УДК 621.3

С.Г. Рассомахин, Т.В. Лавровская

Харьковский национальный университет имени В.Н. Каразина, Харьков

АНАЛИЗ ПРИМЕНЕНИЯ ПРАВИЛА ПРОСТОГО ОКРУГЛЕНИЯ ДЛЯ ПОЛУЧЕНИЯ ВЫЧИСЛИТЕЛЬНО РЕАЛИЗУЕМЫХ МЕТОДОВ ДЕКОДИРОВАНИЯ

В статье рассмотрены основные проблемы практического использования методов случайного и псевдослучайного кодирования, представлен метод возможного решения проблемы, вычислительной реализуемости процесса декодирования псевдослучайных кодов на основе применения правила простого округления.

Ключевые слова: *правило простого округления, правило максимального правдоподобия, методы декодирования, отношение сигнал/шум, код Грея.*

Введение

Постановка проблемы. За последние годы прогресс в технике и микроэлектронике привел к бурному развитию беспроводных цифровых коммуникаций. Беспроводные сети передачи данных обеспечивают гибкость архитектуры, возможность динамического изменения топологии, высокую скорость передачи данных, быстроту проектирования и развертывания. Эти преимущества делают их важнейшим направлением развития цифровых коммуникаций. Немаловажным фактом остается эффективность этих технологий, которая в значительной степени определяется пропускной способностью канала связи, а также удельной частотной и энергетической эффективностью систем передачи информации, использующих помехоустойчивые коды. Несмотря на огромные достижения, полученные в последние годы в области сетевых технологий, рациональное использование физического ресурса каналов передачи остается по-прежнему не решенным. Причиной этого является тот факт, что при существующих методах кодирования и построения физических переносчиков данных (сигналов) повышение скорости информационного обмена в стремлении приблизиться к пропускной способности каналов, как правило, достигается за счет расширения требуемой полосы частот или увеличения мощности передатчиков [1].

Цель работы: разработка простого метода построения и декодирования псевдослучайных кодов на основе правил, мало уступающих по объективности правилу максимального правдоподобия и обладающих вычислительной сложностью, не выше полиномиальной.

1. Постановка задачи

Существенной преградой для практического использования методов случайного и псевдослучайного кодирования является то, что декодирование таких кодов основывается на реализации правила максимального правдоподобия и возможно лишь с использованием переборных алгоритмов.

Стоит отметить, что вычислительная сложность таких алгоритмов возрастает экспоненциально с длиной блока кода и при практически требуемых значениях длины блока является неприемлемой. Поэтому актуальными для дальнейших исследований являются методы построения и декодирования псевдослучайных кодов на основе правил, мало уступающих по объективности правилу максимального правдоподобия и обладающих вычислительной сложностью, не выше полиномиальной.

Основной задачей данной работы является разработка простых методов построения и декодирования линейных помехоустойчивых кодов на основе использования псевдослучайных порождающих матриц. Кроме того, в статье описан упрощенный алгоритм декодирования с помощью правила простого округления (ППО), а так же приведены результаты статистических испытаний этой модели.

2. Аналитическая модель псевдослучайного помехоустойчивого кода

Поскольку линейные блоковые коды характеризуются простыми алгоритмами реализации и, в то же время обладают достаточно мощными корректирующими свойствами, то они, несомненно, являются перспективным направлением при разработке простых вычислительно реализуемых методов декодирования. Линейные коды в контексте данной работы выступают, как множество точек многомерных пространств, порождаемых системой координат, образуемой строками некоторой матрицы G. Матрица G является порождающей и генерируется с помощью алгоритма получения псевдослучайных чисел, равномерно распределённых относительно нуля в диапазоне $(-M, M)$ [2]. Границы диапазона чисел выбираются на основе допустимого энергетического бюджета канала. Строки матрицы G линей-

но независимы, матрица является квадратной с размером, равным длине блока N.

Кодовые слова псевдослучайного помехоустойчивого кода получаются для исходных сообщений источника $X_j^k = \left\{x^j{}_1, x^j{}_2 \ldots x^j{}_k\right\}$ с числовым эквивалентом из диапазона $\left(0,\ldots,2^k-1\right)$, где k – длина блока двоичных символов. Алгоритм получения кодовых слов на основании матрицы G зависит от соотношения параметров k и N, и, фактически, рассматривается в трех случаях:

1. $k < N$.

В данном случае получение j-го кодового слова реализуется простым векторным умножением:

$$K_j = Y_j \cdot G, \qquad (1)$$

$$Y_j = X^k{}_j \left| X^r{}_j = \left\{ x^j{}_1, x^j{}_2 \ldots x^j{}_k, \underbrace{x^j{}_{k+1}, \ldots, x^j{}_{k+r}}_{\text{избыточные символы}} \right\}, \right.$$

$$r = N - k.$$

2. $k=N$.

При данном условии не требуется проведение никаких дополнительных операций, алгоритм (1) реализуется при $Y^N{}_j = X^N{}_j$.

3. $k>N$.

Для реализации векторного умножения (1) необходимо выровнять размер вектора Y_j и матрицы G. Это может быть выполнено путем разбиения блока X_j^k на N субблоков, в каждом из которых содержится k/N бит (рис. 1). Каждая комбинация информационных символов субблока определяется, как соответствующее число в системе счисления $Q : Y_j^N = \left\{y_1^N, \ldots, y_N^N\right\}$, где $y_i^N \in \left[0, Q-1\right]$. Тогда операция кодирования будет иметь вид:

$$K_j = \left(Y_j^N - \frac{2^{k/N}-1}{2} \right) \cdot G. \qquad (2)$$

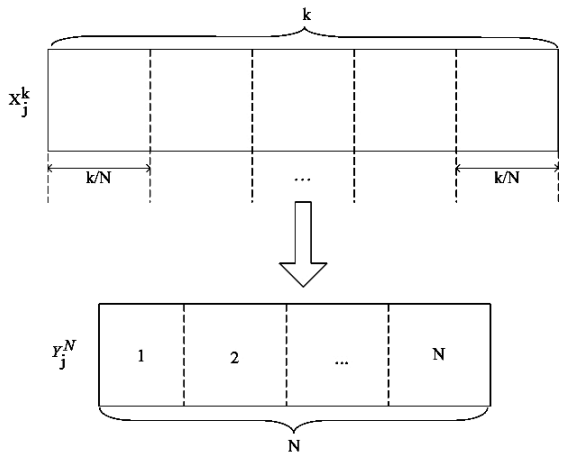

Рис. 1. Преобразование X_j^k в Y_j^N

Разность, вычисляемая в скобках (2) означает центрирование Q-ичных чисел относительно нуля. Данная операция минимизирует энергетические затраты на передачу в случае использования амплитудного представления кодовых символов.

Из рассмотренных выше случаев построения кодовых слов, первый случай в работе рассматриваться не будет, так как соответствует обычному блоковому кодированию с избыточностью, при котором неизбежны потери удельной скорости при передаче информации.

В соответствии с законом больших чисел при достаточно большой размерности пространства кода N точки кодовой книги N-символьного кода распределяются асимптотически равномерно.

В соответствии с законом больших чисел при достаточно большой размерности пространства кода N точки кодовой книги N-символьного кода распределяются асимптотически равномерно.

Для осуществления корректного анализа свойства помехоустойчивости псевдослучайного кода (ПСК) необходимо ограничение на бюджет мощности передатчика (модулятора). Пусть величина данного ограничения, приведенного к одному биту, составляет P_b. Тогда для передачи по каналу одного из N символов кода величина бюджета мощности должна составлять $(k/N)\cdot P_b$. Если предположить использование амплитудной модуляции для канального кодирования одного символа кода, то можно определить величину диапазона распределения псевдослучайных чисел $(-M,+M)$ из условия $P_C = (k/N)\cdot P_b$. При равномерном распределении чисел внутри $(-M,+M)$ средняя мощность (дисперсия) равна:

$$M = \frac{1}{2}\sqrt{\frac{12k}{N}P_b}. \qquad (3)$$

При соблюдении условия (3) генерации канальных символов амплитудного кода отношение сигнал/шум в гауссовом канале, приведенное к одному информационному биту, будет составлять $P_b/(n0/2)$, где $n0$ – спектральная плотность аддитивного белого гауссова шума (АБГШ).

Известно [3], что при превышении отношением сигнал/шум некоторого порогового значения, применение ПСК обеспечивает монотонное (с увеличением N) уменьшение вероятности декодирования с ошибкой p_0:

$$\lim_{N\to\infty} p_o = 0. \qquad (4)$$

Поскольку закон больших чисел начинает эффективно проявляться при очень больших N, то методы переборного декодирования на основе правила максимального правдоподобия [3, 4] становят-

ся вычислительно не реализуемыми. Поэтому в данной статье предлагается рассмотрение упрощенного метода декодирования с использованием векторного умножения принятых кодовых слов на проверочную матрицу, которая является обратной к порождающей матрице:

$$H = G^{-1} \quad (5)$$

Тогда операция декодирования имеет следующий вид:

$$Y^* = K^* \cdot H + \frac{2^{k/N} - 1}{2}, \quad (6)$$

где $K^* = K + \xi$, $\xi = \{\xi_1, \ldots, \xi_N\}$ – вектор, порождаемый АБГШ в гауссовом канале. Значения компонент вектора K^* могут быть, в принципе, произвольными действительными числами. Однако, по определению рассматриваемого кода эти числа должны удовлетворять двум требованиям: во-первых, они должны располагаться в диапазоне $[0, Q-1] = \left[0, 2^{k/N} - 1\right]$, а, во-вторых – должны быть целыми. Таким образом процесс декодирования по рассматриваемому алгоритму, который можно назвать правилом простого округления (ППО), сводится к вычислению (6) и реализации указанных требований.

Естественно, следует ожидать определенных потерь в объективности правила ППО по сравнению с ПМП, а, значит, и снижения помехоустойчивости. Однако данная жертва может оказаться оправданной, если в актуальном диапазоне отношений сигнал/шум будет обеспечено выполнение (4).

3. Математическая модель построения и декодирования ПСК

Математическая модель построена на основе формул описывающих кодирование (2) и декодирование (6) для соотношений k и N, соответствующих случаям 2) и 3), рассмотренным выше. Основной целью модели является экспериментальное определение вероятности декодирования с ошибкой при различных длинах блока кода N и исходного блока двоичных символов k. Математическая модель реализована с помощью пакета Mathcad 14. Кодирование (2) осуществляется на основе порождающей матрицы G, которая генерируется с помощью встроенного генератора псевдослучайных чисел, центрированных относительно нуля:

$$G = \mathrm{rnd}\left(2\sqrt{3}\right) - \sqrt{3}, \quad (7)$$

где $\mathrm{rnd}(z)$ – функция генерации случайного числа, распределенного равномерно в диапазоне $[0, z]$. Поскольку математическая модель использует ППО, то нет необходимости хранить весь массив значений кодовой книги, достаточно, при необходимости, генерировать кодовое слово. Тем самым повышая вычислительную мощность и выполняя условие (4):

$$K = \left\{ G \cdot \left(c(x) - \left(\frac{Q-1}{2} \right) \right) \right\} \sqrt{\frac{12 \cdot k}{N \cdot (2^k - 1)}}. \quad (8)$$

Здесь $c(x)$ – числовой эквивалент субблока, представленный в Q-ичной системе счисления.

Для воспроизведения условий гауссова канала в модели генерируется N-элементный вектор помехи (функция rnorm), порождаемый АБГШ со средней мощностью $(n0/2)$ и нулевым средним:

$$\mathrm{Nois} = \mathrm{rnorm}\left(N, 0, \sqrt{\frac{n0}{2}}\right) \quad (9)$$

Взаимодействие двух векторов является аддитивным:

$$KN = K + Nnois. \quad (10)$$

Таким образом, на выходе канала декодеру доступна оценка кодового слова KN. Для декодирования используется проверочная матрица:

$$H = G^{-1}. \quad (11)$$

Тогда, исходя, из выражения (6), результатом декодирования является оценка переданного сообщения источника:

$$X^* = \mathrm{round}\left[\left(\frac{KN}{\sqrt{\frac{12 \cdot k}{N \cdot \left(2^k - 1\right)}}} \cdot H \right) + \frac{Q-1}{2} \right]. \quad (12)$$

где round – операция целочисленного округления. Для коррекции данной оценки необходима проверка попадания величины X^* в допустимый диапазон Q-ичной системы счисления:

$$X^{**} = \begin{cases} X^*, & \text{если } 0 \le X^* \le Q\text{-}1; \\ Q\text{-}1 & \text{если } X^* \ge Q\text{-}1; \\ 0 & \text{если } X^* < 0. \end{cases} \quad (13)$$

Перевод оценки X^{**} из Q-ичной системы счисления в двоичную дает оценку содержания исходного битового сообщения. Вычисление количества искаженных бит осуществляется побитовой операцией исключающее или XOR, полученной оценки X^{**} и исходного X_j^k:

$$V = X^{**} \oplus X_j^k. \quad (14)$$

Завершающим этапом после проведения достаточного числа вычислительных экспериментов является расчет частости (вероятности) декодирования с ошибкой p_0, приведенной к одному биту.

4. Результаты моделирования ПСК

На рис. 2 и 3 представлены результаты статистических исследований описанной выше модели, кривые на графиках изображают зависимость веро-

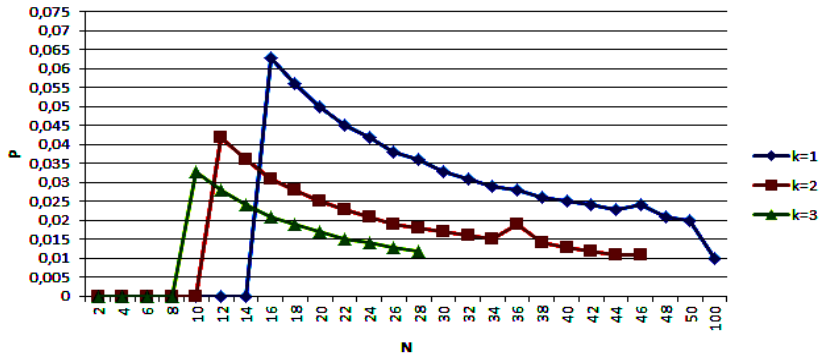

Рис. 2. Зависимость изменения вероятности ошибок при декодировании при SNR=8 и разных k

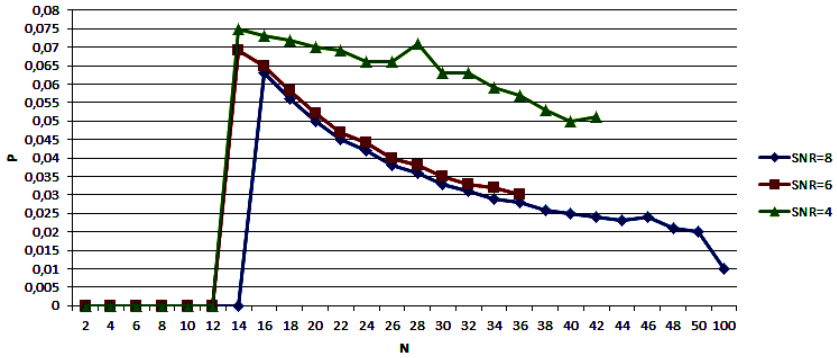

Рис. 3. Зависимость изменения вероятности появления ошибок при декодировании при k=1 и при разном SNR

ятности декодирования с ошибкой при различных длинах блоков двоичных символов k и длине блока сообщения N. Также рассматривалось влияние различных значений соотношения сигнал/шум $SNR = 2, 4, 6$. Несмотря на выбросы, которые присутствуют на графиках, выявлено подтверждение гипотезы (4) о монотонном снижении ошибки с ростом длины блока.

Выводы

Полученные результаты подтверждают истинность гипотезы (4), что означает возможность использования аппарата псевдослучайных порождающих и проверочных матриц для реализации быстрых алгоритмов построения и декодирования ПСК. Правило простого округления при числовом декодировании (6), хотя и приводит к некоторому снижению помехоустойчивости, однако, ввиду возможности компенсации потерь дополнительным увеличением длины блока кода, а также из-за низкой вычислительной сложности является весьма перспективным направлением совершенствования систем передачи данных. Направлением дальнейших исследований может быть модификация рассмотренного алгоритма кодирования при использовании рефлексивного бинарного кода Грея, а также применение методов дополнительной коррекции случайно генерируемых порождающих матриц.

Список литературы

1. Григорьев В.А. Сети и системы радиодоступа [Текст] / В.А. Григорьев, О.И Лагутенко, Ю.А. Распаев. – М.: Эко-Трендз, 2005. – 384 с.

2. Гихман И.И. Теория вероятностей и математическая статистика [Текст] / И.И. Гихман, А.В. Скороход, Н.И. Ядренко. – К.: Высшая шк., 1982. – 439 с.

3. Скляр Б. Цифровая связь. Теоретические основы и практическое применение [Текст] / Б. Скляр; изд. 2-е, испр.; пер. с англ. – М. : Изд. дом "Вильяме", 2003. – 378 с.

4. Рассомахин С.Г. Технология псевдослучайного кодирования в сетевых коммуникационных протоколах канального уровня / С.Г. Рассомахин // Системи обробки інформації. – Х.: ХУПС, 2012. – Вип. 3 (101), т. 2. – С. 206-211.

Поступила в редколлегию 18.02.2015

Рецензент: д-р техн. наук, проф. Г.А. Кучук, Харьковский университет Воздушных Сил им. И. Кожедуба, Харьков.

АНАЛІЗ ЗАСТОСУВАННЯ ПРАВИЛА ПРОСТОГО ОКРУГЛЕННЯ ДЛЯ ОТРИМАННЯ ОБЧИСЛЮВАЛЬНО РЕАЛІЗОВАНИХ МЕТОДІВ ДЕКОДУВАННЯ

С.Г. Рассомахін, Т.В. Лавровська

У статті розглянуто основні проблеми практичного використання методів випадкового і псевдовипадкового кодування, представлений метод можливого вирішення проблеми обчислювальної реалізованості процесу декодування псевдовипадкових кодів на основі застосування правила простого округлення.

Ключові слова: *правило простого округлення, правило максимальної правдоподібності, методи декодування, відношення сигнал / шум, код Грея.*

ANALYSIS OF THE APPLICATION OF SIMPLE RULES FOR ROUNDING COMPUTATIONALLY IMPLEMENTED DECODING METHODS

S.G. Rassomakhin, T.V. Lavrovska

In the article discussed the main problems of practical use the methods of random and pseudo-random coding, presented method of possible solution to the problem of computing the feasibility of the decoding process pseudorandom codes on based the rule of simple rounding.

Keywords: *the rule of simple rounding, rule maximum likelihood, decoding methods, signal / noise ratio, Gray code.*