Информационные процессы, Том 14, № 2, 2014, стр. 151–159.

ПЕРЕДАЧА ИНФОРМАЦИИ В КОМПЬЮТЕРНЫХ СЕТЯХ

Метод кодирования для Q-частотного гауссовского канала с S пользователями[1]

А.А. Фролов, В.В. Зяблов

Институт проблем передачи информации, Российская академия наук, Москва, Россия

Поступила в редколлегию 16.06.2014

Аннотация—В работе рассматривается проблема построения системы асинхронного множественного доступа для многопользовательского Q-частотного канала с аддитивным белым гауссовским шумом (АБГШ). Для решения этой задачи предложена схема кодирования. Основным компонентом данной схемы является недвоичный код с малой плотностью проверок (МПП-код). Для увеличения скорости передачи в систему добавлена вложенная модуляция. Эффективность результирующей системы множественного доступа показана с помощью имитационного моделирования.

КЛЮЧЕВЫЕ СЛОВА: множественный доступ, асинхронный, недвоичный МПП-код, вложенная модуляция.

1. ВВЕДЕНИЕ

В работе рассматривается проблема построения системы множественного доступа для Q-частотного гауссовского канала с S пользователями. Нас интересует асинхронный множественный доступ (терминология из работ [1, 2]), т.е. вид множественного доступа, при котором отдельные пользователи могут иметь доступ к системе независимо от других пользователей и без системной координации. Этот факт позволяет нам рассматривать других пользователей как шум (однопользовательский прием).

В данной работе предложен метод кодирования для данного канала. Этот медод основан на идеях из [2], в то же самое время этот метод является обобщением наших предыдущих работ [3–5]. В этих работах рассматривался идеализированный векторный дизъюнктивный канал (канал ИЛИ). Предполагалось, что канал является бесшумным, т.е. единственное препятствие правильной передаче информации в системе – это активность других пользователей. В этой работе мы используем комплексные сигналы и также добавляем аддитивный шум. Таким образом, эта модель канала гораздо точнее отражает реальное положение вещей.

Главными компонентами нашей схемы кодирования являются коды Каутса–Синглтона [6] и недвоичные МПП-коды [7,8]. Для увеличения скорости передачи в систему добавлена вложенная модуляция. Эффективность результирующей системы множественного доступа показана с помощью имитационного моделирования. Отметим также, что предложенная система проста в реализации и поэтому подходит для практического применения.

2. ПРЕДВАРИТЕЛЬНЫЕ СВЕДЕНИЯ

2.1. Модель канала

Обозначим число активных пользователей через S, $S \geq 2$. Входами канала в некоторый момент времени τ являются комплексные векторы $\mathbf{x}_i = (x_{(i,1)}, x_{(i,2)}, \ldots, x_{(i,Q)}) \in \mathbb{C}^Q, i = 1, \ldots, S,$

[1] Работа выполнена при частичной поддержке Российского фонда фундаментальных исследований (проекты 13-01-12458 и 14-07-31197).

длины Q (число частот или подканалов), а выход канала в момент времени τ – это вектор $\mathbf{y} = (y_1, y_2, \ldots, y_Q) \in \mathbb{C}^Q$,

$$y_j = \sum_{i=1}^{S} x_{(i,j)} + \xi_j, \quad j = 1, \ldots, Q,$$

где $\xi_j = N(0, 2\sigma^2)$ – двумерный (комплексный) аддитивный белый гауссовский шум (АБГШ) с нулевым средним и дисперсией σ^2 по каждой размерности.

2.2. Коды Каутса–Синглтона

Код Каутса–Синглтона (КС-код) – это каскадный код с внешним $[n, k]$-кодом над полем $\mathbb{F}_q$ и следующим внутренним кодом. Занумеруем элементы поля $\mathbb{F}_q$ следующим образом

$$\mathbb{F}_q = \{\, \alpha_1, \alpha_2, \ldots, \alpha_q \,\}.$$

Внутренний код ставит в соответствие каждому элементу поля $\alpha_i \in \mathbb{F}_q$ двоичный вектор длины q с одной единицей в i-ой позиции. Позиции в векторе пронумерованы числами от 1 до q.

Пример 1. Пусть $\mathbf{c} = \left[\, \alpha_2, \alpha_4, \alpha_6, \alpha_1, \alpha_2, \alpha_5 \,\right]$ – это слово кода Рида–Соломона $\mathcal{RS}(6, 2)$ над полем $\mathbb{F}_7$. Слову $\mathbf{c}$ соответствует такое слово $\mathbf{C}$ КС-кода

$$\mathbf{C} = \begin{bmatrix} 0 & 0 & 0 & 1 & 0 & 0 \\ 1 & 0 & 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 1 \\ 0 & 0 & 1 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 \end{bmatrix}.$$

2.3. Ранги

Положим, дана матрица $\mathbf{A}$ размера $m \times n$ над действительным полем. Матрица рангов $\mathbf{A}^{(\mathrm{R})}$ находится следующим образом

$$\mathbf{A}^{(\mathrm{R})}(i, j) = \left|\{\mathbf{A}(k, l) : \mathbf{A}(k, l) < \mathbf{A}(i, j)\}\right|, \quad 1 \le k \le m, 1 \le l \le n.$$

Обозначим операцию вычисления рангов так

$$\mathbf{A}^{(\mathrm{R})} = \mathrm{ranks}\,(\mathbf{A}).$$

Пример 2. Пусть

$$\mathbf{A} = \begin{bmatrix} 0.5 & 0.4 & 0.7 \\ 0.1 & 0.3 & 0.2 \end{bmatrix},$$

тогда

$$\mathbf{A}^{(\mathrm{R})} = \begin{bmatrix} 4 & 3 & 5 \\ 0 & 2 & 1 \end{bmatrix}.$$

3. ПЕРЕДАЧА

Для простоты мы рассмотрим сценарий, в котором все пользователи передают информацию базовой станции (канал “вверх” или uplink).

Мы предполагаем, что все пользователи используют один и тот же алфавит – символы поля $\mathbb{F}_q$, $q < Q$. Мы также предполагаем наличие символьной синхронизации и отсутствие блочной синхронизации. Рассмотрим процесс передачи сообщения i-м пользователем.

3.1. Каскадный код

Обозначим через $\mathcal{C}_{\mathrm{O}}$ внешний $[N, K = RN]$ МПП-код над полем $\mathbb{F}_q$. Обозначим через $\mathcal{C}_{\mathrm{I}}$ внутренний $[n, 1]$-код над тем же полем. В этой работе, дабы упростить описание, мы будем использовать код с повторением над полем $\mathbb{F}_q$ в качестве внутреннего кода. Обобщение на случай другого внутреннего кода не представляет проблем.

На первой стадии мы кодируем K информационных символов поля $\mathbb{F}_q$ ($K \log_2 q$ бит) с помощью каскадного кода $\mathcal{C}_{\mathrm{O}} \diamond \mathcal{C}_{\mathrm{I}}$ и получаем слово $\mathbf{c} \in \mathcal{C}_{\mathrm{O}} \diamond \mathcal{C}_{\mathrm{I}}$ длины Nn (в символах поля $\mathbb{F}_q$).

3.2. КС-код

На второй стадии мы кодируем слово $\mathbf{c} \in \mathcal{C}_{\mathrm{O}} \diamond \mathcal{C}_{\mathrm{I}}$ КС-кодом и получаем матрицу $\mathbf{C}$ размера $q \times Nn$.

3.3. Вложенная модуляция

Рассмотрим фазовую манипуляцию[1] (ФМн) порядка M (M-ФМн). Обозначим через $\mathcal{C}_{\mathrm{E}}$ двоичный $[N_{\mathrm{E}} = Nn \log_2 M, K_{\mathrm{E}} = R_{\mathrm{E}} N_{\mathrm{E}}]$ МПП-код. На третьей стадии мы кодируем K_{E} информационных бит кодом $\mathcal{C}_{\mathrm{E}}$ и получаем кодовое слово $\mathbf{c}_{\mathrm{E}} \in \mathcal{C}_{\mathrm{E}}$ длины $Nn \log_2 M$. Далее мы модулируем $\mathbf{c}_{\mathrm{E}}$ при помощи модулятора M-ФМн и получаем последовательность комплексных величин $\mathbf{t}$ длины Nn. Затем мы ставим элементы $\mathbf{t}$ на позиции матрицы $\mathbf{C}$, где стояли единицы. Таким образом, получается матрица $\mathbf{C_t}$ с комплексными значениями.

Пример 3. Добавим вложенную модуляцию (8-ФМн) к матрице $\mathbf{C}$ из Примера 1. Получим, например, такую матрицу

$$\mathbf{C_t} = \begin{bmatrix} 0 & 0 & 0 & 1 & 0 & 0 \\ 1 & 0 & 0 & 0 & -1 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & \frac{1}{\sqrt{(2)}}(1+i) & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & -i \\ 0 & 0 & i & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 \end{bmatrix}.$$

3.4. Перестановка

На последней стадии формируется матрица $\mathbf{T}$

$$\mathbf{T} = \begin{bmatrix} \mathbf{C_t} \\ \mathbf{0} \end{bmatrix}_{Q \times Nn}.$$

Передача происходит последовательно вектор за вектором. Перед передачей каждого вектора в канал выполняется перестановка его элементов (новая перестановка при передаче каждого вектора). Далее мы предполагаем, что перестановки выбираются случайно и равновероятно из множества всех возможных $Q!$ перестановок.

Замечание 1. Заметим, что добавление вложенной модуляции существенно увеличивает скорость передачи (в переданных битах за одно использование канала). Без вложенной модуляции скорость передачи для одного пользователя равна $R \log_2 q$, с использованием вложенной модуляции – $R \log_2 q + R_{\mathrm{E}} \log_2 M$.

[1] англ. phase-shift keying, PSK

4. ПРИЕМ

На базовой станции каждому пользователю соответствует отдельный приемник. При приеме сообщения от пользователя другие пользователи рассматриваются как шум (однопользовательский прием). Рассмотрим процесс приема сообщения, пришедшего от i-го пользователя. Мы предполагаем, что приемники базовой станции синхронизированы с передатчиками пользователей. Это означает, что позиции Nn столбцов, соответствующих кодовому слову, переданному i-м пользователем, известны на приемнике. Кроме того известны и использовавшиеся перестановки. При приеме каждого из столбцов выполняется обратная перестановка. Таким образом, мы получаем матрицу $\mathbf{R}$ размера $Q \times Nn$. Мы берем только q первых строк матрицы $\mathbf{R}$ и формируем матрицу $\mathbf{Y}$ размера $q \times Nn$, "содержащую" переданную i-м пользователем матрицу $\mathbf{C_t}$.

4.1. Внутренний код

Нам необходимо декодировать N внутренних кодов $\mathcal{C}_\mathrm{I}$. Без ограничения общности рассмотрим лишь декодирование первого внутреннего кода. Пусть матрица $\mathbf{Y}_1$ размера $q \times n$ состоит из первых n столбцов матрицы $\mathbf{Y}$. Нам потребуются еще две матрицы. Пусть $\mathbf{Y}_1^{(A)}$ – это матрица абсолютных величин элементов $\mathbf{Y}_1$, т.е.

$$\mathbf{Y}_1^{(A)}(i,j) = \left|\mathbf{Y}_1(i,j)\right|, \quad 1 \le i \le q, 1 \le j \le n.$$

Пусть

$$\mathbf{Y}_1^{(R)} = \mathrm{ranks}\left(\mathbf{Y}_1^{(A)}\right).$$

Декодирование внутреннего кода выполняется исчерпывающим поиском (см. Алгоритм 1). Рассмотрим два метода декодирования внутреннего кода:

- В первом случае на вход Алгоритма 1 подается матрица $\mathbf{Y}_1^{(A)}$ (сумма модулей, sum-abs);
- Во втором случае на вход Алгоритма 1 подается матрица $\mathbf{Y}_1^{(R)}$ (сумма рангов, sum-ranks).

Замечание 2. Отметим, что декодирование по сумме рангов также использовалось в [9] для немного отличного сценария.

Алгоритм 1. Декодирование внутреннего кода

Вход: матрица $\mathbf{A}$, длина внутреннего кода n
Выход: вектор $\mathbf{r}$, содержащий величины надежности по каждому кодовому слову $\mathcal{C}_\mathrm{I}$
for all $1 \le i \le |\mathcal{C}_\mathrm{I}|$ **do**
  Построить $c_i \in \mathcal{C}_\mathrm{I}$
  Построить слово $\mathbf{C}$ КС-кода по данному c_i
  $\omega \leftarrow \sum_{i,j:\mathbf{C}(i,j)=1} \mathbf{A}(i,j)$
  $\mathbf{r}(i) = \omega/n$
end for

4.2. Внешний код

Рассмотрим два алгоритма декодирования внешнего недвоичного МПП-кода: мажоритарный алгоритм декодирования с жестким решением [10] и алгоритм Сумма-Произведение (Sum-Product, SP) с мягким решением [8]. Абсолютно ясно, как применить мажоритарный алгоритм. Нужно просто принять жесткое решение по каждому из внутренних кодов и подать полученное слово на вход мажоритарного алгоритма.

Чтобы понять, как применить алгоритм Сумма-Произведение, кратко опишем входные и выходные данные этого алгоритма. Для более детального описания см. [8, 11–13]. Предположим, в канал было послано слово $\mathbf{x} = (x_1, x_2, \ldots, x_N) \in \mathbb{F}_q^N$ и получено слово $\mathbf{y} = (y_1, y_2, \ldots, y_N)$. Введем понятие вектора априорных логарифмических распределений.

$$\mathbf{l} = (\mathbf{l}_1, \mathbf{l}_2, \ldots, \mathbf{l}_N),$$

где

$$\begin{aligned}\mathbf{l}_i =&(\ln \Pr(x_i = \alpha_1|y_i),\\ &\ln \Pr(x_i = \alpha_2|y_i),\\ &\ldots,\\ &\ln \Pr(x_i = \alpha_q|y_i)), \quad 1 \le i \le N.\end{aligned}$$

После того, как декодирование закончено, мы получаем вектор апостериорных логарифмических распределений. Чтобы применить алгоритм Сумма-Произведение, мы устанавливаем $\mathbf{l}_i = \mathbf{r}_i, \quad 1 \le i \le N$, где $\mathbf{r}_i$ – это вектор, содержащий надежности по каждому кодовому слову i-го внутреннего кода (см. предыдущий параграф). Здесь мы использовали тот факт, что внутренние коды – это коды с повторением. Из-за этого мы напрямую получили распределения по каждому из символов внешнего кода.

4.3. Вложенная модуляция

После декодирования каскадного кода мы знаем (если декодирование прошло успешно) Nn позиций, где передавалось слово двоичного МПП-кода, модулированное M-ФМн. Из значений матрицы $\mathbf{Y}$ на этих позициях мы формируем последовательность $\mathbf{r}_E$ длины Nn. Элементы $\mathbf{r}_E$ искажены аддитивным шумом и интерференцией от других пользователей.

Под коллизией мы понимаем событие, когда $m > 1$ пользователей передавали в одной позиции. Коллизия имеет кратность m, если в точности m пользователей передавали в одной позиции. Легко проверить, что вероятность коллизии в конкретной позиции можно вычислить так

$$p_c = 1 - \left(1 - \frac{1}{Q}\right)^{S-1},$$

а среднее число позиций $\mathbf{r}_E$, искаженных из-за коллизий, $P = Nnp_c$.

Чтобы уменьшить число ошибок, возникающих из-за коллизий, мы вводим порог (ε_{th}). Мы стираем (это означает, что мы подаем нули на декодер (SP) двоичного МПП-кода для бит, соответствующих стертым позициям) символы $\mathbf{r}_E$, если их абсолютное значение больше либо равно ε_{th}. Мы выбираем ε_{th} так

$$\varepsilon_{th} = \arg\min_t \left\{(1 - p_c)\Pr(\text{er}|\text{no col., t}) + p_c \Pr(\text{er}|\text{col., t})\right\}.$$

После того, как множество стертых символов определено, мы демодулируем оставшиеся символы и подаем получившиеся логарифмические отношения правдоподобия на вход декодера двоичного МПП-кода.

Блок-схема всей системы приведена на Рис. 1.

5. ЧИСЛЕННЫЕ РЕЗУЛЬТАТЫ

В этой секции представлены полученные численные результаты. Приведем все параметры здесь. Пусть $Q = 1024$.

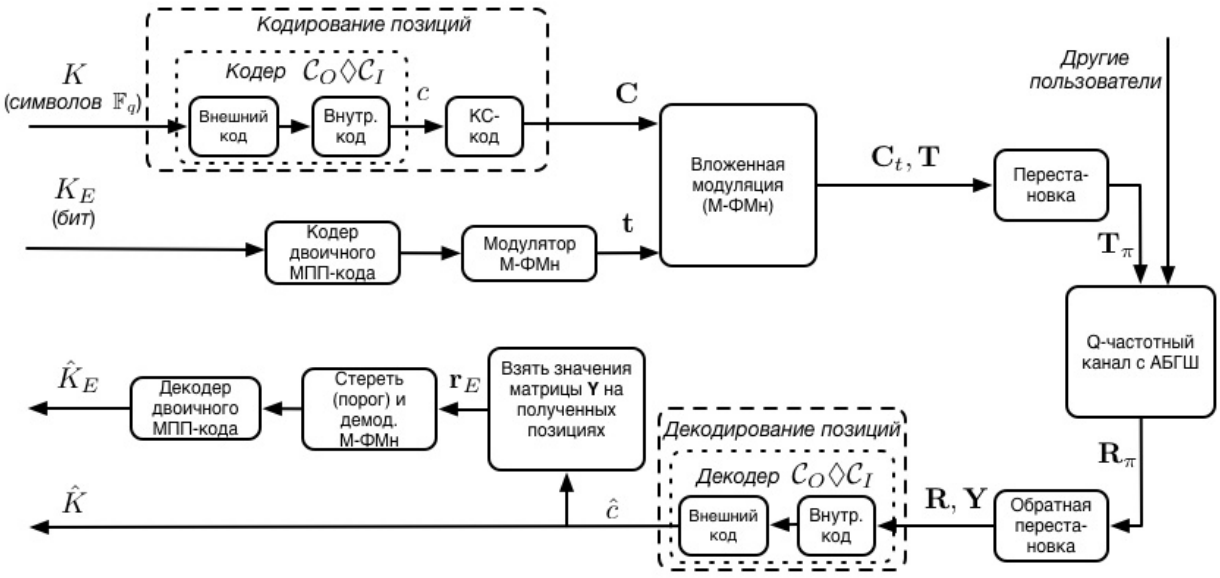

Рис. 1. Блок схема

Параметры кодов. Выберем код с повторением длины $n = 6$ над полем $\mathbb{F}_8$ в качестве внутреннего кода, $[510, 260]$ МПП-код над полем $\mathbb{F}_8$ в качестве внешнего кода (код выбран регулярным, а его матрица построена с помощью алгоритма из [14] (англ. progressive egde growth (PEG) algorithm). Для мажоритарного алгоритма число единиц в столбцах проверочной матрицы выбрано равным 6, для алгоритма Сумма-Произведение – 3. Для использования с вложенной модуляцией выберем двоичный $[9180, 4590]$ регулярный МПП-код с тремя единицами в столбце. В качестве вложенной модуляции выберем 8-ФМн, таким образом $M = 8$.

Модель мешающих пользователей. Из-за случайных перестановок мешающие пользователи ставят свои сигналы в столбцы передаваемой матрицы равновероятно (т.е. с вероятностью $1/Q$ в каждую из позиций столбца). Мы предполагаем наличие идеального контроля мощности. Сигналы мешающих пользователей – это комплексные числа с единичным модулем и фазой, равномерно распределенной на отрезке $[0, 2\pi]$.

Вычисление отношения сигнал/шум (SNR). Мы вычисляем отношение сигнал/шум так

$$SNR = -10\log_{10}(2\sigma^2 Q \log_2 q), \quad \text{внутренний и внешний коды}$$
$$SNR = -10\log_{10}(2\sigma^2 Q \log_2 M), \quad \text{вложенная модуляция}$$

5.1. Внутренний код

Результаты для алгоритмов декодирования sum-abs и sum-ranks приведены на Рис. 2. Число пользователей $S = 100$. Мы видим, что декодер sum-ranks лучше. Этот алгоритм также более надежен в случае отсутствия контроля мощности [9]. Далее мы будем использовать только этот алгоритм.

5.2. Внешний код

Результаты для внешнего кода показаны на Рис. 3. Сплошные линии соответствуют алгоритму Сумма-Произведением (SP), пунктирные – мажоритарному алгоритму. Мы видим, что система очень надежна, хорошие результаты получаются даже для $S = 200$. Также отметим, что алгоритм SP (даже с “нечестной” мягкой информацией) работает гораздо лучше

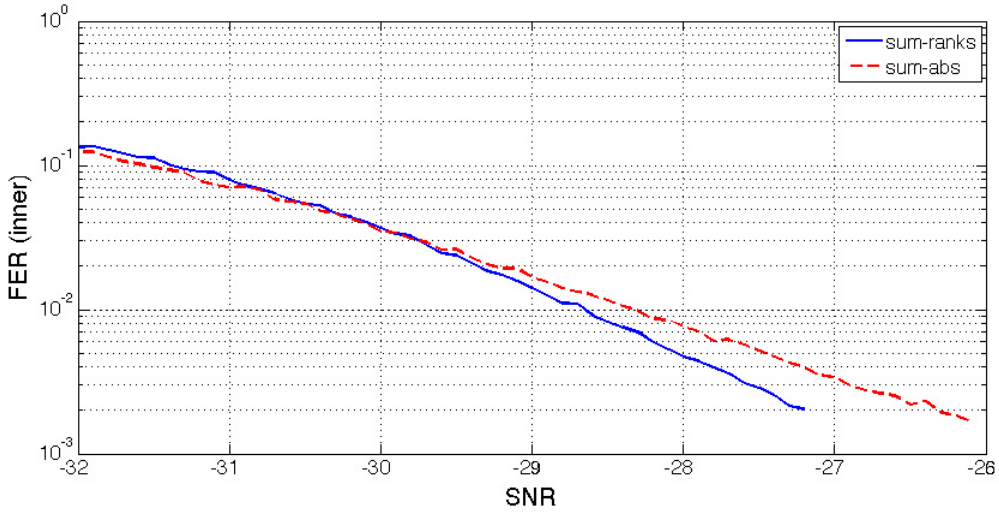

Рис. 2. Декодирование внутреннего кода, $S = 100$

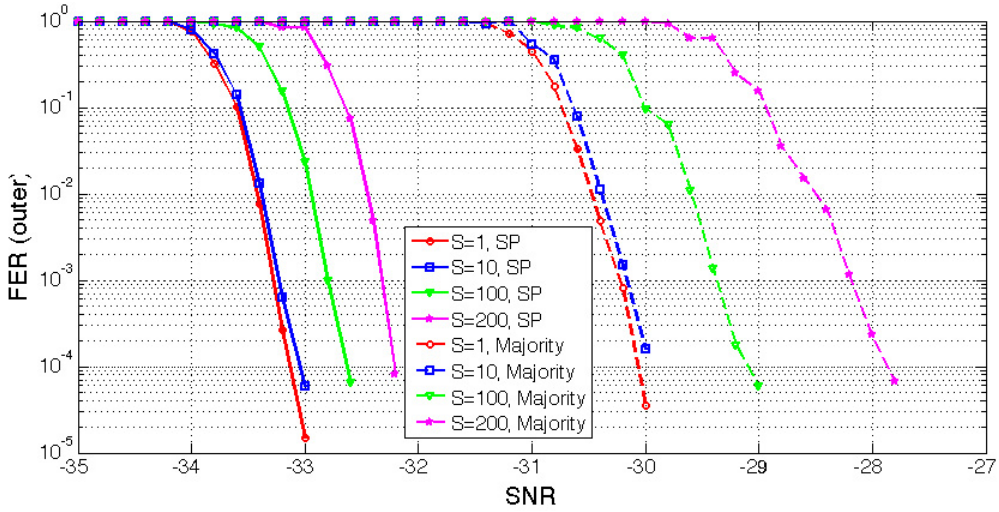

Рис. 3. Декодирование внешнего кода

мажоритарного алгоритма. Получен выигрыш порядка $3-4$ дБ. Далее мы используем только алгоритм SP.

5.3. Вложенная модуляция

И наконец, результаты для вложенной модуляции 8-ФМн показаны на Рис. 4. Мы видим, что результаты довольно хорошие даже для $S = 100$.

6. ЗАКЛЮЧЕНИЕ

Предложена схема кодирования для Q-частотного гауссовского канала с S пользователями. Основным компонентом данной схемы являются коды Каутса–Синглтона и недвоичные МПП-коды. Для увеличения скорости передачи в систему добавлена вложенная модуляция. Эффективность результирующей системы множественного доступа показана с помощью имитационного моделирования.

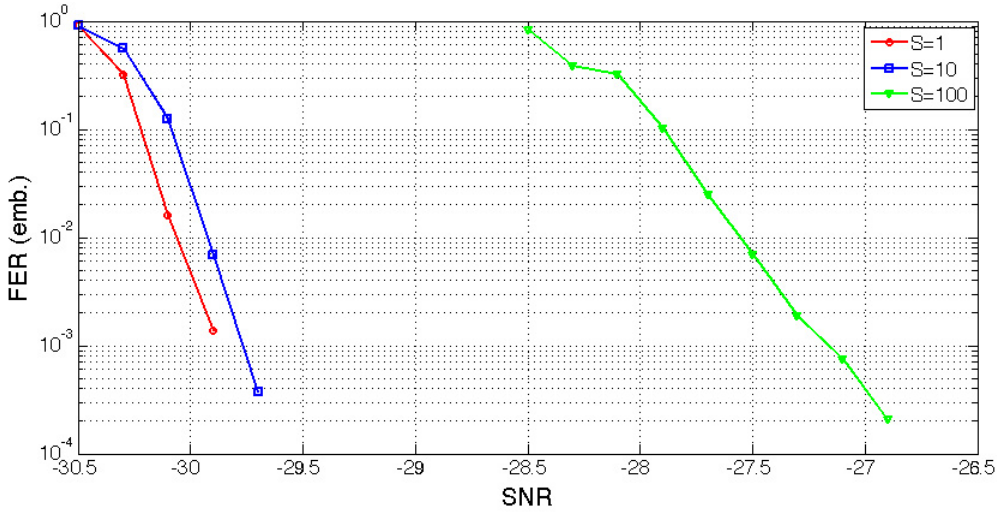

Рис. 4. Декодирование вложенной модуляции

СПИСОК ЛИТЕРАТУРЫ

1. Viterbi A. J. Very Low Rate Convolutional Codes for Maximum Theoretical Performance of Spread-Spectrum Multiple Access Channels. *IEEE J. Select. Areas Commun.*, vol. 8. no. 8. pp. 641–649, 1990.
2. Cohen A., Heller J., Viterbi A. J. A New Coding Technique for Asynchronous Multiple Access Communication. *IEEE Trans. Comm. Technology.*, vol. 19, no. 5. pp. 849–855, 1971.
3. Осипов Д.С., Фролов А.А., Зяблов В.В. Система множественного доступа для векторного дизъюнктивного канала. *Пробл. передачи информ.*, 2012. Т. 48. № 3. С. 52–59.
4. Sidorenko V. R., Fischer R. Low-Complexity List Decoding of Reed-Solomon Coded Pulse Position Modulation. In *9th Int. ITG Conference on Systems, Communication and Coding*, Jan. 21–24, 2013, Munich, Germany.
5. Frolov A. A., Zyablov V. V., Sidorenko V. R., Fischer R. On a Multiple-Access in a Vector Disjunctive Channel. In Proc. *IEEE Int. Symp. Inf. Theory*, Istanbul, Turkey, July 7–12, 2013. pp. 211–215.
6. Kautz W., Singleton R. Nonrandom Binary Superimposed Codes. *IEEE Trans. Inf. Theory*, pp. 363–377, 1964.
7. Gallager R. G. *Low-Density Parity-Check Codes.* Cambridge: MIT Press, 1963.
8. Davey M., MacKay D. J. C. Low Density Parity Check Codes over GF(q). *IEEE Commun. Lett.*, vol. 2 no. 6 pp. 165–167, 1998.
9. Kondrashov K. A., Afanassiev V. B. Ordered statistics decoding for semi-orthogonal linear block codes over random non-Gaussian channels. In Proc. *Thirteenth International Workshop on Algebraic and Combinatorial Coding Theory (ACCT)*, pp.192–196, 2012
10. Фролов А.А., Зяблов В.В. Асимптотическая оценка доли ошибок, исправляемых q-ичными МПП-кодами. *Пробл. передачи информ.*, 2010. Т. 46. № 2. С. 47–65.
11. Barnault L., Declercq D. Fast Decoding Algorithm for LDPC over GF(2q̂). In Proc. *Inf. Theory Workshop*, pp. 70–73, 2003.
12. Wymeersch H., Steendam H., Moeneclaey M. Log-Domain Decoding of LDPC Codes over GF(q). In Proc. *IEEE Intern. Conf. on Commun*, pp. 772–776, 2004.
13. Declercq D., Fossorier M. Decoding Algorithms for Nonbinary LDPC Codes Over GF(q). *IEEE Trans. Comm.*, vol. 55. no. 4 pp. 633–643, 2007.
14. Hu Xiao-Yu, Eleftheriou E. and Arnold D.-M. Regular and irregular progressive edge-growth tanner graphs. *IEEE Trans. Inf. Theory*, vol.51, no.1, pp. 386–398, Jan. 2005

A Coding Technique for Q-Frequency S-User Gaussian Channel

A.A. Frolov, V.V. Zyablov

The paper addresses the problem of constructing an asynchronous multiple access system for a multi-user Q-frequency channel with additive white gaussian noise (AWGN). To solve the problem we propose a coding scheme for the channel. The major component of the scheme is non-binary low-density parity-check (LDPC) code. To increase the transmission rate we introduce the embedded modulation. The efficiency of the resulting multiple-access system is shown by simulations.

KEYWORDS: multiple access, asynchronous, nonbinary LDPC code, embedded modulation.