

ЭЛЕКТРОТЕХНИКА И ЭЛЕКТРОННЫЕ УСТРОЙСТВА

УДК 621.391.037.3

А.А. Гладких, С.М. Наместников, Н.А. Пчелин

ПОВЫШЕНИЕ ДОСТОВЕРНОСТИ ДАННЫХ В СИСТЕМЕ БЕСПРОВОДНЫХ СЕНСОРНЫХ СЕТЕЙ¹



Гладких Анатолий Афанасьевич, доктор технических наук, окончил Военную академию связи им. С.М. Буденного, адъюнктуру ВАС, профессор кафедры «Телекоммуникации» Ульяновского государственного технического университета. Имеет монографии, учебные пособия, статьи и патенты РФ в области помехоустойчивого кодирования и защиты информации. [e-mail: a.gladkikh@ulstu.ru].



Наместников Сергей Михайлович, кандидат технических наук, окончил УлГТУ, аспирантуру там же, доцент кафедры «Телекоммуникации» УлГТУ. Имеет статьи в области статистической обработки сигналов. [e-mail: sernam@ulstu.ru].



Пчелин Никита Александрович, окончил Ульяновское высшее военное командное училище связи. Главный конструктор ФНПЦ АО «НПО «Марс». Имеет публикации в области помехоустойчивого кодирования. [e-mail: pna3@yandex.ru].

Аннотация

Беспроводные сенсорные сети в современных условиях рассматриваются как важная телекоммуникационная составляющая во многих предметных областях, связанных с дистанционным и практически непрерывным получением разнородной информации от заданного множества контрольных точек. Примерами прикладного назначения таких сетей являются системы мониторинга окружающей среды, контроля протяженных периметров или труднодоступных районов, оценка состояния обширных объектов и сооружений. Преимущества таких сетей очевидны,

¹ Исследование выполнено при финансовой поддержке РФФИ и Правительства Ульяновской области в рамках научного проекта № 16-47-732011\18.

но их реализация существенным образом зависит от системы энергоснабжения элементов описываемых сетей в связи с ограниченным сроком действия встроенного аккумулятора для каждого датчика узла. Минимальное энергопотребление датчиков и процессоров узлов имеет решающее значение для успешной реализации сетевых операций. Применение корректирующих кодов позволяет решить указанную задачу наиболее эффективным способом за счет понижения мощности передатчика узла при заданных параметрах на достоверность данных. Очевидно, что понижение мощности передатчика должно быть компенсировано экономной работой декодера избыточного кода. Более мощные коды обеспечивают лучшую производительность узла при меньших энергозатратах, при этом декодеры таких кодов требуют повышенного расхода энергии. Поиск решения указанного противоречия представляет собой актуальную задачу для развития сенсорных сетей. Предыдущие исследования применения избыточных кодов в сенсорных сетях были ориентированы на достаточно изученные алгоритмы обработки сверточных кодов, кодов Рида-Соломона, на системы каскадных кодов. Обработка указанных кодов осуществлялась с использованием жестких методов и основывалась на использовании метрики Хэмминга. В статье доказывается целесообразность применения метода перестановочного декодирования к системе двоичных и недвоичных избыточных кодов, позволяющего повысить энергетический выигрыш кода применительно к двоичным кодам или решить задачу снижения сложности реализации декодера в условиях использования недвоичных вариантов построения таких кодов.

На основе линейных свойств групповых кодов описывается унифицированный алгоритм быстрых матричных преобразований к совокупности систематических кодов над двоичными и расширенными полями Галуа.

Эта процедура используется как атрибут при переходе от основного избыточного кода к его эквивалентному аналогу. Вводится понятие когнитивной процедуры применительно к однотипным перестановкам. Реализация указанных алгоритмов базируется на мягких методах обработки данных.

Ключевые слова: сенсорные сети, мягкое решение символа, перестановочное декодирование, когнитивная карта декодера, каскадное кодирование.

Abstract

Wireless sensor networks (WSN) in modern conditions are considered as an important component of telecommunications in many subject areas associated with remote and near-continuous obtaining diverse information from a given set of control points. Examples of application of such networks are the systems of environmental monitoring, control of long perimeters or inaccessible areas, evaluation of large objects and structures. The advantages of such networks are obvious but their implementation strongly depends on the power supply systems elements of the described networks due to expiration date of the built-in battery for each sensor node. Low-power sensors and processors of the nodes is crucial for the successful implementation of network activities. The use of error correcting codes allows to solve the specified task in the most efficient way by reducing the transmitter power of the node with the specified parameters on the accuracy of the data. Obviously, lowering the transmitter power should be compensated for the economical operation of the decoder of the redundant code. More powerful codes provide better performance node with lower energy consumption, in this case the decoders of such codes require increased energy expenditure. The search of solution to this disconnection is a topical task for the development of sensor networks. Previous studies of the use of redundant codes in sensor networks has been focused on sufficiently studied processing algorithms of convolutional codes, Reed-Solomon codes, concatenated codes system. Processing of these codes was carried out with the use of the harsh methods and based on the use of the Hamming metric. The article proves expediency of application of the method of permutation decoding to the system of binary and non-binary redundant codes, which allows to increase the energy gain code (EVK) for binary codes and solve the problem of reducing the complexity of decoder in terms of the using nonbinary options for constructing such codes.

Based on the linear properties of group codes, the standardized algorithm for fast matrix transformations to a set of systematic codes over the binary and extended Galois fields is described.

The procedure is used as a mandatory attribute in the transition from primary redundant code to its equivalent counterpart. The authors introduce the concept of cognitive procedures with respect to similar permutations. The implementation of these algorithms is based on soft methods of data processing.

Key words: sensor networks, soft symbol solution, permutation decoding, cognitive decoder map, concatenated code.

ВВЕДЕНИЕ

Передовые методы обработки помехоустойчивых кодов в системах радиосвязи, в том числе и в системах беспроводных сенсорных сетей (БСС), безусловно используют мягкие алгоритмы декодирования принятых кодовых векторов. Наиболее обсуждаемой технологией выработки мягких решений символов (MPC) двоичных

кодов является процедура вычисления логарифма отношения правдоподобия [1, 2]. Численные значения этого параметра оцениваются аналитическим выражением вида $\lambda = 2E_b z / \sigma^2$, где E_b – энергия сигнала, приходящаяся на бит, z – уровень принятого сигнала, а σ^2 – дисперсия гауссовского шума. Очевидно, что мешающие факторы в беспроводном канале связи не всегда подчиняются

закономерностям, описываемым потоком независимых ошибок и, более того, знание параметра σ^2 требует предварительных измерений, что приводит к временным задержкам. Более того, указанные измерения по соображениям энергосбережения недопустимы в БСС.

В современных телекоммуникационных системах в качестве критерия эффективности применения в них помехоустойчивого кодирования выбирают значение получаемого от этой процедуры энергетического выигрыша кода (ЭВК). Известно, что в канале с гауссовским шумом при условии, что отношение $E_b/N_0 \rightarrow \infty$, в котором значение N_0 – спектральная плотность гауссовского шума, в случае жестких решений и реализации алгоритма исправления t ошибок или исправления S стираний с использованием метрики Хэмминга (параметр d_{min}) ЭВК оценивается выражениями, приведенными в работах [3, 4].

Разложение групповых двоичных кодов на смежные классы указывает на то, что допускается исправление образцов ошибок, кратность которых выходит за пределы, определяемые метрикой d_{min} [3]. Поэтому более тонкой оценкой ЭВК от применения блокового двоичного кода может служить выражение $D_m = 10 \lg(1 - R + 1/n)$ дБ, где k – число информационных разрядов, n – длина кодового вектора, а $R = k/n$ – скорость кода. Предполагается, что $d_{min} = n - k + 1$, что соответствует параметрам максимально декодируемых кодов [4–6]. Известно, что не двоичные коды, например, коды Рида-Соломона (РС) точно обеспечивают значение D_m , что нельзя сказать о двоичных кодах, которые не являются максимально декодируемыми кодами [3]. Для двоичных кодов наилучший результат приближения к границе D_m обеспечивает метод перестановочного декодирования, который предполагает выработку МРС в ходе приема данных, выбор k наиболее надежных символов из n принятого кодового вектора и формирование на этой основе вектора эквивалентного кода и его поэлементного сравнения с символами принятого из канала связи вектора [3]. С высокой вероятностью это обеспечивает выявления вектора ошибок.

СТАТИСТИЧЕСКИЕ ХАРАКТЕРИСТИКИ БЕСПРОВОДНОГО КАНАЛА БСС

В каналах с неизвестными параметрами, которые характерны для систем БСС, при выработке МРС целесообразно использовать свойства стирающего канала связи с широким интервалом стирания в соответствии с аналитическим выражением

$$\lambda_i(z) = \left| \frac{\lambda_{max}}{\rho M_z} \times z \right|, \quad (1)$$

где λ_{max} – максимальное значение МРС, принятое для данной системы, M_z – математическое ожидание принимаемых сигналов, ρ – интервал стирания (обычно

$0 \leq \rho < 1$), а z – значение принятого сигнала с учетом влияния мешающих факторов [3]. Применение этого метода не требует энергетических затрат и развито в основном на двоичные виды модуляции, но он может быть использован и в системе с сигнально-кодowymi конструкциями [2, 6]. На рисунке 1 представлены результаты испытаний имитационной модели формирования МРС в соответствии с выражением (1) для двоичных видов модуляции. В ходе испытаний оценивалась частота ошибочных решений P_λ для различных λ_i , когда $i = \overline{1, 7}$, при разных отношениях E_b/N_0 .

Из гистограмм заметно, что для формирования комбинаций эквивалентного кода целесообразно использовать оценки от значения λ_4 до значения λ_7 . Точные значения ошибочных решений по результатам имитационного моделирования показаны в таблицах 1 и 2.

В таблице 2 более темная заливка ячеек характеризует выигрыш по достоверности, который обеспечивается фазовой модуляцией относительно амплитудной модуляции при равных значениях параметра E_b .

Пусть принятый из канала связи кодовый вектор с ошибками V_n имеет в своем составе набор оценок λ_i . Ранжируя эти оценки по убыванию, декодер разбивает символы вектора V_n на две группы. В первую группу входят k символов с наибольшими значениями МРС, тогда во вторую группу войдут все оставшиеся символы вектора V_n , в которых с высокой вероятностью сосредоточены ошибки. Перестановка символов фиксируется матрицей перестановок P . Если среди символов первой группы оказывается хотя бы один ошибочный символ, то вектор эквивалентного кода не будет соответствовать переданному вектору, что приведет к ошибке декодирования комбинации $P_{ком}$. При появлении среди k переставленных символов одной ошибки вероятность $P_{ком}$ события будет оцениваться выражением $P_{ком} \approx p_b \times k \approx \lambda_i \times k$. Чтобы снизить риски подобного исхода, допустимо использовать алгоритм перестановочного декодирования, начиная с 4 дБ. При этом в системе продуктивно использовать короткие коды. При меньших отношениях сигнал-шум возникает необходимость применения повтора данных или использования композиции кодов, например, в виде каскадных конструкций. В общем случае перестановочное декодирование обеспечивает дополнительный ЭВК в пределах 2 дБ относительно мягких методов обработки данных, что способно повысить эффект энергосбережения элементов питания БСС [1, 7 – 9].

ОБЩИЕ ПРИНЦИПЫ ПЕРЕСТАНОВОЧНОГО ДЕКОДИРОВАНИЯ

Особенностью перестановочного декодирования является необходимость преобразования порождающей матрицы G основного кода к переставленной матрице эквивалентного кода G_{nep} в соответствии со структурой матрицы P [3, 10–12]. Очевидно подобная процедура

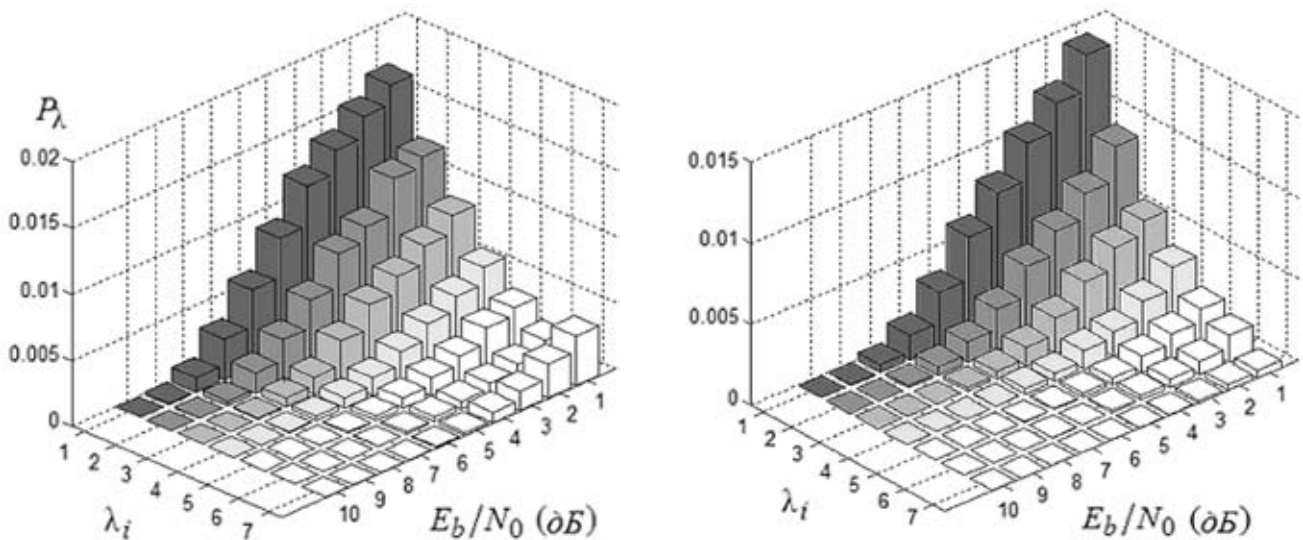


Рис. 1. Гистограммы частоты ошибочной регистрации MPS с различными целочисленными значениями: а) при использовании амплитудной модуляции; б) при использовании фазовой модуляции

Таблица 1

Оценка вероятности ошибочных MPS при использовании амплитудной модуляции

E_b/N_0 (дБ)	σ^2	λ_1	λ_2	λ_3	λ_4	λ_5	λ_6	λ_7
0	1	$1,7 \cdot 10^{-2}$	$1,2 \cdot 10^{-2}$	$9,5 \cdot 10^{-3}$	$5,9 \cdot 10^{-3}$	$3,9 \cdot 10^{-3}$	$2,5 \cdot 10^{-3}$	$3,4 \cdot 10^{-3}$
0,46	0,9	$1,6 \cdot 10^{-2}$	$1,0 \cdot 10^{-2}$	$7,5 \cdot 10^{-3}$	$5,1 \cdot 10^{-3}$	$2,9 \cdot 10^{-3}$	$1,8 \cdot 10^{-3}$	$2,4 \cdot 10^{-3}$
0,97	0,8	$1,3 \cdot 10^{-2}$	$9,2 \cdot 10^{-3}$	$5,9 \cdot 10^{-3}$	$3,5 \cdot 10^{-3}$	$2,1 \cdot 10^{-3}$	$1,2 \cdot 10^{-3}$	$1,1 \cdot 10^{-3}$
1,55	0,7	$1,2 \cdot 10^{-2}$	$7,0 \cdot 10^{-3}$	$4,4 \cdot 10^{-3}$	$2,4 \cdot 10^{-3}$	$1,4 \cdot 10^{-3}$	$6,2 \cdot 10^{-4}$	$7,4 \cdot 10^{-4}$
2,22	0,6	$8,7 \cdot 10^{-3}$	$5,4 \cdot 10^{-3}$	$2,8 \cdot 10^{-3}$	$1,4 \cdot 10^{-3}$	$7,7 \cdot 10^{-4}$	$3,6 \cdot 10^{-4}$	$3,1 \cdot 10^{-4}$
3,01	0,5	$6,0 \cdot 10^{-3}$	$3,8 \cdot 10^{-3}$	$1,6 \cdot 10^{-3}$	$6,4 \cdot 10^{-4}$	$2,8 \cdot 10^{-4}$	$1,6 \cdot 10^{-4}$	$5,0 \cdot 10^{-5}$
3,98	0,4	$3,3 \cdot 10^{-3}$	$1,7 \cdot 10^{-3}$	$4,8 \cdot 10^{-4}$	$2,1 \cdot 10^{-4}$	$1,4 \cdot 10^{-4}$	$2,0 \cdot 10^{-5}$	0
5,23	0,3	$1,0 \cdot 10^{-3}$	$4,1 \cdot 10^{-4}$	$1,4 \cdot 10^{-4}$	$2,0 \cdot 10^{-4}$	0	0	0

Таблица 2

Оценка вероятности ошибочных MPS при использовании двоичной фазовой модуляции

E_b/N_0 (дБ)	σ^2	λ_1	λ_2	λ_3	λ_4	λ_5	λ_6	λ_7
0	1	$1,4 \cdot 10^{-2}$	$9,3 \cdot 10^{-3}$	$5,9 \cdot 10^{-3}$	$3,6 \cdot 10^{-3}$	$2,0 \cdot 10^{-3}$	$1,5 \cdot 10^{-3}$	$3,7 \cdot 10^{-4}$
0,46	0,9	$1,2 \cdot 10^{-2}$	$7,9 \cdot 10^{-3}$	$4,6 \cdot 10^{-3}$	$2,7 \cdot 10^{-3}$	$1,6 \cdot 10^{-3}$	$9,2 \cdot 10^{-4}$	$3,3 \cdot 10^{-4}$
0,97	0,8	$1,0 \cdot 10^{-2}$	$6,2 \cdot 10^{-3}$	$3,4 \cdot 10^{-3}$	$1,8 \cdot 10^{-3}$	$9,7 \cdot 10^{-4}$	$5,2 \cdot 10^{-4}$	$1,9 \cdot 10^{-4}$
1,55	0,7	$7,9 \cdot 10^{-3}$	$4,5 \cdot 10^{-3}$	$2,1 \cdot 10^{-3}$	$1,1 \cdot 10^{-3}$	$4,7 \cdot 10^{-4}$	$3,6 \cdot 10^{-4}$	$5,1 \cdot 10^{-5}$
2,22	0,6	$5,7 \cdot 10^{-3}$	$2,4 \cdot 10^{-3}$	$1,1 \cdot 10^{-3}$	$5,7 \cdot 10^{-4}$	$2,5 \cdot 10^{-4}$	$1,3 \cdot 10^{-4}$	$3,1 \cdot 10^{-5}$
3,01	0,5	$3,2 \cdot 10^{-3}$	$1,6 \cdot 10^{-3}$	$6,2 \cdot 10^{-4}$	$2,2 \cdot 10^{-4}$	$6,0 \cdot 10^{-4}$	$4,0 \cdot 10^{-5}$	$1,0 \cdot 10^{-5}$
3,98	0,4	$1,3 \cdot 10^{-3}$	$6,1 \cdot 10^{-4}$	$1,9 \cdot 10^{-4}$	$6,0 \cdot 10^{-5}$	$1,0 \cdot 10^{-5}$	0	0
5,23	0,3	$5,0 \cdot 10^{-4}$	$9,1 \cdot 10^{-5}$	$2,0 \cdot 10^{-5}$	0	0	0	0

не вызывает сложностей вычислительного характера, но последующий шаг перевода матрицы G_{nep} в систематическую форму более сложен, поскольку требует вычисления обратной матрицы, матрицы миноров и нахождения на этой основе обратной матрицы с последующим преобразованием вида $G_{nep} \Rightarrow G_{cuc}$. Производство подобных вычислений для каждой принятой комбинации делает перестановочное декодирование совершенно непроизводительным при решении задач повышения достоверности данных в системах управления реального времени. Для кратного снижения сложности вычислительного процесса $G_{nep} \Rightarrow G_{cuc}$ предла-

гается создать систему эталонных матриц G_{i_3} , каждая из которых будет соответствовать i -му набору перестановок номеров надежных символов принятых кодовых векторов. Преобразование образца матрицы G_{i_3} для любой другой перестановки из соответствующего набора номеров G_{i_3} предлагается осуществлять методом быстрых матричных преобразований (БМП), общая суть которых раскрывается ниже.

Указанные преобразования носят линейный характер, но для двоичных блоковых кодов не все перестановки символов кодовых комбинаций приводят к эквивалентному коду. Такие коды не являются максимально

декодируемыми, и поэтому часть перестановок не обеспечивает свойство невырожденности матриц G_{nep} . Это замечание не относится к системе недвоичных кодов. В любом случае при выделении из принятого вектора k надежных символов номера этих символов могут быть распределены как $k!$ перестановок. Оставшиеся $(n-k)$ номеров аналогично могут быть распределены как $(n-k)!$ перестановок. Всевозможные сочетания перестановок из $k!$ и перестановок из $(n-k)!$ представляют набор эквивалентных кодов для выделенной группы символов. Общее количество таких групп в используемом коде будет составлять C_n^k , следовательно, применение аппарата эталонных матриц в комплексе с БМП снижает объем памяти декодера в $k! \times (n-k)!$ раз.

Пусть в системе обмена данными используется недвоичный код РС с параметрами (7,3,5). Матрица G этого кода в систематической форме имеет вид, где столбцы матрицы нумеруются обычным образом слева направо:

$$G = \begin{pmatrix} \alpha^0 & 0 & 0 & \alpha^4 & \alpha^0 & \alpha^4 & \alpha^5 \\ 0 & \alpha^0 & 0 & \alpha^2 & \alpha^0 & \alpha^6 & \alpha^6 \\ 0 & 0 & \alpha^0 & \alpha^3 & \alpha^0 & \alpha^1 & \alpha^3 \end{pmatrix}, \quad (2)$$

здесь и далее α – примитивный элемент поля $GF(2^3)$.

Пусть надежным символами в некотором принятом кодовом векторе кода РС будут символы с номерами (1 3 5), а менее надежные символы в порядке убывания значений их надежности, например, располагаются в последовательности вида (7 2 4 6). Тогда из выражения (2) следует

$$G_{nep} = \begin{pmatrix} \alpha^0 & 0 & \alpha^0 & \alpha^5 & 0 & \alpha^4 & \alpha^4 \\ 0 & 0 & \alpha^0 & \alpha^6 & \alpha^0 & \alpha^2 & \alpha^6 \\ 0 & \alpha^0 & \alpha^0 & \alpha^3 & 0 & \alpha^3 & \alpha^1 \end{pmatrix}. \quad (3)$$

Для реализации преобразования вида $G_{nep} \Rightarrow G_{cuc}$ в выражении (3) выделяют образ ключевой матрицы вида Q размерности $k \times k$, которая включает в себя первые k столбцов. Тогда обратная матрица для Q является собственно ключевой и однозначно указывает на действия, которые необходимо произвести над строками матрицы G_{nep} для перевода ее в систематическую форму, поскольку $Q \times Q^{-1} = E$. Для рассматриваемого

примера $Q_{3 \times 3} = \begin{pmatrix} \alpha^0 & 0 & \alpha^0 \\ 0 & 0 & \alpha^0 \\ 0 & \alpha^0 & \alpha^0 \end{pmatrix}$, для этой матрицы

$$\det Q = \alpha^0, \text{ и матрица миноров } Q_{3 \times 3}^* = \begin{pmatrix} \alpha^0 & 0 & 0 \\ \alpha^0 & \alpha^0 & \alpha^0 \\ 0 & \alpha^0 & 0 \end{pmatrix},$$

тогда

$$Q_{3 \times 3}^{*T} = \begin{pmatrix} \alpha^0 & \alpha^0 & 0 \\ 0 & \alpha^0 & \alpha^0 \\ 0 & \alpha^0 & 0 \end{pmatrix} = \frac{1}{\det Q} \begin{pmatrix} \alpha^0 & \alpha^0 & 0 \\ 0 & \alpha^0 & \alpha^0 \\ 0 & \alpha^0 & 0 \end{pmatrix}$$

$$\text{и } Q_{3 \times 3}^{-1} = \begin{pmatrix} \alpha^0 & \alpha^0 & 0 \\ 0 & \alpha^0 & \alpha^0 \\ 0 & \alpha^0 & 0 \end{pmatrix}, \text{ тогда } Q_{3 \times 3} \times Q_{3 \times 3}^{-1} = E.$$

Для получения первой строки матрицы в процедуре $G_{nep} \Rightarrow G_{cuc}$ следует умножить первую строку матрицы G_{nep} на α^0 (элемент x_{11} в матрице $Q_{3 \times 3}^{-1}$), затем множить вторую строку матрицы G_{nep} на α^0 (элемент x_{12} в матрице $Q_{3 \times 3}^{-1}$) и сложить полученные результаты по правилу сложения степеней примитивного элемента α в поле $GF(2^3)$. Поступая аналогично с другими ключевыми строками матрицы $Q_{3 \times 3}^{-1}$, получаем переставленную матрицу кода в систематической форме:

$$G_{nep} \Rightarrow G_{cuc} = \begin{pmatrix} \alpha^0 & 0 & 0 & \alpha^1 & \alpha^0 & \alpha^1 & \alpha^3 \\ 0 & \alpha^0 & 0 & \alpha^4 & \alpha^0 & \alpha^5 & \alpha^5 \\ 0 & 0 & \alpha^0 & \alpha^6 & \alpha^0 & \alpha^2 & \alpha^6 \end{pmatrix}. \quad (4)$$

Выполнение подобных действий в процессоре БСС потребует значительных ресурсов по питанию. В ходе исследований установлено, что при сохранения номеров позиций в перестановках k надежных и $(n-k)$ ненадежных символов следует в первом случае переставлять строки матрицы (4), а во втором случае столбцы этой матрицы. Например, при получении надежных символов с последовательностью (1 5 3) в выражении (4) меняются местами строки, не относящиеся к единичной матрице у второй и третьей строки:

$$G_{nep} \Rightarrow G_{cuc153} = \begin{pmatrix} \alpha^0 & 0 & 0 & \alpha^1 & \alpha^0 & \alpha^1 & \alpha^3 \\ 0 & \alpha^0 & 0 & \alpha^6 & \alpha^0 & \alpha^2 & \alpha^6 \\ 0 & 0 & \alpha^0 & \alpha^4 & \alpha^0 & \alpha^5 & \alpha^5 \end{pmatrix}. \quad (5)$$

В случае изменения перестановки номеров ненадежных символов в выражении (4) меняются местами столбцы несистематической части матрицы. Например, при перестановке (2 7 4 6) из выражения (4) будет получено выражение вида:

$$G_{nep} \Rightarrow G_{cuc} = \begin{pmatrix} \alpha^0 & 0 & 0 & \alpha^0 & \alpha^1 & \alpha^1 & \alpha^3 \\ 0 & \alpha^0 & 0 & \alpha^0 & \alpha^4 & \alpha^5 & \alpha^5 \\ 0 & 0 & \alpha^0 & \alpha^0 & \alpha^6 & \alpha^2 & \alpha^6 \end{pmatrix}. \quad (6)$$

Поскольку возможно сочетание вариантов (5) и (6) целесообразно в памяти декодера удерживать единственное упорядоченное значение перестановок, по которому выполнять процедуру $G_{nep} \Rightarrow G_{cuc}$. Например, указанные перестановки целесообразно выполнять, используя образец вида (1 3 5) и (2 4 6 7). Очевидно, этот образец может быть легко получен из выражения (4). Канонический вид преобразования вида $G_{nep} \Rightarrow G_{cuc}$ имеет вид:

$$G_{nep} \Rightarrow G_{cuc} = \begin{pmatrix} \alpha^0 & 0 & 0 & \alpha^0 & \alpha^1 & \alpha^3 & \alpha^1 \\ 0 & \alpha^0 & 0 & \alpha^0 & \alpha^5 & \alpha^5 & \alpha^4 \\ 0 & 0 & \alpha^0 & \alpha^0 & \alpha^2 & \alpha^6 & \alpha^6 \end{pmatrix}. \quad (7)$$

ДЕКОДИРОВАНИЯ НЕДВОИЧНЫХ КОДОВ С ИСПОЛЬЗОВАНИЕМ ПЕРЕСТАНОВОК

Недвоичные коды в информационно-управляющих комплексах могут использоваться самостоятельно или в составе произведения кодов (каскадных конструкциях) на внешней ступени декодирования [3]. На примере кодов РС можно показать, что перестановочное декодирование таких кодов приводит к снижению вычислительной сложности декодера за счет образования постоянных структур в вычислительном процессе декодирования. Образование таких структур не требует обработки стохастических данных кода РС от комбинации к комбинации в процедуре их декодирования, что в конечном счете способствует снижению сложности вычислительного процесса.

Пусть в системе применяется код РС (7,3,5), который способен исправить до четырех стираний, и пусть в качестве внутреннего кода используется укороченный код Хэмминга (6,3,3). За счет декодирования комбинаций этого кода выявляются ненадежно принятые символы, которые обозначим через символ S_i , где $i \in \overline{0,6}$ означает номер позиции в комбинации кода РС. Надежные элементы произвольно обозначим через примитивный элемент поля $GF(2^3)$ как α^j , где $j \in \overline{0,6}$. Предположим, что ненадежные символы по результатам декодирования комбинаций внутреннего кода разместились так, как показано ниже.

0	1	2	3	4	5	6
α^2	S_1	S_2	α^6	S_3	α^2	S_4

В соответствии с расстановкой значений стираний S_i декодер формирует полином синдромов $g(x_c)$. Естественно, что при разных номерах позиций стираний S_i для каждой кодовой комбинации декодер должен менять номера этих позиций, что требует определенного времени. В случае перестановочного декодирования применительно к коду РС значения S_i всегда одинаковы. Например, для приведенной выше таблицы расстановка стираний будет иметь неизменный от комбинации к комбинации кода РС вид.

0	1	2	3	4	5	6
S_1	S_2	S_3	S_4	α^2	α^6	α^3

Естественно, что значения α^j на позициях 4, 5 и 6 будут меняться. Процедура вычисления коэффициентов для $g(x_c)$ принимает вид, показанный в таблице 3.

В таблице 3 выделены столбцы, которые не будут изменять своего значения при заданных параметрах кода

для всего множества принятых приемником комбинаций. С учетом свойства замкнутости элементов поля и возведения в степень на каждой комбинации кода РС при оценке полинома $g(x_c)$ будет тратиться на 9 операций меньше, что составляет около 28% от классического алгоритма. Полином синдромов в конкретном случае будет иметь вид $g(x_c) = x^0\alpha^5 + x\alpha^6 + x^2\alpha^0 + x^3\alpha^2$.

Вторым шагом в процедуре декодирования комбинации кода РС является вычисление полинома локаторов ошибок, который может быть представлен для данного как

$$L(x) = (1 + x\alpha)(1 + x\alpha^2)(1 + x\alpha^3)(1 + x\alpha^4) \Rightarrow \Rightarrow \text{постоянная величина для данного кода.}$$

Можно показать, что для поиска этого полинома экономится до 24 операций сложения и умножения в поле $GF(2^3)$, а с учетом поиска производной полинома $L(x)$, которая тоже является постоянной величиной для кода, тратится на 28 операций меньше. Можно утверждать, что в системе перестановочного алгоритма кода РС экономия по числу операций составляет до 38% от общего числа элементарных операций классического алгоритма декодирования кодов РС в пересчете на блок данных.

Существует другой путь вычисления вектора ошибок, который опирается на метод перестановочного декодирования. Теоретическая основа метода изложена выше. Пусть передатчик отправил вектор кода РС в виде:

$$V_{nep} = \alpha^2 \quad \alpha^2 \quad \alpha^2 \quad \alpha^2 \quad \alpha^2 \quad \alpha^2 \quad \alpha^2$$

и пусть вектор помехи в момент передачи вектора V_{nep} имел вид $V_{ном} = \alpha^4 0 \alpha^3 0^0 \alpha^1$:

$$V_{ном} = \alpha^4 \quad 0 \quad \alpha^3 \quad 0 \quad \alpha^0 \quad 0 \quad \alpha^1.$$

В результате на входе декодера появится вектор, представляющий собой сумму векторов V_{nep} и $V_{ном}$:

$$V_{np} = V_{nep} \oplus V_{ном};$$

$$V_{np} = \alpha^1 \quad \alpha^2 \quad \alpha^5 \quad \alpha^2 \quad \alpha^6 \quad \alpha^2 \quad \alpha^4.$$

Пусть в векторе V_{np} надежно принятыми элементами по показателям функции правдоподобия, полученной от демодулятора, элементы (1 3 6) оказываются наиболее надежными. В этом случае переставленная порождающая матрица для данного вектора соответствует выражению (8). Умножая V_{np} на $G_{nep} \Rightarrow G_{suc}^2$ получим вектор эквивалентного кода, который принимает вид:

$$V_{np} \times G_{nep} \Rightarrow G_{suc} = \alpha^2 \quad \alpha^2 \quad \alpha^2 \quad \alpha^2 \quad \alpha^2 \quad \alpha^2 \quad \alpha^2. \quad (8)$$

Вид полученного вектора (8) соответствует переданному вектору V_{nep} . Это означает, что при любой другой раскладке показателей информационного вектора,

Таблица 3

Алгоритм формирования элементов полинома локаторов ошибок

Для x^0	α^2	α^4	\oplus	α^6	α^5	\oplus	α^3	α^6	=	α^5
Для x^1	α^2	$(\alpha^4)^2 = \alpha^1$	\oplus	α^6	$(\alpha^5)^2 = \alpha^3$	\oplus	α^3	$(\alpha^6)^2 = \alpha^5$	=	α^6
Для x^2	α^2	$(\alpha^4)^3 = \alpha^5$	\oplus	α^6	$(\alpha^5)^3 = \alpha^1$	\oplus	α^3	$(\alpha^6)^3 = \alpha^4$	=	α^0
Для x^3	α^2	$(\alpha^4)^4 = \alpha^2$	\oplus	α^6	$(\alpha^5)^4 = \alpha^6$	\oplus	α^3	$(\alpha^6)^4 = \alpha^3$	=	α^2

определяющего структуру вектора $V_{пер}$, и иных вариантах реализации вектора помехи $V_{ном}$, сложение вектора из выражения (8) с вектором $V_{пр}$ приведет к формированию вектора помехи $V_{ном}$ в явном виде, что в итоге будет означать корректное завершение процедуры декодирования. При всей простоте описанных действий алгоритм с точки зрения применения его в БСС имеет серьезный недостаток. Он энергоемок, поскольку сложность реализации алгоритма с матричными вычислениями определяется как $O(n^3)$, что недопустимо в процессорах БСС. Это приводит к необходимости поиска порождающего полинома для переставленного кода. Зная полином такого кода и применив его параметры в сдвиговом регистре кодера переставленного кода, можно снизить сложность реализации декодера с $O(n^3)$ до $O(n)$. Однако поиск порождающего полинома переставленного кода представляет отдельную научную задачу, решение которой требует специального исследования и описания.

ЗАКЛЮЧЕНИЕ

Развитие БСС имеет широкие перспективы в различных областях, связанных с контролем качества заданных параметров топологически сложных систем с множеством труднодоступных элементов, оценкой состояния и целостности протяженных объектов, охраной периметров большой длины и обширных площадей, в системах оценки трафика дорожного движения и регулирования его с целью оптимизации по заданным критериям. По-видимому, сферы применения БСС по мере развития этой технологии будут расширяться, а востребованность технологии будет нарастать.

Узким местом в БСС являются элементы питания, срок действия которых необходимо поддерживать за счет неэнергоемких технологий. Основная доля энергии элементов питания станций БСС расходуется на поддержание режима приема-передачи данных. За счет эффекта ЭВК помехоустойчивое кодирование способствует снижению мощности передатчика, поэтому внедрение в процессоры БСС средств помехоустойчивого кодирования является актуальной задачей.

Наибольший эффект от применения избыточных кодов следует ожидать на пути использования перестановочного декодирования, демонстрирующего для двоичных кодов наибольший из возможных ЭВК. За счет отказа от матричных вычислений в системе двоичного перестановочного декодирования по предварительным оценкам энергоемкость процедуры декодирования может быть снижена от 20% до 35%.

При использовании недвоичных кодов параметр ЭВК остается постоянной величиной для выбранного кода, но использование перестановочного декодирования

снижает сложность реализации процессора декодера со значения $O(n^3)$ до $O(n)$, за счет снижения доли матричных вычислений.

Перспективным направлением на пути использования средств перестановочного декодирования является поиск путей отказа от эталонных матриц и соответственно отказа от матричных преобразований и замены их соответствующими порождающими полиномами эквивалентных кодов, которые могут непосредственно использоваться в сдвиговых регистрах при кодировании данных таких кодов.

СПИСОК ЛИТЕРАТУРЫ

1. Lettieri P., Fragouli C., Srivastava M.B. Low power error control for wireless links. In Proceedings of the 3rd Annual ACM/IEEE International Conference on Mobile Computing and Networking (MOBICOM '97), Budapest, Hungary, September 1997, pp. 139–150.
2. Деев В.В. Методы модуляции и кодирования в современных системах связи. – СПб. : Наука, 2007. – 267 с.
3. Гладких А.А., Наместников С.М., Пчелин Н.А. Эффективное перестановочное декодирование двоичных блоковых избыточных кодов // Автоматизация процессов управления. – 2017. – № 1 (47). – С. 67–74.
4. Зяблов В.В., Цветков М.А. Метод обнаружения ошибочного декодирования с использованием списков // Информационные процессы. – 2004. – Т. 4, № 2. – С. 188–201.
5. Конопелько В.К., Липницкий В.А. Теория норм синдромов и перестановочное декодирование помехоустойчивых кодов. – М. : Едиториал УРСС, 2004. – 176 с.
6. Мак-Вильямс Ф.Дж. Перестановочное декодирование систематических кодов // Кибернетический сборник. Новая серия. – 1965. – Вып. 1. – С. 35–37.
7. Морелос-Сарагоса Р. Искусство помехоустойчивого кодирования. Методы, алгоритмы, применение. – М. : Техносфера, 2005 – 320 с.
8. Питерсон У., Уэлдон Э. Коды, исправляющие ошибки / пер. с англ. под ред. Р.Л. Добрушина и С.Н. Самойленко. – М. : Мир, 1976. – 594 с.
9. Прокис Джон. Цифровая связь / пер. с англ. под ред. Д.Д. Кловского. – М. : Радио и связь, 2000. – 800 с.
10. Климов Р.В., Солодовникова Д.Н. Методы формирования индексов мягких решений символов на основе модификации параметров канала со стираниями // Радиотехника. – 2014. – № 11. – С. 90–93.
11. Гладких А.А., Климов Р.В., Чилихин Н.Ю. Методы эффективного декодирования избыточных кодов и их современные приложения. – Ульяновск : УлГТУ, 2016. – 258 с.
12. Гладких А.А., Климов Р.В. Численное моделирование обобщенной процедуры формирования индексов мягких решений // Инфокоммуникационные технологии. – 2013. – Т. 12, № 2. – С. 22–28.