УДК 621.391

СОВЕРШЕНСТВОВАНИЕ СПОСОБОВ ОБМЕНА ИНФОРМАЦИЕЙ В ВЫСОКОСКОРОСТНЫХ БЕСПРОВОДНЫХ ИНФОРМАЦИОННЫХ СЕТЯХ С ИСПОЛЬЗОВАНИЕМ НОВЫХ ТИПОВ АНСАМБЛЕЙ ДИСКРЕТНЫХ ПОСЛЕДОВАТЕЛЬНОСТЕЙ

Жук А. П.[1], Петренко В. И. [1], Кузьминов Ю. В. [1], Жук Е. П. [1], Луганская Л. А. [1]

[1]ФГАОУ ВПО «Северо-Кавказский федеральный университет», Ставрополь, Россия (355029, г. Ставрополь, просп. Кулакова, 2), e-mail: info@ncfu.ru

В статье рассматривается задача повышения структурной скрытности информационного обмена в высокоскоростных беспроводных информационных сетях на основе усовершенствования способа передачи информации за счет стохастического использования ансамблей дискретных ортогональных многоуровневых последовательностей. Сущность предлагаемого способа заключается в том, что для передачи сообщений, сменяемых от одного информационного символа к другому, предлагается использовать стохастическим образом системы ортогональных многоуровневых последовательностей, описываемых собственными векторами диагональной симметрической матрицы. Сравнительный анализ предлагаемого способа передачи информации показывает преимущество его использования для повышения структурной скрытности передаваемых сообщений в высокоскоростных беспроводных информационных сетях на основе технологии CDMA по сравнению с наиболее известными способами многоканальной передачи информации.

Ключевые слова: структурная скрытность, стохастическое использование, дискретные ортогональные многоуровневые последовательности.

IMPROVEMENT OF METHODS OF INFORMATION SHARING HIGH-SPEED WIRELESS INFORMATION NETWORKS WITH THE USE OF NEW TYPES OF ENSEMBLES OF DISCRETE SEQUENCES

Zhuk A. P.[1], Petrenko V. I. [1], Kuzminov U. V.[1], Zhuk E. P.[1], Luganskaja L. A.[1]

[1]North Caucasian Federal University, Stavropol, Russia (355029, Stavropol, prospect Kulakov 2), e-mail: info@ncfu.ru

The article considers the problem of structural secrecy of information exchange in high-speed wireless information networks on the basis of improving ways of transmitting information through stochastic use of ensembles of discrete orthogonal multi-tiered sequences. The essence of the method consists in that for transmission of messages of the exchangeable information from one character to another using a stochastic systems, orthogonal multi-tiered sequences described own vectors diagonal symmetric matrix. Comparative analysis of the proposed method of transmitting information, shows the advantage of using it to improve structural secrecy of messages transmitted high-speed wireless information networks on the basis of technology CDMA compared with the most known methods of multichannel information transfer.

Keywords: structural secrecy, stochastic use, discrete orthogonal multi-level sequence.

Введение

Технология многостанционного доступа с кодовым разделением каналов (Code Division Multiple Access – CDMA) получает все более широкое распространение в современных системах радиосвязи различного назначения. Системы такого рода используют для передачи информации по каналу связи ансамбли дискретных последовательностей в виде шумоподобных сигналов (ШПС) [7].

Сегодня технологии CDMA находят применение в сотовых системах подвижной связи, системах беспроводного абонентского доступа, спутниковых системах подвижной связи, беспроводных компьютерных сетях и др. Данная технология (IMT-2000) легла в

основу большей части проектов стандартов, реализуемых в высокоскоростных беспроводных информационных сетях третьего поколения 3G.

Известно [7], что конфиденциальность передачи сообщений в беспроводных информационных сетях может быть достигнута путем обеспечения:

- энергетической скрытности сигналов – переносчиков информации;
- структурной скрытности сигналов – переносчиков информации;
- информационной скрытности передаваемого сообщения.

Сравнительный анализ возможных способов обеспечения конфиденциальности информации в беспроводных информационных сетях на основе технологии CDMA показывает, что наиболее целесообразно использовать не все выше перечисленные способы, а лишь те, которые относятся к оценке структурной скрытности, ввиду наименьшей проработанности данного направления [2].

Целью статьи является повышение структурной скрытности информационного обмена в высокоскоростных беспроводных информационных сетях на основе усовершенствования способа передачи информации за счет стохастического использования ансамблей дискретных ортогональных многоуровневых последовательностей.

В настоящее время известно несколько способов обмена информацией в высокоскоростных беспроводных информационных сетях на основе технологии CDMA, обеспечивающих структурную скрытность информационного обмена, использующие различные ансамбли дискретных последовательностей [2, 3, 6, 7]:

1. Способ многостанционного доступа с кодовым разделением каналов, описываемый стандартом IS-95 (коммерческое название cdmaOne), суть которого заключается в расширении спектра частот на основе использования 64 видов последовательностей, сформированных по закону функций Уолша [6]. Поскольку применяемые последовательности взаимно ортогональны, то взаимные помехи между каналами передачи базовой станции отсутствуют [3].

Недостатком этого способа является то, что сигналы Уолша имеют регулярную структуру, которая заранее известна. Поэтому беспроводная информационная сеть, построенная на основе стандарта IS-95, будет обладать низкой структурной скрытностью.

2. Способ многостанционного доступа, используемый в системе передачи данных с кодовым разделением каналов, который включает операцию одновременной передачи сложных широкополосных сигналов на основе нелинейных последовательностей де Брейна со сменой формы последовательности в процессе передачи сообщения от одного информационного символа к другому [8].

Несмотря на то что количество ортогональных сигналов, формируемых на основе кодовых словарей де Брейна, больше числа ортогональных сигналов Уолша размерности N, однако их количество является конечным для любой размерности N, что позволяет сделать вывод об их низкой структурной скрытности.

3. Способ передачи информации в системах с кодовым разделением каналов, заключающийся в том, что для передачи сообщений применяют производные ортогональные системы сигналов, которые получают в результате перемножения каждого сигнала ортогональной системы на производящий сигнал. В качестве основы используется исходная система ортогональных сигналов, являющаяся первым сомножителем, а в качестве второго сомножителя используется производящий сигнал, при этом каждый ортогональный сигнал исходной системы посимвольно умножают на производящий сигнал [2, 6, 7].

Количество известных производных ортогональных сигналов размерности N, безусловно, больше числа ортогональных сигналов Уолша, однако их количество ограничено, они существуют только для определенных размерностей N, что позволяет сделать вывод об их низкой структурной скрытности.

Таким образом, можно сделать вывод, что все существующие способы обмена информацией в высокоскоростных беспроводных информационных сетях на основе технологии CDMA имеют существенный недостаток, заключающийся в том, что количество структур ансамблей дискретных последовательностей, используемых в них для передачи информации, мало, что, в свою очередь, свидетельствует о высокой вероятности раскрытия структуры используемых сигналов-переносчиков.

По мнению авторов, данный недостаток можно существенно снизить за счет применения в высокоскоростных беспроводных информационных сетях на основе технологии CDMA способа передачи информации на основе хаотически формируемых ансамблей дискретных многоуровневых ортогональных сигналов.

Сущность предлагаемого способа заключается в том, что для передачи сообщений, сменяемых от одного информационного символа к другому, предлагается использовать системы ортогональных последовательностей, описываемых собственными векторами диагональной симметрической матрицы A размерностью N [2]:

$$A = \begin{bmatrix} \alpha_{1,1} & \alpha_{1,2} & \dots & \alpha_{1,N} \\ \alpha_{2,1} & \alpha_{2,2} & \dots & \alpha_{2,N} \\ \dots & \dots & \dots & \dots \\ \alpha_{N,1} & \alpha_{N,2} & & \alpha_{N,N} \end{bmatrix}, \qquad (1)$$

где $\alpha_{i,j} = \alpha_{j,i}, (i = \overline{1,N};\ j = \overline{1,N})$.

При этом используется свойство ортогональности собственных векторов, заключающееся в том, что собственные векторы, соответствующие различным собственным значениям нормального оператора, попарно ортогональны [5].

Известно, что всякий ненулевой вектор x называется собственным вектором матрицы A, если найдется такое число λ, что будет выполняться равенство:

$$A \cdot x = \lambda \cdot x. \tag{2}$$

Это число λ называется собственным значением матрицы A, соответствующим собственному вектору x.

Если в пространстве выбран определенный базис, то уравнение (2) для собственных векторов и собственных значений линейного преобразования можно записать в матричной форме:

$$A \cdot X = \lambda \cdot X. \tag{3}$$

Всякий ненулевой столбец X, для которого выполняется равенство (3), называется собственным вектором матрицы A, соответствующим собственному значению λ.

Собственный вектор матрицы A – это столбец, составленный из координат собственного вектора $x = (x_1, x_2, ..., x_N)$ линейного преобразования $y = A \cdot x$ в выбранном базисе.

Собственные векторы x_i вещественной диагональной симметрической матрицы A, отвечающие различным собственным значениям λ_i, ортогональны, т.е. их скалярное произведение равно нулю [4]:

$$\overline{x_i \cdot x_j} = 0, (i = \overline{1, N};\ j = \overline{1, N}) \tag{4}$$

Из вышесказанного следует, что для любой вещественной диагональной симметрической матрицы A, описываемой соотношением (1), существует набор собственных значений $\lambda = \{\lambda_1, \lambda_2, ..., \lambda_N\}$ и каждому собственному значению соответствует собственный вектор x_i, который попарно ортогонален с любым из собственных векторов, соответствующих другим собственным значениям матрицы A.

Таким образом, множество диагональных элементов матрицы A, описываемых соотношением (1), позволяет получить множество собственных векторов x_i этой матрицы, которое можно использовать в качестве модели ансамблей дискретных ортогональных многозначных последовательностей (АДОМП) [2].

Поэтому стохастическое применение множества АДОМП, описываемых собственными векторами различных диагональных симметрических матриц, позволит повысить структурную скрытность высокоскоростных беспроводных информационных

сетей на основе технологии CDMA. Нелинейность формируемых структур сигналов достигается за счет того, что на каждом такте передачи информационного сообщения, расширяющая последовательность в виде одного из сигналов ортогональной системы сигналов, описываемых собственными векторами диагональной симметрической матрицей, формируется путем стохастического задания набора диагональных коэффициентов, симметрической матрицы, генератором случайных положительных чисел.

Предлагаемый способ осуществляется в следующей последовательности: сначала с помощью вспомогательного синхронизирующего сложного сигнала передающая аппаратура базовой станции и приемная аппаратура каждой из 2^{m-1} абонентских станций вводится в цикловую фазу. Затем посредством манипуляции вспомогательного сигнала синхронизации на каждый канал передается служебная информация (единый начальный блок для всех абонентских станций). После выполнения указанной процедуры начинается одновременная передача всем абонентам цифровой информации, при этом каждому биту информации фиксированного канала ставится в соответствие сложный сигнал, структура которого зависит от значений коэффициентов диагональной положительно определенной симметрической матрицы, которые формируются генератором случайных положительных чисел, причем расширение информационной последовательности происходит указанным выше способом [9].

После передачи очередного информационного бита на передающей и приемной стороне производится синхронная смена коэффициентов диагональной положительно определенной симметрической матрицы, поступающих от идентичных генераторов случайных положительных чисел (ГСПЧ) в приемной и передающей стороне, на основе которых происходит расчет сформированных стохастическим образом АДОМП, описываемых собственными векторами диагональных положительно определенных симметрических матриц. При этом сигнал, используемый на приемной стороне для корреляционной обработки, будет иметь структуру, совпадающую с сигналом, излучаемым передатчиком, и, следовательно, может быть использован для обработки информационного потока, адресованного получателю цифровой информации.

Сравним предлагаемый способ передачи информации с известными способами по параметру структурной скрытности передаваемого сообщения.

Для расчета количества структур сигналов Z в предлагаемом способе использовалась формула для неупорядоченных сочетаний с повторением элементов [1]:

$$Z = C_n^k = \left(\frac{(n+k-1)!}{k! \cdot (n-1)!} \right) \cdot N, \qquad (5)$$

где n – диапазон возможных значений диагональных коэффициентов матрицы A (например n=5);

k – количество элементов диагональной симметрической матрицы размерностью N находящихся ниже или выше главной диагонали;

N – размерность диагональной симметрической квадратной матрицы A и количество каналов передачи, используемых в высокоскоростных беспроводных информационных сетях на основе технологии CDMA.

Для расчета количества элементов k диагональной симметрической матрицы размерностью N находящихся ниже или выше главной диагонали используется следующее соотношение:

$$k = \frac{N \cdot N - N}{2}. \tag{6}$$

Для расчета количества структур сигналов де Брейна, используемых в способе №2, в качестве расширяющих последовательностей использовалась формула [8]:

$$Z = \left(2\prod_{i=1}^{d} b_i \right) \cdot N, \tag{7}$$

где b_i – число элементов в i-м цикле подстановки V_{10} , содержащей два и более элементов;

m – число элементов памяти регистра сдвига;

d – общее число циклов подстановки V_{10} с двумя и более элементами.

Для расчета количества структур сигналов в способе №1 и способе №3 использовалась формула для неупорядоченных сочетаний с повторением элементов [2]:

$$Z = C_g^N = \left(\frac{(g + N - 1)!}{N! \cdot (g - 1)!} \right) \cdot N, \tag{8}$$

где $g = 2$;

N – размерность ансамбля сигналов.

Результаты расчетов количество возможных структур сигналов, формируемых каждым из способов передачи информации в высокоскоростных беспроводных информационных сетях на основе технологии CDMA, представлены в таблице 1.

На основе проведенных расчетов количества возможных структур сигналов Z, полученных известными и предлагаемым способами, можно сделать следующие выводы.

Таблица 1 – Результаты расчетов количества возможных структур сигналов

Количество каналов передачи N	**Количество всевозможных структур сигналов Z**			
	Предлагаемый способ	**Способ №1**	**Способ №2**	**Способ №3**

16	$1{,}4\times10^{8}$	16	192	272
32	8×10^{10}	32	$9{,}2\times10^{3}$	1×10^{3}
64	$4{,}4\times10^{13}$	64	$2{,}1\times10^{6}$	$4{,}1\times10^{3}$
128	$8{,}8\times10^{16}$	128	$3{,}7\times10^{11}$	$1{,}6\times10^{4}$
256	$2{,}5\times10^{20}$	256	$1{,}3\times10^{20}$	$6{,}5\times10^{5}$

Выводы:

1. В статье представлен способ передачи информации на основе стохастического применения АДОМП, который позволяет на основе множества собственных векторов диагональной симметрической матрицы *A* получить множество структур дискретных многоуровневых ортогональных сигналов.

2. Сравнительный анализ способа передачи информации на основе хаотически формируемых ансамблей дискретных ортогональных многоуровневых последовательностей показал преимущество его использования для повышения структурной скрытности передаваемых сообщений в высокоскоростных беспроводных информационных сетях на основе технологии CDMA по сравнению с наиболее известными способами многоканальной передачи информации.

3. Увеличение числа структур сигналов формируемых предложенным способом и, как следствие, уменьшение вероятности их раскрытия может быть достигнуто за счет расширения диапазона *n* возможных значений диагональных коэффициентов симметрической матрицы *A*.

Список литературы

1. Волковец А. И. Теория вероятности и математическая статистика: Практикум для студ. всех спец. БГУИР дневной формы обучения / А. И. Волковец, А. Б. Гуринович. – Мн.: БГУИР, 2003. – С.5.

2. Жук А. П., Иванов А. С. Вариант повышения структурной скрытности системы передачи информации с кодовым разделением каналов // Труды Северо-Кавказского филиала Московского технического университета связи и информатики. – Ростов–на–Дону.: ПЦ «Университет» СКФ МТУСИ, 2011. – 348 с.

3. Защита информации в системах мобильной связи: Учебное пособие для вузов /А. А. Чекалин, А. В. Заряев, С. В. Скрыль и др.; Под общей научной редакцией доктора техн. наук А. В. Заряева и доктора техн. наук С. В. Скрыля. – 2-е изд. испр. и доп. – М.: Горячая линия – Телеком, 2005. – 171 с.

4. Клиот-Дашинский М. И. Алгебра матриц и векторов: Учебники для вузов. Специальная литература. 3-е изд., стер. – СПб.: Издательство «Лань», 2001. – 160с.
5. Корн Г., Корн Т.. Справочник по математике (для научных работников и инженеров). – М.: Издательство «Наука», 1974. – 436 с.
6. Никитин Г. И. Применение функций Уолша в сотовых системах связи с кодовым разделением каналов: Учеб. пособие / СПбГУАП. – СПб., 2003. – 86 с.
7. Общесистемные вопросы защиты информации. Коллективная монография / Под ред. Е. М. Сухарева. Кн. 1. – М.: Радиотехника, 2003. – 296с.
8. Патент Российской Федерации № 2234191, кл. H04B7/216, H04L9/26 от 24.07.2001
9. Столингс В. Беспроводные линии связи и сети. : Пер. с англ. – М.: Издательский дом «Вильямс», 2003. – 213 с.

Рецензенты:

Тищенко Е.Н., д.э.н., профессор, заведующий кафедрой информационная безопасности ФГБОУ ВПО «Ростовский государственный экономический университет (РИНХ)», г.Ростов-на-Дону.

Шуваев А.В., д.э.н., профессор, профессор кафедры прикладной информатики ФГБОУ ВПО «Ставропольский государственный аграрный университет», г. Ставрополь.