова: *H.264, цифровые водяные знаки, антикоалиционные коды.*

Введение. Фильмы, а также другая видеопродукция часто подвергаются нелицензионному распространению, при этом правообладатели не получают прибыли. Для борьбы с таким неконтролируемым распространением видеопродукции можно использовать метод внесения индивидуального цифрового водяного знака (ЦВЗ) в каждую продаваемую копию фильма. Этот знак будет содержать идентификационную информацию о покупателе копии. Тогда по каждой нелицензионно распространяемой копии можно будет установить ее покупателя. Чтобы недобросовестные покупатели не уничтожали ЦВЗ, он должен быть устойчив к различным видам атак. Особое внимание необходимо обратить на коалиционные атаки, при которых несколько недобросовестных покупателей, используя свои копии, создают новую.

Задача защиты видеопродукции при помощи ЦВЗ может быть разделена на четыре этапа: построение множества идентификационных меток, внедрение одной из меток в видеопоследовательность, извлечение метки из пиратской копии видеопоследовательности, поиск участников коалиции по извлеченной метке.

Как правило, для работы с видеопотоком (вставка и извлечение метки) применяются алгоритмы обработки видеоданных, использующие специфические модели потока и атакующего, а при построении пространства меток и обнаружении участников пиратской коалиции применяются алгоритмы, разработанные в рамках теории помехоустойчмвого кодирования. Цель настоящей статьи — построить схему согласованной работы алгоритмов этих двух типов. Рассмотрим разработанные независимо решения для двух задач и на их базе предложим новый интегрированный подход. В работе исследуются методы вставки ЦВЗ для видеопотоков, сжатых в формате H.264, так как этот формат наиболее популярен и используется в различных приложениях.

Алгоритмы вставки ЦВЗ. При вставке цифровых водяных знаков в сжатый видеопоток возможно использовать только декодирование энтропийного кода, так как процедура полного перекодирования потока отнимает много вычислительных ресурсов, что создает дополнительные трудности при распространении видеопродукции. После декодирования энтропийного кода можно извлечь из потока (и следовательно, внести информацию) векторы движения и квантованные частотные коэффициенты дискретного косинусного преобразования (ДКП) макроблоков. Метод изменения частотных коэффициентов обеспечивает устойчивость к атакам при фиксированном уровне вносимых искажений, поэтому его активно исследуют [1—5], и в настоящей статье он тоже использован.

DC	$AC_{0,1}$		
$AC_{1,0}$	$AC_{1,1}$		

Рассмотрим блок 4×4 (см. рисунок) после применения ДКП и квантования, он состоит из основного DC коэффициента и набора AC коэффициентов, упорядоченных по частоте. Выделенные на рисунке низкочастотные AC коэффициенты содержат большую часть энергии, поэтому изменять нужно именно их, это обеспечит стойкость к атакам, связанным с обработкой кадра. Алго-

ритм вставки характеризуется тремя параметрами: глубина продавливания коэффициентов (L), количество изменяемых коэффициентов в блоке и число изменяемых блоков в кадре, он основан на правиле:

$$AC_{i,j} = AC_{i,j} \pm L,$$

знак определяется передаваемым битом. Стоит отметить, что для детектирования необходим исходный блок. Задав эти параметры, можно получить информационную емкость одного кадра.

Для определения сочетаний предельно допустимых значений параметров, не приводящих к существенному ухудшению визуального качества, алгоритма был исследован ряд видеофрагментов. Для оценки вносимых искажений применялся ряд метрик (SSIM, PSNR), а также проводилось субъективное визуальное оценивание. Для того чтобы вносимые искажения нельзя было заметить, необходимо на этапе предвычислений для вставки выбирать текстурные блоки (содержащие мало ненулевых коэффициентов). Отметим, что метод выбора блоков „открыт“, а секретным ключом является изменяемый коэффициент. Задачей атакующего будет угадывание коэффициента для изменения, так как если он изменит все коэффициенты, то произойдет значительная потеря в качестве.

Антикоалиционные коды. Существует несколько классов антикоалиционных кодов, стойкость которых к атакам с заданным размером коалиции доказана [6, 7]. Эти коды отличаются от кодов, исправляющих ошибки, тем, что вместо алгоритма декодирования используют алгоритм поиска участников коалиции по искаженной метке. Оба класса позволяют выявить участников коалиции, если она не превышает заданного размера, при этом гарантируется, что с высокой степенью вероятности будет найден хотя бы один участник. Основными параметрами таких кодов являются:

— число пользователей в системе,

— предполагаемый максимальный размер коалиции,

— параметр безопасности системы.

Поскольку коды Тардоша [7] имеют минимальную длину последовательностей благодаря своей вероятностной природе, то для исследований были выбраны именно они. Использование более коротких кодов позволит сократить долю используемых блоков, доступных для вставки, уменьшить количество вносимых искажений и повысить уровень обеспечиваемой безопасности.

Коды Тардоша предназначены для борьбы с коалиционными атаками и мало исследованы на стойкость к шумовым атакам (случайным искажениям не обнаруженных участниками коалиции битов). В настоящей статье была смоделирована атака шумом на коды Тардоша, благодаря чему удалось выяснить, что при даже небольшом проценте шума (2—3 %) вероятность обвинения невиновного пользователя высока. В работе [7] рассмотрена возможность проведения шумовых атак и предложен способ борьбы с ними путем удлинения кодов, Однако антикоалиционные коды имеют очень большую длину (до 2 МБ), поэтому такой путь решения нежелателен.

Для того чтобы данные коды можно было использовать без удлинения, нужно снизить влияние шума на вероятность ошибки при определении злоумышленника. Для решения этой задачи модель канала, используемая в алгоритме поиска, должна быть лучше согласована с реальным каналом, т.е. необходимо использовать дополнительную информацию, получаемую при извлечении битов метки из видеопоследовательности. В частности, использование при принятии решения об извлекаемом бите не только знака отклонения частотного коэффициента, но и амплитуды позволит определить уровень надежности полученных символов. Для лучшего соответствия модели каналу был введен новый символ — стирание. Он помещается в извлеченную последовательность, когда невозможно точно определить, какой символ передавался — 0 или 1. При поиске участников коалиции по извлеченному кодовому слову стертые позиции не учитываются, т.е. код укорачивается.

Было смоделировано воздействие различных уровней шума и стираний на извлеченную последовательность. Результаты показывают, что с ростом уровня шума вероятность ошибочного определения злоумышленника увеличивается, а с ростом уровня стираний — почти сохраняется. Эксперименты показали также, что данная замена не уменьшает вероятность определения злоумышленника. Таким образом, если, к примеру, из 30 % шума на последовательность 10 % шума удастся заменить стираниями, то вероятность ошибки уменьшается более чем на 25 %.

С помощью предложенного метода вставки и извлечения ЦВЗ в тестовый набор видео последовательностей были внедрены метки, после чего был проведен ряд атак. Результаты экспериментов показали, что наиболее успешны атаки постфильтрации и уменьшения размера кадра, которые приводят к 19—21 % ошибок извлечения. При использовании на этапе извлечения дополнительных символов стирания вероятность ошибки извлечения снижается с 19—21 до 0,6 %.

Заключение. Коды Тардоша позволяют успешно бороться с коалиционными атаками пользователей, однако требуется их значительное удлинение для обеспечения стойкости к шумовым атакам. Шумовые атаки неизбежны, так как предложенный метод вставки ЦВЗ позволяет не избежать ошибок, а только снизить их вероятность до 20 %. При этом использование символов стираний в кодах Тардоша дает снижение вероятности ошибки обнаружения злоумышленника при исходной длине кода.

СПИСОК ЛИТЕРАТУРЫ

1. *Su P.-C., Li M.-L., Chen I.-F.* A content-adaptive digital watermarking scheme in H.264/AVC Compressed videos // Proc. Intern. Conf. on Intelligent Information Hiding and Multimedia Signal Processing. 2008. P. 849—852.

2. *Su P.-C., Chen I.-F., Chen C.-C.* A practical design of digital video watermarking for content authentication // Signal Processing: Image Communication. 2011. P. 413—426.

3. *Saryazdi S., Demehri M.* A blind dct domain digital watermarking // Sciences of Electronic, Technologies of Information and Telecommunicatios. 2005. P. 55—57.

4. *Mansouri A., Aznaveh A. M., Torkamani-Azar F., Kurugollu F.* A low complexity video watermarking in H.264 compressed domain // IEEE Transact. on Information Forensics and Security. 2010. Vol. 5, N 4. P. 649—657.

5. *Беззатеев С. В., Литвинов М. Ю., Трояновский Б. К., Филатов Г. П.* Выбор алгоритма преобразования, обеспечивающего изменение структуры изображения // ИУС. 2006. № 6(25). С. 2—6.

6. *Boneh D., Shaw J.* Collusion-Secure Fingerprinting for Digital Data // IEEE Transact. on Information Theory. 1998. Vol. 44, N 5. P. 1897—1905.

7. *Tardos G.* Optimal probabilistic fingerprint codes // Proc. ACM Symp. on Theory of Computing. NY, USA, 2003. P. 116—125.

Сведения об авторах

Александра Валентиновна Афанасьева — магистр; Санкт-Петербургский государственный университет аэрокосмического приборостроения, кафедра безопасности информационных систем; программист; E-mail: alra@vu.spb.ru

Денис Олегович Иванов — Санкт-Петербургский государственный университет аэрокосмического приборостроения, кафедра безопасности информационных систем; программист; E-mail: denis.ivo@vu.spb.ru

Дмитрий Алексеевич Рыжов — аспирант; Санкт-Петербургский государственный университет аэрокосмического приборостроения, кафедра безопасности информационных систем; E-mail: dr@vu.spb.ru

Рекомендована кафедрой
№ 51 безопасности информационных систем

Поступила в редакцию
01.02.13 г.

СИСТЕМЫ ХРАНЕНИЯ ИНФОРМАЦИИ

УДК 004.021

В. С. Дужин, Г. С. Евсеев, Е. М. Линский

ОЦЕНКА ЭФФЕКТИВНОСТИ АЛГОРИТМА УПРАВЛЕНИЯ ОБЪЕМОМ РАЗДЕЛОВ КЭША СИСТЕМЫ ХРАНЕНИЯ ДАННЫХ

Рассматривается модель кэша системы хранения данных, состоящего из двух разделов. Построен алгоритм управления объемом разделов. Исследовано влияние ошибок определения текущего и последующего состояния потока на качество работы алгоритма.

Ключевые слова: *системы хранения данных, кэш, оценка эффективности.*

Введение. Использование кэша в системе хранения данных позволяет существенно уменьшить время доступа к информации. К такой системе обращаются приложения, отправляя запросы на получение данных. Каждому приложению в кэше выделен отдельный раздел. Будем считать, что каждое приложение характеризуется требованием на время обработки запроса, выражающимся в среднем значении HR (Hit Rate, отношение числа запросов, найденных в кэше, к общему числу запросов за определенный временной интервал для его раздела).

В настоящей статье рассматривается алгоритм, динамически перераспределяющий границы раздела.

В отличие от работ [1, 2], в которых рассматриваются эвристические алгоритмы управления кэшем, в настоящей статье предложена модель кэша, состоящего из двух разделов, позволяющая проводить анализ алгоритмов управления.

Модель системы. Рассмотрим LRU-кэш, с которым работают два приложения, каждому из них ставится в соответствие свой раздел в кэше, свой поток входных запросов и требуемое значение HR.

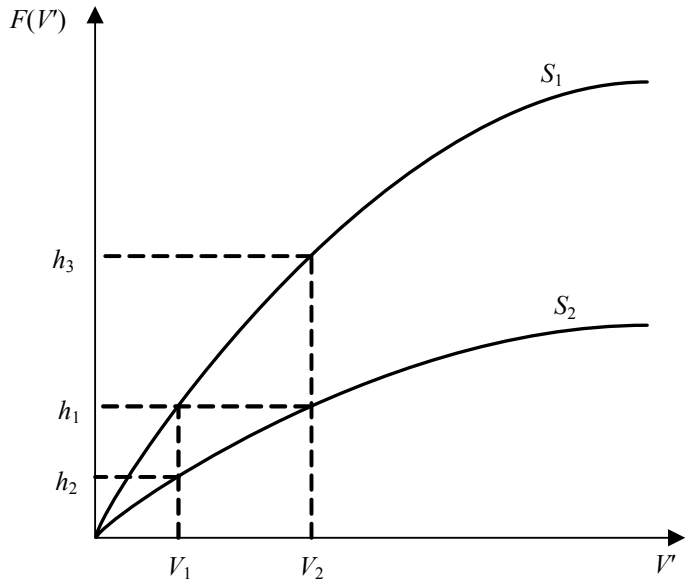
Входные потоки характеризуются интенсивностью запросов и распределением стекового расстояния, под которым будем понимать количество различных адресов между двумя обращениями к одному и тому же адресу [3—4].

Пусть входные потоки к каждому разделу могут находиться в двух состояниях: S_1 и S_2. Состояния различаются видом гистограммы стековых расстояний. Считается, что любой раздел, входной поток к которому находится в состоянии S_1, удовлетворяет требованию по HR, если его размер (объем) равен V_1. Раздел, входной поток к которому находится в состоянии S_2, удовлетворяет требованию, если его объем равен V_2. Будем считать, что $V_2 = 2V_1$, $V_{\text{cache}} = 3V_1$, где V_{cache} — суммарный объем кэша.

Рассмотрим дискретную временную модель: пусть $N_1 = N_2 = N$ — интенсивность запросов к разделам в определенный интервал времени, а ξ_1, ξ_2 — число запросов к адресам, находящимся в кэше (за то же время). Вероятности переходов между состояниями *i*-го потока описываются матрицей переходов марковской цепи:

$$\begin{bmatrix} P_i(S_1 \mid S_1) & P_i(S_2 \mid S_1) \\ P_i(S_1 \mid S_2) & P_i(S_2 \mid S_2) \end{bmatrix}. \quad (1)$$

На рисунке приведены функции распределения вероятностей стековых расстояний для потоков в состояниях S_1 и S_2.



Заметим, что при заданном размере раздела V' величина $F(V')$ может рассматриваться как средний HR на данном разделе, т.к. $F(V')$ – вероятность того, что стековое расстояние не превысит V' (запрашиваемый адрес будет найден в кэше).

Будем считать, что требование к размеру раздела состоит в том, чтобы средний HR был не меньше h_1. Как видно из рисунка, это условие не выполняется, когда входной поток находится в состоянии S_2, а объем раздела равен V_1.

Алгоритм управления кэшем. Рассмотрим алгоритм управления размерами разделов в кэше, обеспечивающий улучшение качества работы системы за счет ее динамической адаптации к изменениям входного потока. В течение каждого временного интервала собирается статистика по входным потокам, на основании которой оценивается состояние потоков в данном интервале. Прогноз состояния входных потоков в последующем временном интервале осуществляется на основе этих оценок и матриц (1). В конце каждого интервала происходит перераспределение объемов разделов в соответствии с этим прогнозом. Например, если состояние потока в предыдущем интервале оценено как $\hat{S}_1$, а $P(S_2 \mid S_1) > 0,5$, то прогнозируется, что в следующем интервале поток перейдет в состояние S_2.

Ниже представлен способ получения оценки состояния входного потока. Пусть текущий объем раздела равен V_1, за последний интервал пришло N запросов, при этом ξ из них были найдены в кэше. В этом случае вероятность того, что входной поток к данному разделу находился в состоянии S_1, определяется следующим образом:

$$P(S_1 \mid V_1, N, \xi) = \frac{P(S_1, \xi \mid V_1, N)}{P(\xi \mid V_1, N)}. \quad (2)$$

Выражение (2) получено из формулы для вероятностей зависимых событий [5] (в данном случае случайными величинами являются S_1 и ξ, а V_1 и N — постоянными). Аналогичным образом определяется вероятность нахождения входного потока к разделу в состоянии S_2. Обозначим через $R(V_1, N, \xi)$ отношение этих вероятностей и преобразуем его следующим образом:

$$R(V_1,N,\xi)=\frac{P(S_1,\xi\,|\,V_1,N)}{P(S_2,\xi\,|\,V_1,N)}=\frac{P(\xi\,|\,S_1,V_1,N)P(S_1\,|\,V_1,N)}{P(\xi\,|\,S_2,V_1,N)P(S_2\,|\,V_1,N)}. \quad (3)$$

Вероятности того, что из N пришедших заявок ξ будут найдены в кэше, описываются биномиальным распределением:

$$\begin{cases} P(\xi\,|\,S_1,V_1,N)=C_N^{\xi}h_1{}^{\xi}(1-h_1)^{N-\xi}, \\ P(\xi\,|\,S_2,V_1,N)=C_N^{\xi}h_2{}^{\xi}(1-h_2)^{N-\xi}. \end{cases} \quad (4)$$

Вероятность того, что заявка найдена в кэше, равна h_1 и h_2 для состояний входного потока S_1 и S_2 соответственно (см. рисунок). Заметим, что $P(S_1\,|\,V_1,N)$ и $P(S_2\,|\,V_1,N)$ не зависят от случайной величины ξ и определяются исключительно из матрицы переходов марковской цепи (1):

$$\begin{cases} P(S_1\,|\,V_1,N)=P(S_1), \\ P(S_2\,|\,V_1,N)=P(S_2). \end{cases} \quad (5)$$

Подставив (4) и (5) в выражение (3), после необходимых преобразований получим:

$$R(V_1,N,\xi)=\left(\frac{h_1(1-h_2)}{h_2(1-h_1)}\right)^{\xi}\left(\frac{1-h_1}{1-h_2}\right)^{N}\frac{P(S_1)}{P(S_2)}, \quad (6)$$

таким же образом получим отношение для потока к разделу размера V_2:

$$R(V_2,N,\xi)=\left(\frac{h_3(1-h_1)}{h_1(1-h_3)}\right)^{\xi}\left(\frac{1-h_3}{1-h_1}\right)^{N}\frac{P(S_1)}{P(S_2)}. \quad (7)$$

По формулам (6), (7) можно оценить состояние входного потока за временной интервал. Будем считать, что при $R>1$ входной поток в состоянии S_1, а при $R\le 1$ — в S_2:

$$\hat{S}(V,N,\xi)=\begin{cases} \hat{S}_1, \text{ если } V=V_1, R(V_1,N,\xi)>1, \\ \hat{S}_2, \text{ если } V=V_1, R(V_1,N,\xi)\le 1, \\ \hat{S}_1, \text{ если } V=V_2, R(V_2,N,\xi)>1, \\ \hat{S}_2, \text{ если } V=V_2, R(V_2,N,\xi)\le 1. \end{cases} \quad (8)$$

Заметим, что достаточно определить оценку (8) лишь для одного потока: при оценке состояния первого потока $\hat{S}_1$ ему назначается объем V_1, а второму — V_2 (это связано с тем, что $V_{\text{cache}}=3V_1$, а распределять не весь объем кэша нецелесообразно). Если оценка состояния первого потока $\hat{S}_2$, ему назначается объем V_2, а второму — V_1.

Кэш выделяется, в первую очередь, тому потоку, оценка состояния которого более достоверна. Достоверность определяется тем, насколько значение R отличается от единицы: при $R=1$ оценки становятся равновероятными, а значит их достоверность минимальна.

Таким образом, вначале вычисляются значения R для каждого раздела, затем устанавливается размер того раздела, для которого R больше (если $R<1$, то в сравнении будет участвовать величина $\frac{1}{R}$). Другому разделу назначается оставшийся объем кэша.

Оценка работы алгоритма. Рассмотрим методику оценки качества работы алгоритма управления кэшем, которое определим как вероятность того, что на каком-либо временном интервале требования на HR будут удовлетворены для обоих разделов. На качество работы алгоритма влияют ошибка оценки текущих состояний потоков, вызванная низкой интенсивностью входных потоков, а также ошибка определения последующего состояния, связанная со

случайным характером переключения состояний входных потоков. Сначала рассмотрим идеальный случай, когда обе ошибки отсутствуют (построим верхнюю границу качества), затем — когда присутствует лишь ошибка определения последующего состояния и, наконец, когда присутствуют обе ошибки.

Вычислим верхнюю границу качества описанного алгоритма. Будем считать, что состояния потоков на каждом временном интервале известны заранее. Соответственно выбираются оптимальные размеры разделов во всех случаях, когда это возможно. Требования по HR не выполняются лишь тогда, когда оба входных потока находятся в состоянии S_2, поскольку в этом случае потребуется объем $2V_2 > V_{\text{cache}}$. Верхняя граница качества алгоритма определяется следующим выражением:

$$Q_1 = 1 - P_1(S_2)P_2(S_2), \tag{9}$$

где $P_1(S_2)$ и $P_2(S_2)$ — вероятность нахождения в состоянии S_2 потоков запросов к 1-му и 2-му разделам, которая определяется из формулы полной вероятности [5]:

$$P_i(S_2) = P_i(S_1)P_i(S_2 \mid S_1) + P_i(S_2)P_i(S_2 \mid S_2), \tag{10}$$

где $i = 1, 2$. Поскольку поток может быть в состоянии S_1 либо в состоянии S_2,

$$P_i(S_1) = 1 - P_i(S_2). \tag{11}$$

Подставим (11) в (10) и после необходимых преобразований получим:

$$P_i(S_2) = \frac{P_i(S_2 \mid S_1)}{P_i(S_1 \mid S_2) + P_i(S_2 \mid S_1)}. \tag{12}$$

Рассуждая аналогичным образом, можно вычислить вероятность нахождения потока в состоянии S_1:

$$P_i(S_1) = \frac{P_i(S_1 \mid S_2)}{P_i(S_1 \mid S_2) + P_i(S_2 \mid S_1)}. \tag{13}$$

Перепишем (9) с учетом (12):

$$Q_1 = 1 - \frac{P_1(S_2 \mid S_1)P_2(S_2 \mid S_1)}{\big(P_1(S_1 \mid S_2) + P_1(S_2 \mid S_1)\big)\big(P_2(S_1 \mid S_2) + P_2(S_2 \mid S_1)\big)}. \tag{14}$$

Вычислим оценку качества алгоритма при условии, что известны состояния входных потоков за прошедший временной интервал (интенсивность потоков $N \to \infty$), при этом прогноз следующего состояния осуществляется на основе матрицы переходов (1).

В таблице перечислены состояния системы, состоящей из двух разделов. Каждое состояние характеризуется объемом разделов и состояниями их входных потоков. Заметим: когда система находится в состояниях 1, 2, 5, 7, разделам хватает выделенных объемов для выполнения требований. В состояниях 4, 8 требования не могут быть удовлетворены в принципе, поскольку входные потоки к обоим разделам находятся в состоянии S_2. В состояниях 3, 6 требования могут быть выполнены, если объем разделов выбран правильно. Таким образом, оценка качества работы данного алгоритма вычисляется с помощью следующего выражения:

$$Q_2 = Q_1 - (P(3) + P(6)), \tag{15}$$

где $P(3)$, $P(6)$ — вероятности перехода системы в соответствующие состояния. Выражение (15) справедливо, поскольку $P(3)$ и $P(6)$ — вероятности несовместных событий.

Введем обозначение $V^{(i)} = \{V^{(1)}, V^{(2)}\}$. Пусть при $V^{(1)}$ первый раздел получает объем V_1, второй V_2, а при $V^{(2)}$ — наоборот.

Пусть $P_{\text{ош}}(S^{(1)}, S^{(2)}, V^{(1)})$ — вероятность того, что распределение разделов $V^{(1)}$ даст ошибку, если на предыдущем интервале состояние первого раздела было $S^{(1)}$, а второго — $S^{(2)}$. Аналогичным образом определяется $P_{\text{ош}}(S^{(1)}, S^{(2)}, V^{(2)})$. Тогда минимальная вероятность ошибки для ситуации $S^{(1)} = S_1$, $S^{(2)} = S_1$ определяется следующим образом:

$$P_{\text{ош}}(S_1, S_1) = \min\left\{P_{\text{ош}}(S_1, S_1, V^{(1)}), P_{\text{ош}}(S_1, S_1, V^{(2)})\right\}.$$

№ состояния	Объем 1-го раздела	Объем 2-го раздела	Состояние 1-го потока	Состояние 2-го потока	Требования по HR
1	V_1	V_2	S_1	S_1	Выполнены
2	V_1	V_2	S_1	S_2	Выполнены
3	V_1	V_2	S_2	S_1	Не выполнены из-за ошибки
4	V_1	V_2	S_2	S_2	Невыполнимы
5	V_2	V_1	S_1	S_1	Выполнены
6	V_2	V_1	S_1	S_2	Не выполнены из-за ошибки
7	V_2	V_1	S_2	S_1	Выполнены
8	V_2	V_1	S_2	S_2	Невыполнимы

Вероятность ошибки определяется как сумма таких вероятностей для всех комбинаций $S^{(1)}$, $S^{(2)}$:

$$P_{\text{ош}} = P(3) + P(6) = \sum_{i=1}^{2}\sum_{j=1}^{2} \min\left\{P_{\text{ош}}(S_i, S_j, V^{(1)}), P_{\text{ош}}(S_i, S_j, V^{(2)})\right\}. \tag{16}$$

Перепишем (15) с учетом (16):

$$Q_2 = Q_1 - \sum_{i=1}^{2}\sum_{j=1}^{2} \min\left\{P_{\text{ош}}(S_i, S_j, V^{(1)}), P_{\text{ош}}(S_i, S_j, V^{(2)})\right\}.$$

Очевидно, что данный алгоритм работает лучше, когда состояния входных потоков изменяются редко: при стремлении элементов главной диагонали матрицы (1) к единице Q_2 стремится к Q_1 ($P(S_1 \mid S_2)$ и $P(S_2 \mid S_1)$ стремятся к нулю, вероятности $P(3)$ и $P(6)$ стремятся к нулю и выражение (15) вырождается в (14)).

Теперь рассмотрим ситуацию, когда оценка состояний входных потоков производится при конечной выборке. В этом случае к ошибке оценки следующего состояния добавляется ошибка оценки текущего состояния.

Определим зависимость качества алгоритма от интенсивности N. Для этого выпишем матрицу переходов системы из двух разделов:

$$\begin{cases} P(1) = \sum\limits_{i=1}^{8} P(i)P(1 \mid i), \\ P(2) = \sum\limits_{i=1}^{8} P(i)P(2 \mid i), \\ \quad\vdots \\ P(8) = \sum\limits_{i=1}^{8} P(i)P(8 \mid i). \end{cases} \tag{17}$$

Пусть $V(i)$ — распределение объемов разделов в *i*-м состоянии системы, например, $V(6) = V^{(2)}$.

Поскольку изменение объема раздела и изменение состояний входных потоков являются независимыми событиями, вероятность перехода из *j*-го в *i*-е состояние системы может быть представлена в виде произведения вероятности изменения объема раздела с V_{t-1} на V_t и вероятностей переходов состояний потоков 1-го и 2-го раздела соответственно: $P_1(S_t \mid S_{t-1})$ и $P_2(S_t \mid S_{t-1})$:

$$P(i \mid j) = P(V_t, S_t^{(1)}, S_t^{(2)} \mid V_{t-1}, S_{t-1}^{(1)}, S_{t-1}^{(2)}) = P(V_t \mid V_{t-1}, S_{t-1}^{(1)}, S_{t-1}^{(2)}) P_1(S_t \mid S_{t-1}) P_2(S_t \mid S_{t-1}).$$

Вычислим $P(V_t \mid V_{t-1}, S_{t-1}^{(1)}, S_{t-1}^{(2)})$ для случая $V_t = V^{(2)}, V_{t-1} = V^{(1)}$. Пусть оценка состояния первого потока оказалась более достоверной. Для того чтобы объем 1-го раздела стал равен V_2, необходимо, чтобы в предыдущем интервале была получена оценка состояния потока $\hat{S}^{(2)} = S_2$. При этом объем данного раздела в предыдущем интервале должен быть равен V_1. Из (8) следует, что для этого должно быть выполнено условие $R(V_1, N, \xi) \le 1$. Соответственно $P(V_t \mid V_{t-1}, S_{t-1}^{(1)}, S_{t-1}^{(2)}) = P(R(V_1, N, \xi) \le 1)$.

После необходимых преобразований с учетом (6), (12), (13) получим:

$$P(V_t \mid V_{t-1}, S_{t-1}^{(1)}, S_{t-1}^{(2)}) = P\left(\xi < \ln\left(\left(\frac{1-h_2}{1-h_1}\right)^N \frac{P_1(S_2 \mid S_1)}{P_1(S_1 \mid S_2)}\right) \ln\left(\frac{h_1(1-h_2)}{h_2(1-h_1)}\right)\right). \quad (18)$$

Обозначим правую часть неравенства (18) через Ξ и перепишем его с учетом того, что ξ имеет биномиальное распределение:

$$P(V_t \mid V_{t-1}, S_{t-1}^{(1)}, S_{t-1}^{(2)}) = \sum_{m=0}^{m<\Xi} C_N^m h_2^m (1-h_2)^{N-m}. \quad (19)$$

Вычислив аналогичным образом все условные вероятности системы (17), получим систему из 8 уравнений с 8 неизвестными. Решив эту систему, получим значения *P*(4), *P*(8), *P*(3) и P(6). Качество работы данного алгоритма оценивается как

$$Q_3(N) = 1 - (P(4) + P(8) + P(3) + P(6)).$$

Заключение. В работе построена модель кэша системы хранения данных, состоящего из двух разделов, размеры которых адаптивно изменяются. Исследовано влияние ошибки определения текущего состояния потока и ошибки выбора следующего состояния потока на качество работы алгоритма. В дальнейшем предполагается обобщить данные результаты для ситуации, когда кэш содержит более двух разделов.

СПИСОК ЛИТЕРАТУРЫ

1. *Qureshi M. K., Patt Y. N.* Utility-Based Cache Partitioning: A Low-Overhead, High-Performance, Runtime Mechanism to Partition Shared Caches // Proc. of the 39th Annual IEEE/ACM Intern. Symp. on Microarchitecture (MICRO 39). IEEE Comp. Soci. Washington, DC, USA, 2006. P. 423—432.

2. *Goyal P., Jadav D., Modha D. S., Tewari R.* CacheCOW: QoS for storage system caches // Proc. of the 11th Intern. Conf. on Quality of Service (IWQoS'03). Berlin: Springer-Verlag, 2003. P. 498—515.

3. *Feitelson D. G.*, Workload Modeling for Computer Systems Performance Evaluation [Электронный ресурс]: <http://www.cs.huji.ac.il/~feit/wlmod/>.

4. *Марковский С. Г., Тюрликов А. М.* Использование адресов абонентов для разрешения конфликтов в канале с шумом // ИУС. 2006. № 2(21). С. 27—37.

5. *Венцель Е. С.* Теория вероятностей. М.: Наука, 1964. 575 с.

Сведения об авторах

Василий Сергеевич Дужин — аспирант; Санкт-Петербургский государственный университет аэрокосмического приборостроения, кафедра безопасности информационных систем; E-mail: vduzhin@gmail.com

Григорий Сергеевич Евсеев — канд. техн. наук, доцент; Санкт-Петербургский государственный университет аэрокосмического приборостроения, кафедра моделирования вычислительных и электронных систем; E-mail: egs@vu.spb.ru

Евгений Михайлович Линский — канд. техн. наук, доцент; Санкт-Петербургский государственный университет аэрокосмического приборостроения, кафедра безопасности информационных систем; E-mail: evlinsky@vu.spb.ru

Рекомендована кафедрой
№ 51 безопасности информационных систем

Поступила в редакцию
01.02.13 г.

УДК 681.3

В. А. Богатырев, С. В. Богатырев, А. В. Богатырев

ОЦЕНКА НАДЕЖНОСТИ ОТКАЗОУСТОЙЧИВЫХ КЛАСТЕРОВ С НЕПОСРЕДСТВЕННЫМ ПОДКЛЮЧЕНИЕМ УСТРОЙСТВ ХРАНЕНИЯ

Предложен подход к оценке надежности кластеров с прямым подключением двухвходовых устройств хранения и серверов при ограничении предельно допустимого времени пребывания запросов в системе. Проанализировано влияние вариантов такого подключения на надежность системы с учетом вероятности выполнения запросов в заданные сроки.

Ключевые слова: *отказоустойчивость, кластер, надежность, резервирование, устройство хранения, сервер.*

Введение. Высокие отказоустойчивость, доступность, надежность и производительность распределенных вычислительных систем достигаются при объединении узлов обработки и хранения данных в кластеры [1, 2].

При построении небольших кластерных систем в ряде случаев целесообразно прямое подключение узлов разных уровней между собой, например, серверных узлов и устройств хранения (архитектура DAS, Directly Attached Storage [1]).

Поскольку надежность и производительность кластера зависят от вариантов объединения его узлов, представляет интерес исследование альтернатив, обеспечивающих большую отказоустойчивость, надежность и доступность системы при одинаковых затратах на ее реализацию [3—5].

Двухуровневые структуры с непосредственным подключением резервированных узлов. Рассмотрим варианты конфигурации двухуровневых кластерных систем. Будем считать, что на верхнем уровне (ВУ) выделяется m дублированных узлов. Таким образом, общее число узлов верхнего уровня равно $2m$, общее число узлов нижнего уровня (НУ) будем также считать равным $2m$. Узлы верхнего уровня объединяются в пары (дублируются) по функциональной принадлежности реализуемых приложений или по разделению обслуживаемого ими потока запросов [6—9].

Представляет определенный интерес исследование вариантов построения кластеров с прямым подключением узлов разного уровня, в частности серверов, к устройствам хранения [1, 2]. Цель таких исследований — выбор конфигурации, обеспечивающей при одинаковых затратах на реализацию системы ее большую отказоустойчивость, надежность и доступность.

В рамках указанного направления в работах [10, 11] исследованы варианты прямого подключения дублированных серверов к устройствам хранения без учета ограничений на время обслуживания запросов. Поскольку для систем, функционирующих в реальном времени, такие ограничения важны, в настоящей статье исследуется влияние конфигураций прямого подключения узлов двухуровневого кластера на выполнение функциональных запросов при ограничении времени их пребывания в системе.

Варианты построения кластера. Рассмотрим конфигурации кластерных систем с непосредственным подключением устройств хранения к серверам приложений m типов [10, 11]. На рис. 1 приведены варианты кластеров: *а* — S1, *б* — S2 , *в* — S3. Будем считать, что запрос j-го потока (к i-му приложению) может быть обслужен хотя бы одним из выделенных для этого потока серверов (сервером i-го приложения) при взаимодействии с любым из подключенных к нему устройств хранения (узлов НУ). Кратность резервирования серверов будем считать 2/1, в этом случае общее число узлов ВУ $2m$, общее число узлов НУ также будем считать равным $2m$.

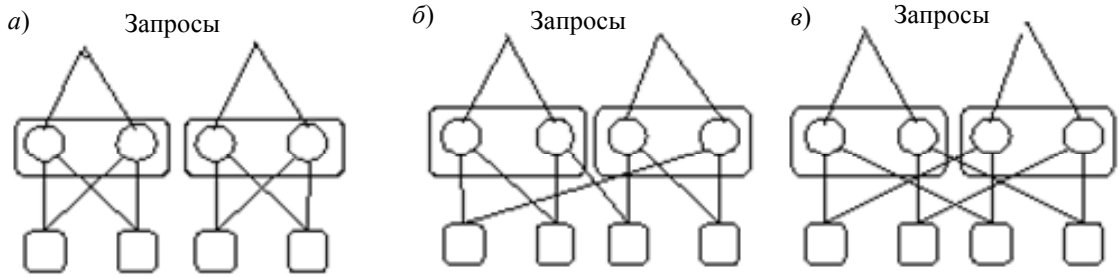


Рис. 1

Будем считать, что все серверы и устройства хранения (узлы ВУ и НУ) имеют по два порта (входа), что позволяет строить резервированные системы с отсутствием единой точки отказа без использования коммутаторов, которые в ряде случаев могут вносить дополнительную ненадежность в систему.

Проанализируем надежность представленных на рис. 1 вариантов структур [11] с учетом ограничений по предельно допустимому времени обслуживания запросов. Подчеркнем что эти варианты характеризуются одинаковыми затратами на их построение, но позволяют достичь различных уровней надежности и отказоустойчивости, что и обусловливает актуальность их исследования.

При исправности двух резервированных серверов некоторого приложения конфигурации S1, S2 и S3 сохраняют функциональность, если действует хотя бы одно из двух, трех либо четырех связанных с рассматриваемыми серверами устройств хранения соответственно. При дееспособности одного сервера приложения для всех вариантов конфигураций (см. рис. 1) функциональность сохраняется, если исправно хотя бы одно из двух связанных с сервером устройств хранения. Таким образом, отказоустойчивость конфигурации S3 выше, оценим надежность ее и базовой конфигурации S1 [10].

Вычислим вероятность безотказной работы (ВБР) конфигурации S1 (рис. 1, *а*) при условии исправности хотя бы одного сервера и одного устройства хранения в каждой из m дублированных групп [11]:

$$P_1(t) = \left\{\left[1-\left(1-p_1(t)\right)^2\right]\left[1-\left(1-p_2(t)\right)^2\right]\right\}^m,$$

где $p_1(t) = \exp(-\lambda_1 t), p_1(t) = \exp(-\lambda_1 t), \lambda_1,\ \lambda_2$ — интенсивность отказов сервера и устройства хранения.

В этой формуле не введены ограничения на время выполнения запросов, характерные для систем реального времени. С учетом этих ограничений считается, что система может выполнить некоторое приложение (поток запросов), если запрос может быть обслужен хотя бы одним узлом ВУ и хотя бы одним узлом НУ, а время пребывания запросов не превышает t_0.

Будем считать, что среднее время обслуживания запросов в серверах включает их взаимодействие с устройствами хранения, тогда

$$P_1(t) = \left[1-\left(1-p_2(t)\right)^2\right]\left[\left(p_1(t)\right)^2 g_2 + 2p_1(t)(1-p_1(t))g_1\right].$$

Вычислим вероятность того, что время пребывания запросов в i параллельно работающих серверах меньше t_0 [12]:

$$g_i = \begin{cases} 0, \ if \ \ (\Lambda v/i) \ge 1, \\ 1-\left(\dfrac{\Lambda v}{i}\right)\exp\left(-\left(\dfrac{1}{v}-\dfrac{\Lambda}{i}\right)t_o, -if \ \ (\Lambda v/i) < 1, \end{cases}$$

Оценим ВБР системы для конфигураций S2 и S3 при условии непревышения t_0 (ограничения по времени пребывания запросов не учитываются, т.е. g_1=1, g_2=1):

$$P_2(t) = \left[1-\left(1-p_2(t)\right)^3\right]\left(p_1(t)\right)^2 g_2 + 2p_1(t)(1-p_1(t))\left[1-\left(1-p_2(t)\right)^2\right]g_1,$$

$$P_3(t) = \left[1-\left(1-p_2(t)\right)^4\right]\left(p_1(t)\right)^2 g_2 + 2p_1(t)(1-p_1(t))\left[1-\left(1-p_2(t)\right)^2\right]g_1.$$

Кривые *1—3* на рис. 2 иллюстрируют результаты расчета вероятности безотказной работы структур S1—S3 при $\lambda_1=10^{-4}$, $\lambda_2=2\cdot10^{-4}$ ч$^{-1}$. Из графиков видна зависимость ВБР исследуемых структур от варианта соединения двухвходовых серверов и устройств хранения, причем затраты на реализацию сравниваемых структур одинаковы.

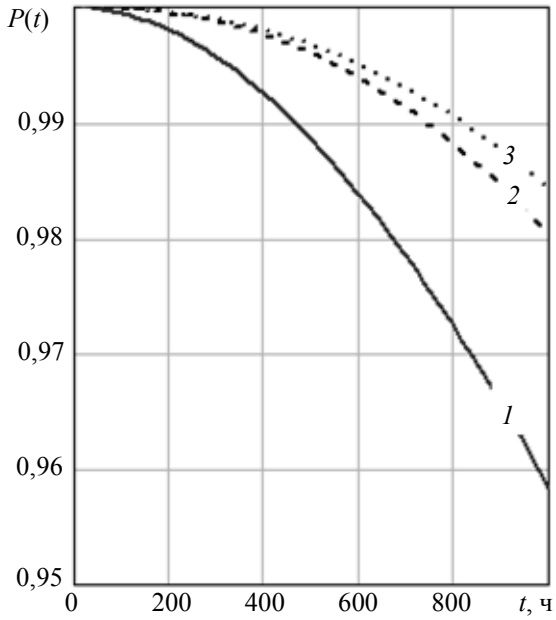


Рис. 2

На рис. 3 представлены результаты расчета вероятности выполнения запросов за время, меньшее t_0 ($\lambda_1=10^{-4}$, $\lambda_1=2\cdot10^{-4}$ ч$^{-1}$, среднее время обслуживания запроса сервером, с учетом обращений к системе хранения — 1 с). Кривые *1, 2* соответствуют ВБР конфигураций S3 и S1;

кривые *3, 4, 5* для конфигурации S3 (*6, 7, 8* — для S1) соответствуют вероятности выполнения запросов при t_0=10, 5, 2 с соответственно. Интенсивность потока рассматриваемых функциональных запросов 1 $с^{-1}$(рис. 3, *а*) и 1,5 $с^{-1}$ (рис. 3, *б*).

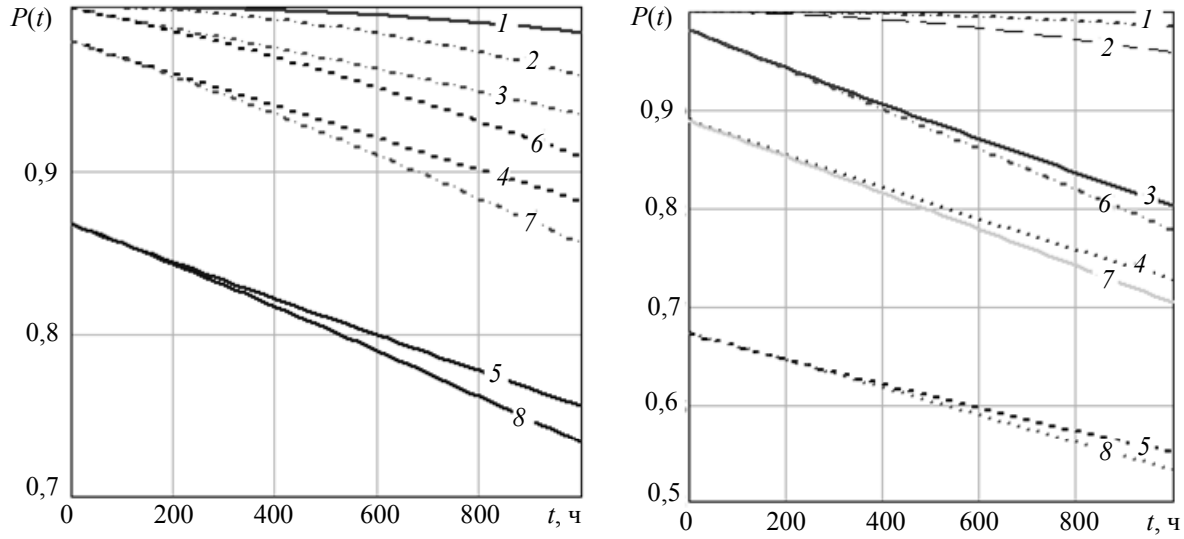


Рис. 3

Проведенные расчеты подтвердили существенную зависимость надежности кластеров от порядка прямого подключения устройств хранения к серверам приложений при явном преимуществе конфигурации S3 по отказоустойчивости, ВБР и надежности в случае выполнения запросов в установленные сроки.

Заключение. Предложен подход к оценке надежности кластерных вычислительных систем с прямым подключением двухвходовых устройств хранения и серверов, позволяющий учитывать вероятность выполнения запросов при непревышении предельно допустимого времени их пребывания в системе. Продемонстрировано влияние вариантов подключения серверов и устройств хранения на надежность системы при одинаковых издержках на ее реализацию. Даны рекомендации по выбору вариантов конфигурации резервированных кластеров.

СПИСОК ЛИТЕРАТУРЫ

1. *Juud J.* Principles of SAN Design. San Jose: Brocade Bookshelf, 2008. 589 p.

2. *Clark T.* The New Data Center. New technologies are radically reshaping the data center. Brocade Bookshelf. San Jose, 2010. 156 p.

3. *Богатырев В. А.* Надежность функционально-распределенных резервированных структур с иерархической конфигурацией узлов // Изв. вузов. Приборостроение. 2000. Т. 43, № 4. С. 67—70.

4. *Богатырев В. А.* О влиянии размещения функциональных ресурсов на отказоустойчивость информационно-вычислительных систем с функциональной реконфигурацией // Информационные технологии. 2002. Т. 45, № 2. С. 10—15.

5. *Богатырев В. А.* Безотказность систем из функционально неоднородных модулей // Приборы и системы. Управление, контроль, диагностика. 2002. № 3. С. 6—8.

6. *Богатырев В. А.* К размещению резервированных функциональных ресурсов в системах с функциональной реконфигурацией // Управляющие системы и машины. 2003 № 3. С. 42—45.

7. *Богатырев В. А.* Надежность вариантов размещения функциональных ресурсов в однородных вычислительных сетях // Электронное моделирование. 1997. № 3. С. 21—25.

8. *Богатырев В. А.* К оценке надежности систем из многофункциональных модулей // Автоматизация и современные технологии. 2001. № 6. С. 12—15.

9. *Богатырев В. А., Богатырев С. В.* Объединение резервированных серверов в кластеры высоконадежной компьютерной системы // Информационные технологии. 2009. № 6. С. 41—47.

10. *Bogatyrev V. A.* Fault Tolerance of Clusters Configurations with Direct Connection of Storage Devices // Automatic Control and Computer Sciences. 2011. Vol. 45, N 6. P. 330—337.

11. *Богатырев В. А., Богатырев А. В., Богатырев С. В.* Надежность кластерных вычислительных систем с дублированными связями серверов и устройств хранения // Информационные технологии. 2013. № 2. С. 27—32.

12. *Клейнрок Л.* Теория массового обслуживания. М.: Машиностроение, 1979. 432 с.

Сведения об авторах

Владимир Анатольевич Богатырев — д-р техн. наук; Санкт-Петербургский государственный университет аэрокосмического приборостроения, кафедра безопасности информационных систем; профессор;
E-mail: Vladimir.bogatyrev@gmail.com

Станислав Владимирович Богатырев — Санкт-Петербургский государственный университет аэрокосмического приборостроения, кафедра безопасности информационных систем; младший научный сотрудник;
E-mail: realloc@gmail.com

Анатолий Владимирович Богатырев — аспирант; Санкт-Петербургский национальный исследовательский университет информационных технологий, механики и оптики, кафедра вычислительной техники;
E-mail: ganglion@gmail.com

Рекомендована кафедрой
№ 51 безопасности информационных систем

Поступила в редакцию
01.02.13 г.

SUMMARY

P. 9—14.

AN APPROACH TO DEVELOPMENT OF BLOCK-COMMUTATIVE CODES WITH LOW DENSITY OF PARITY CHECK

Methods of low-density parity-check codes construction are proposed. The codes constructions are presented, results of application of the codes in AWGN channel are demonstrated.

Keywords: LDPC-code, Gilbert code, block-permutation construction.

Data on authors

Alexander V. Kozlov — St. Petersburg State University of Aerospace Instrumentation, Department of Information Systems Security; Leading Programmer; E-mail: akozlov@vu.spb.ru

Evgeny A. Krouk — Dr. Techn. Sci., Professor; St. Petersburg State University of Aerospace Instrumentation, Department of Information Systems Security; E-mail: ekrouk@vu.spb.ru

Andrey A. Ovchinnikov — Cand. Techn. Sci.; St. Petersburg State University of Aerospace Instrumentation, Department of Information Systems Security; E-mail: mldoc@vu.spb.ru

P. 14—17.

THE LOWER BOUND OF SYSTEMATIC UNIFORMLY ROBUST CODE LENGTH

Basic definitions of error-detecting robust codes are formulated; the area of the codes application is described. The lower bound of the length of systematic R-uniformly distributed codes is deduced. Comparison with the present-day results is carried out.

Keywords: nonlinear code, robust code, lower bound, minimal code length.

Data on author

Maksim O. Alekseev — Post-Graduate Student; St. Petersburg State University of Aerospace Instrumentation, Department of Aerospace Computer Technologies; E-mail: alexeevmo@gmail.com

P. 17—20.

MODIFICATION OF GOERTZEL-BLAHUT ALGORITHM

The classic Goertzel-Blahut algorithm for computation of discrete Fourier transform over a finite field is considered along with several modifications of the classic algorithm. It is shown that the modified Goertzel—Blahut algorithm is closely related to the fast Fourier transform algorithms rather than to the semi-fast algorithms.

Keywords: discrete Fourier transform, fast Fourier transform, algorithm complexity, fast algorithm, semi-fast algorithm, finite field.

Data on author

Sergey V. Fedorenko — Dr. Techn. Sci., Professor; St. Petersburg State University of Aerospace Instrumentation, Department of Information Systems Security; E-mail: sfedorenko@ieee.org

P. 20—24.

A NEW ALGORITHM FOR LIST DECODING OF TURBO CODES

The problem of list decoding of turbo codes is considered. A new algorithm of window-based list decoder of convolutional code with soft output is developed in the frames of the parallel turbo decoding method. The proposed algorithm is shown to outperform the algorithm presented earlier; the gain in performance is obtained not only with short words, but also with words of considerable length.

Keywords: turbo codes, turbo decoding, list decoding.

Data on authors

Akmal I. Akmalkhodzhaev — St. Petersburg State University of Aerospace Instrumentation, Department of Information Systems Security; Programmer; E-mail: Akmal.ilh@gmail.com

Alexander V. Kozlov — St. Petersburg State University of Aerospace Instrumentation, Department of Information Systems Security; Leading Programmer; E-mail: akozlov@vu.spb.ru

P. 24—27.

A NEW CONSTRUCTION OF SYSTEMATIC ROBUST CODE

A concept of a robust code is presented. Basic characteristics of such a code are formulated, and a new construction method is proposed. A nonlinear function is introduced to compute check symbols. Analysis of the code robustness in the case of unidirectional errors is performed.

Keywords: nonlinear function, robust code, unidirectional errors, exponential function.

Data on author

Maksim O. Alekseev — Post-Graduate Student; St. Petersburg State University of Aerospace Instrumentation, Department of Aerospace Computer Technologies; E-mail: alexeevmo@gmail.com

P. 28—34.

A METHOD OF ASSESSMENT OF WIRELESS NETWORK TOPOLOGY WITH THE USE OF A PRIORY INFORMATION ON DEVICE POSITION

Approaches to estimation of path loss for sensor network are considered. The stochastic model of the relative positions of the network devices and state-of-art method of channel quality estimation in the frames of the model are analyzed. A new method of the estimation based on maximum a posteriori probability (MAP) is presented. The proposed method is compared with classical RSSI estimation method.

Keywords: sensor network, path loss, maximum a posteriori probability estimation, RSSI.

Data on authors

Evgeny A. Bakin — St. Petersburg State University of Aerospace Instrumentation, Department of Processing and Electronic Systems; Assistant; E-mail: jenyb@vu.spb.ru

Konstantin N. Smirnov — Post-Graduate Student; St. Petersburg State University of Aerospace Instrumentation, Department of Processing and Electronic Systems; E-mail: kossmir@gmail.com

P. 35—41.

ANALYSIS OF INTERFERENCE CANCELLATION PROCEDURE IN OFDM SYSTEMS WITH RANDOM MULTIPLE ACCESS

Interference cancellation procedure in a centralized wireless network is considered. The PHY layer of the network uses OFDM modulation, while the MAC layer employs random multiple access. The error probability of interference cancellation is estimated. The dependence of maximal stable throughput of multiple access algorithms on the SNR is derived.

Keywords: OFDM, interference cancellation, random multiple access.

Data on authors

Maxim A. Grankin — Post-Graduate Student; St. Petersburg State University of Aerospace Instrumentation, Department of Infocommunication Systems; E-mail: m.grankin@vu.spb.ru

Evgeny V. Pustovalov — St. Petersburg State University of Aerospace Instrumentation, Institute of Computer Security in Computational Networks and System; Scientist; E-mail: eugeny@vu.spb.ru

Andrey M. Turlikov — Dr. Techn. Sci.; St. Petersburg State University of Aerospace Instrumentation, Department of Infocommunication Systems; E-mail: turlikov@vu.spb.ru

P. 42—45.

SYNTHESIS OF OPTIMAL RULE OF SIGNAL RECEPTION AGAINST CROSS TALK IN WCAN SYSTEM

Wireless chip area network (WCAN) system using ultra wide band (UWB) range and pulse position modulation (PPM) is considered. A new algorithm for signal reception is developed on the base of calculation of likelihood function maximum. Results of analytical calculation of the bit error rate, as well as modeling results are presented.

Keywords: wireless chip area network, ultra wide band, pulse position modulation, bit error rate, maximum of likelihood function.

Data on authors

Konstantin B. Gurnov — St. Petersburg State University of Aerospace Instrumentation, Department of Processing and Electronic Systems; Assistant; E-mail: kocta4212@mail.ru

Grigory S. Evseev — Cand. Techn. Sci.; St. Petersburg State University of Aerospace Instrumentation, Department of Processing and Electronic Systems; E-mail: egs@vu.spb.ru

P. 45—51.

ON CALCULATION OF MESSAGE DELAY WITH CODING ON TRANSPORT LAYER OF DATA-TRANSMISSION NETWORK

The model used for calculation of the gain obtained by using coding at the transport layer of data-communication network is considered. Analytical estimates for the gain are compared with simulation results.

Keywords: transport layer coding, error correction codes, message delay.

Data on authors

Evgeny A. Krouk — Dr. Techn. Sci., Professor; St. Petersburg State University of Aerospace Instrumentation, Department of Information Systems Security; E-mail: ekrouk@vu.spb.ru

Dmitry A. Malichenko — St. Petersburg State University of Aerospace Instrumentation, Department of Information Systems Security; Assistant; E-mail: dml@vu.spb.ru

P. 52—57.

ANALYSIS OF ENERGY-SAVING MODES IN MOBILE USER DEVICE

Power saving techniques based on periodical disconnection of subscriber's device is considered. Energy consumption by the device and mean initial delay are estimated with the use of a standard mathematical model.

Keywords: power saving, mobile user device, sleep-mode, burst traffic model.

Data on authors

Evgeny V. Pustovalov — St. Petersburg State University of Aerospace Instrumentation, Institute of Computer Security in Computational Networks and System; Scientist; E-mail: eugeny@vu.spb.ru

Andrey M. Turlikov — Dr. Techn. Sci.; St. Petersburg State University of Aerospace Instrumentation, Department of Infocommunication Systems; E-mail: turlikov@vu.spb.ru

P. 58—61.

PROTECTION OF ULTRA-LIGHT AUTHENTICATION PROTOCOLS AGAINST ATTACKS ON LSB

An advanced version of mutual authentication protocol LMAP++ is presented. The proposed improvement is based on substitution of standard addition operation modulo 2^m by addition operation modulo 2^m–1, and application of only simplest arithmetic operations. The proposed modification complexity is compared with complexity of known methods for increasing the reliability of the protocol LMAP + +.

Keywords: RFID, ultra-light protocol, LMAP++, authentication.

Data on authors

Danil A. Kovalev — Post-Graduate Student; St. Petersburg State University of Aerospace Instrumentation, Department of Technologies of Information Security; E-mail: iostreamawm@gmail.com

Sergey V. Bezzateev — Dr. Techn. Sci.; St. Petersburg State University of Aerospace Instrumentation, Department of Technologies of Information Security; Head of the Department; E-mail: bsv@aanet.ru

P. 62—67.

METHOD OF SIDE INFORMATION GENERATION FOR DISTRIBUTED VIDEO CODING SYSTEMS

Main problems of distributed video coding are considered. Using reference codec DISCOVER as an example, advantages and disadvantages of basic coding methods are analyzed. A new method for generation of side information based on hierarchical motion estimation is proposed. Efficiency of a codec based on the proposed method as compared with DISCOVER is illustrated with rate-distortion diagrams

Keywords: video compression, distributed video coding (DVC), Wyner-Ziv video coding, WZ-frames, temporal video interpolation, motion estimation.

Data on authors

Anton I. Veselov — Post-Graduate Student; St. Petersburg State University of Aerospace Instrumentation, Department of Infocommunication Systems; E-mail: anton.veselov@gmail.com

Marat R. Gilmutdinov — Cand. Techn. Sci.; St. Petersburg State University of Aerospace Instrumentation, Department of Infocommunication Systems; E-mail: mgilmutdinov@gmail.com

Boris S. Filippov — Post-Graduate Student; St. Petersburg State University of Aerospace Instrumentation, Department of Infocommunication Systems; E-mail: FilippovBoris@gmail.com

P. 68—70.

VIDEO WATERMARKING ALGORITHM FOR H.264 COMPRESSED VIDEO

A method of video protection from redistribution with digital watermarks is proposed. The most popular family of digital watermarking algorithms for H.264 standard is considered. The problem of construction of individual labels resistant to coalition attacks is addressed. The Tardos code is chosen because of minimum length among the existing codes.

Keywords: H.264, watermarking, frame-proof codes.

Data on authors

Alexandra V. Afanasyeva — Master of Sci.; St. Petersburg State University of Aerospace Instrumentation, Department of Information Systems Security; Programmer; E-mail: alra@vu.spb.ru

Denis O. Ivanov — St. Petersburg State University of Aerospace Instrumentation, Department of Information Systems Security; Programmer; E-mail: denis.ivo@vu.spb.ru

Dmitry A. Ryzhov — Post-Graduate Student; St. Petersburg State University of Aerospace Instrumentation, Department of Information Systems Security; E-mail: dr@vu.spb.ru

P. 71—77.

EFFICIENCY ASSESSMENT OF CACHE PARTITION SIZES MANAGEMENT ALGORITHM IN STORAGE SYSTEM

A model of storage system cache consisting of two partitions is considered. An algorithm that redistributes the partitions sizes is proposed. The impact of current and next state detection errors on algorithm efficiency is evaluated.

Keywords: storage systems, cache, efficiency evaluation.

Data on authors

Vasily S. Duzhin — Post-Graduate Student; St. Petersburg State University of Aerospace Instrumentation, Department of Information Systems Security; E-mail: vduzhin@gmail.com

Grigory S. Evseev — Cand. Techn. Sci.; St. Petersburg State University of Aerospace Instrumentation, Department of Processing and Electronic Systems; E-mail: egs@vu.spb.ru

Evgeny M. Linsky — Cand. Techn. Sci.; St. Petersburg State University of Aerospace Instrumentation, Department of Information Systems Security; E-mail: evlinsky@vu.spb.ru

P. 77—81.

ESTIMATION OF RELIABILITY OF FAILURE-SAFE CLUSTERS WITH DIRECT CONNECTION TO STORAGE DEVICES

Variants of configuration of clusters with direct connection to binary-input storage devices and servers are considered. An approach to estimation of reliability of the configurations is proposed.

Keywords: fault tolerance, cluster, reliability, reservation, storage device, server.

Data on authors

Vladimir A. Bogatyrev — Dr. Techn. Sci., Professor; St. Petersburg State University of Aerospace Instrumentation, Department of Information Systems Security;
E-mail: Vladimir.bogatyrev@gmail.com

Stanislav V. Bogatyrev — St. Petersburg State University of Aerospace Instrumentation, Department of Information Systems Security; Junior Scientist; E-mail: realloc@gmail.com

Anatoly V. Bogatyrev — Post-Graduate Student; St Petersburg National Research University of Information Technologies, Mechanics and Optics, Department of Computer Technology;
E-mail: ganglion@gmail.com