Использование помех для защиты данных в радиоканале

В.П. Цветов[1]

[1]Самарский национальный исследовательский университет им. академика С.П. Королева, Московское шоссе 34А, Самара, Россия, 443086

Аннотация. В работе предложен вариант применения схемы квадратурной модуляции с ортогональным частотным разделением при мультиплексировании цифровых потоков, пригодный для защиты данных на основе симметричного шифрования в радиоканале с естественными или наведенными помехами. Метод защиты основан на чувствительности модели декодирования сигнала к вариациям измеряемых значений. Помехи, присутствующие в радиоканале, играют роль случайной части ключа блока аддитивного криптопреобразования. Схема не требует дополнительных вычислительных затрат и не влияет на пропускную способность радиоканала.

1. Введение

Перспективной технологией мультиплексирования цифровых потоков является ортогональное частотное разделение OFDM (Orthogonal frequency-division multiplexing), которое оперирует с большим количеством спектрально близких и дискретно модулированных ортогональных поднесущих [1-2]. В тех случаях, когда для модулирования поднесущих применяется квадратурная амплитудная модуляция QAM (Quadrature Amplitude Modulation), схема модуляции называется QAM OFDM [3-4]. Математическая модель формирования и декодирования QAM OFDM-сигнала рассмотрена, например, в [5] и сводится к решению следующей задачи.

Зададим конечное множество кодовых значений (символов)

$$Q_m^N = \left\{ Z = \left\langle z_0, z_1, .., z_{N-1} \right\rangle \mid z_k = x_k + I \cdot y_k \wedge (x_k, y_k) \in q_h^m \right\} \subset \square^N,$$

где $I^2 = -1$, и $q_m^h = \left\{ (h \cdot k_1, h \cdot k_2) \mid k_1, k_2 \in 0, .., 2 \cdot m - 1, m \in \square \right\}$.

Каждому кортежу $Z_N \in Q_m^N$ поставим в соответствие функцию $s(t) = \sum_{k=0}^{N-1} z_k \cdot e^{\frac{I 2\pi kt}{T}}$, определенную на замкнутом интервале $[0, T]$. Требуется определить $Z_N = \left\langle z_0, z_1, .., z_{N-1} \right\rangle$ по известной функции $s(t)$. Интервал $[0, T]$ называется интервалом длительности кода (символа) и, наряду со значениями m и N, определяет скорость передачи данных.

В предложенной постановке функция $s(t)$ моделирует передачу QAM OFDM-сигнала в идеальном радиоканале без помех с базовой пропускной способностью $C_B = \frac{2N(\log(m)+1)}{T}$ бит/с. Функции $e^{\frac{I 2\pi kt}{T}}$, при $k \in 0..N-1$, моделируют поднесущие сигнала.

Заметим, что для решения поставленной задачи достаточно знания значений функции $s(t_n)$ на конечном наборе временных отсчетов $t_n = \frac{T}{N} \cdot n$, где $n \in 0..N-1$. Действительно, обозначим $F_{NN} = \left(\varepsilon_N^{kn}\right) = \left(e^{\frac{I 2\pi kn}{N}} \right)$ - квадратная матрица порядка N, n - номер строки, k - номер столбца, $Z_N = \left\langle z_0, z_1, .., z_{N-1} \right\rangle$, $S_N = \left\langle s_0, s_1, .., s_{N-1} \right\rangle = \left\langle s(t_0), s(t_1), .., s(t_{N-1}) \right\rangle$. Тогда Z_N удовлетворяет системе линейных алгебраических уравнений (СЛАУ)

$$F_{NN} Z_N = S_N, \tag{1}$$

откуда $Z_N = \frac{1}{N} F_{NN}^* S_N$, где $F_{NN}^* = \left(\varepsilon_N^{-nk}\right) = \left(e^{\frac{-I 2\pi kn}{N}} \right)$ - эрмитово сопряженная матрица к матрице F_{NN}.

Здесь и далее, для простоты, матричные записи СЛАУ вида (1) будут обозначать записи вида

$$F_{NN} Z_N^T = S_N^T, \tag{2}$$

где верхний индекс обозначает операцию транспонирования.

Легко показать, что и в общем случае, при $M \geq N$, имеют место равенства

$$F_{MN} Z_N = S_N^M, \; Z_N = \frac{1}{M} F_{NM}^* S_N^M, \tag{3}$$

где $S_N^M = \left\langle s_0, s_1, .., s_{M-1} \right\rangle = \left\langle s(t_0), s(t_1), .., s(t_{M-1}) \right\rangle$, $t_n = \frac{T}{M} \cdot n$, $n \in 0..M-1$, $F_{MN} = \left(\varepsilon_M^{kn}\right) = \left(e^{\frac{I 2\pi kn}{M}} \right)$ и $F_{NM}^* = \left(\varepsilon_M^{-nk}\right) = \left(e^{\frac{-I 2\pi kn}{M}} \right)$ - прямоугольные матрицы размерностей $M \times N$ и $N \times M$, соответственно.

В качестве модели передачи QAM OFDM-сигнала в радиоканале с аддитивными помехами примем функцию $\tilde{s}(t) = s(t) + \delta s(t)$, где $\left\| \delta s(t) \right\|_{L^2(0,T)} < \delta$.

Если $\tilde{S}_N = S_N + \Delta S_N = \left\langle \tilde{s}_0, \tilde{s}_1, .., \tilde{s}_{N-1} \right\rangle$, $\Delta S_N = \left\langle \delta_0, \delta_1, .., \delta_{N-1} \right\rangle = \left\langle \delta(t_0), \delta(t_1), .., \delta(t_{N-1}) \right\rangle$, и $\tilde{Z}_N$ - решение СЛАУ

$$F_{NN} \tilde{Z}_N = \tilde{S}_N, \tag{4}$$

то

$$\frac{\left\| \Delta Z_N \right\|_N}{\left\| Z_N \right\|_N} \leq \mu\left(F_{NN}\right) \frac{\left\| \Delta S_N \right\|_N}{\left\| S_N \right\|_N}, \tag{5}$$

где $\left\| \Delta Z_N \right\|_N = \left\| Z_N - \tilde{Z}_N \right\|_N = \frac{1}{N} \cdot \left\| F_{NN}^* \Delta S_N \right\|_N$, $\mu\left(F_{NN}\right) = \frac{1}{N} \cdot \left\| F_{NN} \right\|_{NN} \cdot \left\| F_{NN}^* \right\|_{NN}$, $\left\| Z_N \right\|_N = \sqrt{\sum_{k=0}^{N-1} \left| z_k \right|^2}$, $\left\| F_{NN} \right\|_{NN} = \sup_{Z \in \mathbb{C}^N} \frac{\left\| F_{NN} Z_N \right\|_N}{\left\| Z_N \right\|_N}$.

Для обратимых матриц A_{NN} значение $\mu\left(A_{NN}\right) = \left\| A_{NN} \right\|_{NN} \cdot \left\| A_{NN}^{-1} \right\|_{NN}$ называется числом обусловленности матрицы A_{NN} (в евклидовой норме). Оно является мерой устойчивости решения СЛАУ $A_{NN} X_N = B_N$ относительно погрешности ее правой части. Чем больше значение $\mu\left(A_{NN}\right)$, тем более норма разности точного и возмущенного решения отличается от нормы погрешности.

В данном случае $\mu\left(F_{NN}\right)=1$ и, при согласовании величины h с соотношением сигнал-шум, для нахождения Z_N по значению $\tilde{Z}_N=\frac{1}{N}F_{NN}^{*}\tilde{S}_N$ достаточно применить критерий «ближайшего соседа» $Z_N=\arg\min_{Z_N\in Q_N^m}\left\|Z_N-\tilde{Z}_N\right\|_N$.

В последующих разделах схема QAM OFDM модуляции в радиоканале с шумами будет использована в качестве элемента системы защиты передаваемых данных от несанкционированного доступа.

2. Неустойчивая схема QAM OFDM модуляции

Рассмотрим схему QAM OFDM модуляции с прежними значениями m, N и T, но при сужении функции сигнала $s(t)=\sum_{k=0}^{N-1}z_k\cdot e^{\frac{I2\pi kt}{T}}$ с интервала $[0,T]$ на его подинтервал $\left[0,\frac{T\cdot N}{M}\right]\subseteq[0,T]$, где $M\geq N$. Последнее означает увеличение пропускной способности идеального радиоканала без помех по сравнению с базовой до $C_M=\frac{2N\left(\log(m)+1\right)}{\frac{T\cdot N}{M}}=\frac{2M\left(\log(m)+1\right)}{T}\geq\frac{2N\left(\log(m)+1\right)}{T}=C_B$ бит/с. При этом сохраняются его основные QAM OFDM характеристики.

Зададим набор временных отсчетов $t_n=\frac{T}{M}\cdot n$ функции $s(t)$ на интервале $\left[0,\frac{T\cdot N}{M}\right]$, при $n\in 0..N-1$. Очевидно, Z_N удовлетворяет СЛАУ

$$F_{NN}^{M}Z_N=S_N^{M}, \tag{6}$$

где $S_N^{M}=\left\langle s_0^{M},s_1^{M},..,s_{N-1}^{M}\right\rangle=\left\langle s(t_0),s(t_1),..,s(t_{N-1})\right\rangle$, и $F_{NN}^{M}=\left(\varepsilon_M^{kn}\right)=\left(e^{\frac{I2\pi kn}{M}}\right)$ - квадратная матрица порядка N. Заметим, что $\det\left(F_{NN}^{M}\right)\neq 0$, при $M\geq N$. Таким образом, СЛАУ (6) имеет единственное решение $Z_N=\left(F_{NN}^{M}\right)^{-1}S_N^{M}$.

Как и ранее, при наличии в радиоканале аддитивных помех $\tilde{s}(t)=s(t)+\delta s(t)$ будем рассматривать задачу решения СЛАУ (7)

$$F_{NN}^{M}\tilde{Z}_N=\tilde{S}_N^{M}, \tag{7}$$

где $\tilde{S}_N^{M}=\left\langle\tilde{s}_0^{M},\tilde{s}_1^{M},..,\tilde{s}_{N-1}^{M}\right\rangle=\left\langle\tilde{s}(t_0),\tilde{s}(t_1),..,\tilde{s}(t_{N-1})\right\rangle$.

Заметим, что при $M\gg N$, матрица F_{NN}^{M} становится плохо обусловленной. Численные эксперименты показали экспоненциальный рост числа обусловленности матрицы $\mu\left(F_{NN}^{M}\right)$, в зависимости от роста M. Так, например, при $N=16$, $\mu\left(F_{NN}^{N+s}\right)\approx e^{5.4\cdot s+7.8}$, а при $N=32$, $\mu\left(F_{NN}^{N+s}\right)\approx e^{11.1\cdot s+16.6}$, $s\in 1..2\cdot N$.

Это приводит к значительным различиям между решениями задачи (5) и (6) даже для небольших значений нормы помех $\left\|\delta s(t)\right\|_{L^2(0,T)}<\delta$, и тем самым делает невозможным применение критерия «ближайшего соседа» для нахождения Z_N по значениям $\tilde{Z}_N$.

Как было продемонстрировано в серии численных экспериментов среднее значение $\frac{\left\|\left(F_{16,16}^{32}\right)^{-1}\Delta\right\|_{16}}{\left\|\Delta\right\|_{16}}\approx 10^{6}$, где $\Delta S_N^{M}=\left\langle\delta_0^{M},\delta_1^{M},..,\delta_{N-1}^{M}\right\rangle=\left\langle\delta(t_0),\delta(t_1),..,\delta(t_{N-1})\right\rangle$, и $\left\|\Delta S_N^{M}\right\|_N<\frac{h}{2}$.

3. Переход к устойчивой схеме за счет выбора секретного ключа

Положим $N = 2 \cdot N_0$, $M = 2 \cdot N$, и будем изучать решения СЛАУ (6)-(7) с матрицей F_{NN}^{M}. В предыдущем разделе было отмечено, что такая схема обеспечивает удвоение пропускной способности радиоканала по сравнению с базовой, но приводит к значительным погрешностям при декодировании сигнала на фоне помех.

Рассмотрим квадратную подматрицу матрицы F_{NN}^{M} порядка N_0, составленную из элементов, стоящих на пересечении четных строк и четных столбцов. Обозначим эту подматрицу $F_{N_0N_0}^{1}$.

Понятно, что $F_{N_0N_0}^{1} = \left(\varepsilon_{4N_0}^{(2k)\cdot(2n)}\right) = \left(\varepsilon_{N_0}^{kn}\right) = \left(e^{\frac{I2\pi kn}{N_0}} \right)$, $\det\left(F_{N_0N_0}^{1}\right) \neq 0$, и $\left(F_{N_0N_0}^{1}\right)^{-1} = \frac{1}{N_0}\left(\varepsilon_{N_0}^{-nk}\right)$, где $k, n \in 0..N_0 - 1$, и $\mu\left(F_{N_0N_0}^{1}\right) = 1$.

Также рассмотрим квадратную подматрицу матрицы F_{NN}^{M} порядка N_0, составленную из элементов, стоящих на пересечении четных строк и нечетных столбцов. Обозначим эту подматрицу $F_{N_0N_0}^{2}$. Понятно, что $F_{N_0N_0}^{2} = \left(\varepsilon_{4N_0}^{(2k+1)\cdot(2n)}\right) = \left(e^{\frac{I2\pi(2k+1)n}{2N_0}} \right) = \left(e^{\frac{I2\pi kn}{N_0}} \cdot e^{\frac{I2\pi n}{2N_0}} \right) = \left(\varepsilon_{N_0}^{kn} \cdot \varepsilon_{2N_0}^{n}\right)$,

$\det\left(F_{N_0N_0}^{2}\right) \neq 0$, и $\left(F_{N_0N_0}^{2}\right)^{-1} = \frac{1}{N_0}\left(\varepsilon_{N_0}^{-nk} \cdot \varepsilon_{2N_0}^{-k}\right)$, где $k, n \in 0..N_0 - 1$, и $\mu\left(F_{N_0N_0}^{2}\right) = 1$.

Зафиксируем и будем считать известным на передающей и приемной стороне секретный ключ $\Gamma_N^0 = \left\langle 0, \gamma_0, 0, \gamma_1, .., 0, \gamma_{N_0-1} \right\rangle \in \square^N = \square^{2N_0}$.

Зададим кодовое значение $Z_N^0 = \left\langle z_0, 0, z_1, 0, .., z_{N_0-1}, 0 \right\rangle$.

Положим $Z_N^+ = Z_N^0 + \Gamma_N^0 = \left\langle z_0, \gamma_0, z_1, \gamma_1, .., z_{N_0-1}, \gamma_{N_0-1} \right\rangle$.

В этом случае модель передачи символа Z_N^+ в QAM OFDM-канале с аддитивными помехами примет вид.

$$F_{NN}^{M} Z_N^+ + \Delta S_N^M = F_{NN}^{M} Z_N^0 + F_{NN}^{M} \Gamma_N^0 + \Delta S_N^M = \tilde{S}_N^M, \tag{8}$$

где $\Delta S_N^M = \left\langle \delta_0^M, \delta_1^M, .., \delta_{N-1}^M \right\rangle$.

Обозначая $\tilde{S}_N^0 = \left\langle s_0^0, s_1^0, .., s_{N-1}^0 \right\rangle = \tilde{S}_N^M - F_{NN}^{M} \Gamma_N^0$, запишем (8) в виде

$$F_{NN}^{M} Z_N^0 + \Delta S_N^M = \tilde{S}_N^0. \tag{9}$$

Учитывая структуру Z_N^0, запишем (9) в виде

$$F_{NN_0}^{M} Z_{N_0}^0 + \Delta S_N^M = \tilde{S}_N^0, \tag{10}$$

где $F_{NN_0}^{M}$ - прямоугольная матрица размерности $N \times N_0$, составленная из элементов матрицы F_{NN}^{M}, содержащихся в четных столбцах, а $Z_{N_0}^0 = \left\langle z_0, z_1, .., z_{N_0-1} \right\rangle \in \square^{N_0}$.

В силу (10) при любых $K \in 1..N$ должны выполняться равенства

$$F_{KN_0}^{M} Z_{N_0}^0 + \Delta S_K^M = \tilde{S}_K^0, \tag{11}$$

где $\Delta S_K^M = \left\langle \delta_0^M, \delta_1^M, .., \delta_{K-1}^M \right\rangle$, $S_K^0 = \left\langle s_0^0, s_1^0, .., s_{K-1}^0 \right\rangle$.

С учетом сказанного в начале раздела, в случае $K = N_0$ получаем

$$F_{N_0N_0}^{1} Z_{N_0}^0 + \Delta S_{N_0}^M = \tilde{S}_{N_0}^0, \tag{12}$$

где $\tilde{S}_{N_0}^0 = \tilde{S}_{N_0}^M - F_{N_0N_0}^{2} \Gamma_{N_0}^0$, $\Gamma_{N_0}^0 = \left\langle \gamma_0, \gamma_1, .., \gamma_{N_0-1} \right\rangle \in \square^{N_0}$.

Обозначим $\tilde{Z}_{N_0}^0$ единственное решение уравнения

$$F_{N_0N_0}^{1} \tilde{Z}_{N_0}^0 = \tilde{S}_{N_0}^0, \tag{13}$$

тогда будет иметь место оценка

$$\frac{\left\| Z^{0}_{N_0} - \tilde{Z}^{0}_{N_0} \right\|_{N_0}}{\left\| Z^{0}_{N_0} \right\|_{N_0}} \le \mu\left(F^{1}_{N_0 N_0}\right) \frac{\left\| \Delta S^{M}_{N_0} \right\|_{N_0}}{\left\| S^{M}_{N_0} \right\|_{N_0}} = \frac{\left\| \Delta S^{M}_{N_0} \right\|_{N_0}}{\left\| S^{M}_{N_0} \right\|_{N_0}}, \quad (14)$$

при этом, очевидно, $\left\| \Delta S^{M}_{N_0} \right\|_{N_0} \le \left\| \Delta S^{M}_{N} \right\|_{N}$.

Теперь, для нахождения $Z^{0}_{N_0}$ (и, следовательно, Z^{0}_{N}) по значению $\tilde{Z}^{0}_{N_0}$ достаточно применить критерий «ближайшего соседа» $Z^{0}_{N_0} = \arg \min_{Z^{0}_{N_0} \in Q^{m}_{N}} \left\| Z^{0}_{N_0} - \tilde{Z}^{0}_{N_0} \right\|_{N_0}$.

Заметим, что предложенная схема обеспечивает пропускную способность радиоканала $C^{0}_{M} = \frac{2N_0(\log(m)+1)}{\frac{T \cdot N}{M}} = \frac{4N_0(\log(m)+1)}{T} = \frac{2N(\log(m)+1)}{T} = C_B$ бит/с. Таким образом, пропускная способность равна базовой, однако при наличии помех декодирование сигнала без знания секрета $\Gamma^{0}_{N_0} = \left\langle \gamma_0, \gamma_1, .., \gamma_{N_0-1} \right\rangle$ будет затруднено.

Серия численных экспериментов показала надежное декодирование сигнала по схеме с секретом даже при таком уровне помех, при котором регуляризирующие методы решения СЛАУ (7) обеспечивали, в среднем, не более 45% успешного определения элементов кодового значения $Z_N = \left\langle z_0, z_1, .., z_{N-1} \right\rangle$.

Заметим, что полученные результаты обобщаются, как минимум, на случаи $N = m \cdot N_0$, $M = m \cdot N$, при натуральных $m > 2$. Для двукратных схем, $N_0 = 2^k$, численная реализация моделей декодирования допускает применение алгоритмов быстрого преобразования Фурье.

4. Заключение

В работе предложен вариант применения QAM OFDM-модуляции для защиты передаваемых данных в радиоканале с помехами на основе схемы симметричного шифрования. В качестве секрета используются значения амплитуд нечетных поднесущих гармоник сигнала. Передаваемые данные искажаются за счет случайных помех, а сложность их декодирования без знания секрета обусловливается высокой чувствительностью схемы модуляции к вариациям измеряемых значений.

Заметим, что после обязательной процедуры синхронизации QAM OFDM-канала секретные ключи могут согласованно вырабатываться для каждого передаваемого кодового значения, что усилит общую криптостойкость сеанса связи.

Схема не влияет на пропускную способность радиоканала и не требует дополнительных вычислительных затрат на проведение криптопреобразований передаваемых данных.

5. Литература

[1] Bahai, A. Multi-Carrier Digital Communications: Theory and Publications of OFDM / A. Bahai, B. Saltzberg, M. Ergen // New York: Springer, 2004.

[2] Goldsmith, A. Wireless Communications // Cambridge University Press, Cambridge, 2005.

[3] Hanzo, L. Single- and Multi-carrier Quadrature Amplitude Modulation / L. Hanzo, W. Webb, T. Keller // New York: Wiley, 2000.

[4] Леонович, Г.И. Перспективные направления развития беспроводных сенсорных сетей / Г.И. Леонович, А.И. Данилин, В.В. Сергеев, В.П. Цветов, С.В. Куприянов // Актуальные проблемы радиоэлектроники и телекоммуникаций: материалы Всероссийской научно-технической конференции – Самара: ООО «Артель», 2019. – С. 8-11.

[5] Цветов, В.П. Об одной задаче декодирования символов по неполным данным в радиоканале // Сборник трудов III международной конференции ИТНТ. – Самара: Новая техника, 2017. – С. 954-957.

Wireless channel noises and data protection

V.P. Tsvetov[1]

[1]Samara National Research University, Moskovskoe Shosse 34A, Samara, Russia, 443086

Abstract. The paper proposes an application of a quadrature amplitude modulation (QAM) scheme using orthogonal frequency division multiplexing (OFDM) transmission for data protection. Our approach bases on the symmetric encryption and uses a natural or induced noise in a wireless channel as a random part of a secret key. The main idea for this is the sensitivity of the signal decoding model to variations of measured values. This kind of protection does not require additional computational costs and does not affect the bandwidth of the channel.