УДК 621.391

А. А. ЗАМУЛА, канд. техн. наук

ПРЕДЛОЖЕНИЯ ПО ПОСТРОЕНИЮ ШИРОКОПОЛОСНЫХ СИСТЕМ ПЕРЕДАЧИ СО СЛОЖНЫМИ СИГНАЛАМИ

Введение

Одним из методов обмена данными в системах передачи информации (СПД) является метод, основанный на использовании динамической смены соответствия: *m* бит сообщения – 2^m сложных сигналов. Для реализации метода должны быть определены требования к источнику сложных сигналов с точки зрения решения классических задач теории оптимального приема (обнаружение, различение, оценка параметров и др.), а также сформулированы условия, обеспечивающие установление такого правила смены соответствия *m* бит сообщения – 2^m сложных сигналов, предсказание которого нарушителем возможно с вероятностью, не превышающей допустимую.

Цель статьи – разработка предложений по построению скрытной системы передачи информации на основе использования сигналов с расширенным спектром.

Постановка задачи выбора сложных сигналов для широкополосных систем передачи

Известно, что любой сигнал $S(t)$ конечной энергии может быть представлен как сумма несчётного числа гармонических колебаний, амплитуды и фазы которых в пределах бесконечно малого диапазона частот $[f, f+df]$ определяются спектральной плотностью или спектром $\overline{S}(f)$. Математическим отображением этого факта служит пара обратного и прямого преобразования Фурье

$$S(t)=\int_{-\infty}^{\infty}\overline{S}(f)\exp(j2\pi ft)df,\ \tilde{S}(f)=\int_{-\infty}^{\infty}S(t)\exp(-2\pi ft)dt. \qquad (1)$$

Для характеристики размера зоны, в которой сосредоточена энергия сигнала во временной или частотной области, используются обозначения длительности сигнала T или полосы ΔF соответственно. Детерминированный сигнал, для которого $T\Delta F >> 1$, и полоса которого может изменяться независимо от длительности, называется сигналом с расширенным спектром или широкополосным.

Типичным для теории связи является подход, заключающийся в разработке оптимального приемного устройства, которое с наилучшим качеством восстановит информацию, содержащуюся в наблюдаемом колебании. Определение оптимального алгоритма обработки, базирующегося на учёте специфических свойств переданного сигнала, позволяет синтезировать оптимальным образом и сам сигнал, т.е. выбрать наилучшим образом метод его кодирования и модуляции.

В теории связи наиболее распространённой моделью служит канал с аддитивным белым гауссовским шумом, в котором вероятность трансформации каналом заданного входного сигнала в то или иное выходное наблюдение $y(t)$ (переходная вероятность – $P[y(t)\,|\,S(t)]$) экспоненциально уменьшается с ростом квадрата Евклидова расстояния между переданным сигналом и выходным наблюдением:

$$P\left[y(t)\middle|S(t)\right]=\kappa\exp\left(-\frac{1}{N_0}\,d(s,y)\right), \qquad (2)$$

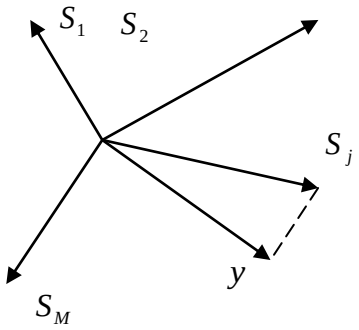
где κ – константа, не зависящая от $S(t)$ и $y(t)$, N_0 – спектральная плотность мощности одностороннего белого шума; а Евклидово расстояние между $S(t)$ и $y(t)$ определяется как

$$d(S,y)=\sqrt{\int_0^T\left[y(t)-S(t)\right]^2 dt}. \tag{3}$$

Согласно соотношениям (2) и (3) похожесть сигнала (вероятность того, что он преобразован каналом в наблюдение $y(t)$ уменьшается с увеличением Евклидова расстояния между $S(t)$ и $y(t)$. В случае равной вероятности всех сообщений источника (что достигается при правильном проектировании системы) оптимальной стратегией наблюдателя, обеспечивающей минимальную ошибку перепутывания действительно переданного с некоторым другим сигналом, является правило (критерий) максимального правдоподобия (МП). Согласно данному алгоритму, после того, как колебание $y(t)$ стало достижимым (принято), решение принимается в пользу того сигнала, для которого вероятность трансформации его каналом в принятое наблюдение $y(t)$ является наибольшим (по сравнению с вероятностями для других сигналов). С учётом изложенного, МП решение для гауссова канала может быть преобразовано в правило минимума расстояния

$$d(S_j,y)=\min d(S_j,y)\Rightarrow H_j, \tag{4}$$

т.е. решение принимается в пользу сигнала $S_j(t)$, поскольку он наиболее близок (в смысле Евклидова расстояния) к наблюдению $y(t)$ среди всех конкурирующих сигналов (рис. 1).



$$d(S_j,y)=\min\ d(S_i,y)$$

Рис. 1

С учётом используемой геометрической интерпретации сигналов можно ввести длину сигнала $\|S\|$ как его расстояние относительно начала координат. Тогда из (3) следует, что $\|S\|=d(S,0)=\sqrt{E}$, где

$$E=\int_0^T S^2(t)dt, \tag{5}$$

– энергия сигнала. Другой важной геометрической характеристикой является скалярное произведение (U,V) двух сигналов: $U(t),V(t)$

$$(U,V)=\int_0^T U(t)\cdot V(t)dt, \tag{6}$$

которое может трактоваться как предельная форма скалярного произведения двух *n*-мерных векторов. Эта же характеристика может быть вычислена с помощью длины векторов и косинуса угла α между ними: $(U,V) = \|U\|\|V\|\cos\alpha$, и, таким образом, скалярное произведение свидетельствует о близости или похожести сигналов, поскольку, чем ближе сигналы одинаковой длины (энергии) друг к другу, тем меньше $\cos\alpha$ отличается от единицы, и тем больше скалярное произведение. На основании этого скалярное произведение (6) называют также корреляцией сигналов.

Раскрыв скобки в (3), приходим к соотношению

$$d^2(S_i, y) = \int_0^T y^2(t)dt - 2\int_0^T y(t)\cdot S(t)dt + \int_0^T S^2(t)dt = \|y\|^2 - 2Z_i + \|S_i\|^2, \qquad (7)$$

где Z_i – соответствует корреляции между наблюдением $y(t)$ и i-м сигналом $S_i(t)$:

$$Z_i(y, S_i) = \int_0^T y(t)\cdot S(t)dt. \qquad (8)$$

Первое слагаемое в правой части соотношения (7) фиксировано для данного наблюдения и не влияет на анализируемые расстояния и решение, какой из сигналов был принят. Последний член суммы есть ни что иное, как энергия i-го сигнала E_i. Учитывая это, правило минимума расстояния (4) может быть сформулировано как правило максимума корреляции:

$$Z_j - \frac{E_j}{2} = \max(Z_i - \frac{E_j}{2}) \Rightarrow H_j, \qquad (9)$$

означающее, в частности, что из M возможных сигналов с одинаковой энергией фактически принятым считается тот, который имеет максимум корреляции с наблюдением $y(t)$.

Приведенные рассуждения указывают на способ конструирования множества сигналов. На рис. 2 изображены сигнальные векторы.

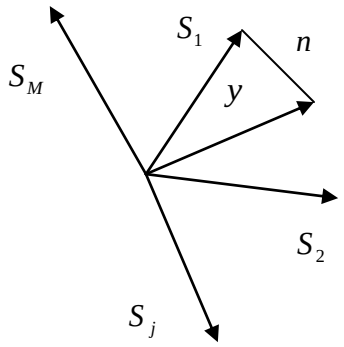


Рис. 2

Предположим, что передавался сигнал S_1 и что он подвергается искажению в канале с аддитивным белым гауссовым шумом, следствием чего служит добавление к S_1 вектора шума *n*. Гауссовский вектор *n* характеризуется симметричным (сферическим) вероятностным распределением, экспоненциально спадающим с увеличением длины вектора *n*, что очевидно следует из (2) после удаления из него сигнала (т.е. при подстановки $S(t) = 0$). Следователь-

но, вектор наблюдения $y = s_1 + n$ будет случайным образом перемещаться вокруг S_1, как это показано на рисунке, и тогда, согласно правилу минимума расстояния (4), как только *y* окажется ближе к некоторому другому, чем S_1 сигналу, то будет принято ошибочное решение. Для минимизации вероятности возникновения такого рода ошибки следует располагать другие сигналы на максимально большом расстоянии от S_1. Поскольку любой из M сигналов может передаваться равновероятно, т.е. занимать место S_1, то, очевидно, что все расстояния следует делать максимально большими.

Задача построения множества максимально удалённых друг от друга сигналов (входящая в класс так называемых задач упаковки) оказывается достаточно сложной и пока что не имеет общего решения.

Различают две классические версии широкополосной модуляции: прямой последовательностью и $d(S_i, S_j), 1 \le i \le j \le M$ прыгающей частотой [1]. Идея прямого расширения спектра состоит в амплитудно-фазовой модуляции дискретных последовательностей (сигнатур) пользователя потоком данных. Например, выполняется умножение битового информационного потока $B_k(t)$-го абонента на специфическую для каждого пользователя (в многопользовательских системах, например в CDMA приложениях) на сигнатуру $S_k(t)$, а результат произведения $S_k(t) \cdot B_k(t)$ моделирует непрерывную несущую, т.е.

$$S_k(t, b_k) = S_k(t) \cdot B_k(t) \cdot \cos(2\pi f_0 t)$$

где $b_k = (..., b_{k,-1}, b_{k,0}, b_{k,1}, ...)$ – битовый поток *k*-го пользователя, а $B_k(t) = b_{k,i} = \pm 1, (i-1)T_b < t < iT_b$ (T_b – длительность импульсов положительной и отрицательной полярности информационного сигнала *k*-го пользователя).

В описанном примере битовый поток первоначально модулирует бинарную сигнатуру, а результат используется для бинарной фазовой манипуляции несущей.

В [1] показано, что в качестве сигнатур в системе с прямым расширением должен использоваться такой ансамбль детерминированных последовательностей, все представители которого в идеале обладают нулевой постоянной составляющей, идеальной периодической автокорреляционной функцией (АКФ) и нулевой периодической взаимокорреляционной функцией (ВКФ).

Широкое практическое использование имеют минимаксные ансамбли: *m*-последовательности, множества Голда, множества Кассами и их расширения, ансамбли Камалетдинова, характеристические коды и др.

Условия построения абсолютно стойкой системы передачи на уровне источника сигналов

Обоснование выбора того или иного класса минимаксных ансамблей для рассматриваемого метода передачи данных выходит за рамки данной статьи. Основное внимание будет сосредоточено на условиях, обеспечивающих установление правила смены соответствия *m* бит сообщения – 2*m* сложных сигналов, при выполнении которых предсказание нарушителем правила смены соответствия возможно с вероятностью, не превышающей допустимую. И в этом смысле можно говорить о некотором значении криптографической стойкости СПИ на уровне источника сложных сигналов.

На рис. 3 представлена структурная схема формирования сигнала в динамическом радиоканале, состоящая из ИИ – источника информации, ДМ – динамического модулятора, УФУП – устройства формирования управляющей последовательности.

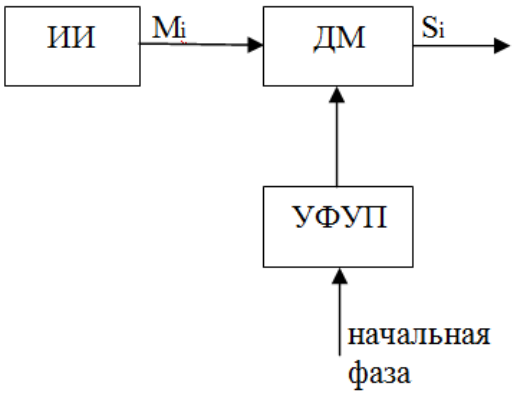


Рис. 3

Пусть имеется некоторый источник информации, создающий в фиксированный момент времени одно из M возможных сообщений. Каждое из M конкурирующих сообщений передается посредством сигнала: S = {S_i(t): i = 1,2, …, M} вида (1). На число сигналов M (или мощность множества S) не накладываются никакие ограничения и, если это необходимо, множество S может быть бесконечным.

Радиоканалы, в которых выполняются эти условия, называют динамическими.

Модулятор обеспечивает формирование сложных сигналов, а демодулятор (устройство обработки сложных сигналов) – их поиск, обнаружение и различение. Символы сообщения от источника информации, представленные в виде m бит, поступают в динамический модулятор, в котором в соответствии с символами управляющей последовательности УФУП, осуществляется выбор 2^m из M сложных сигналов и таким образом устанавливается соответствие: m бит – 2^m сложных сигналов. При появлении на входе динамического модулятора m бит сообщения в канал связи излучается сложный сигнал S_i, выбранный в зависимости от значения управляющей последовательности.

По истечении времени T соответствие m бит – 2^m сложных сигналов изменяется по определенному закону (правилу).

Нарушитель, осуществляющий наблюдение за каналом связи, может реализовывать различные стратегии воздействия на СПД: перехват излученных сигналов, их анализ, попытки распознавания сигналов и определения закона их излучения, формирование и постановка помех с целью навязывания ложных сообщений и др.

В демодуляторе на станции приема производится различение одного из 2^m разрешенных информационных сигналов. После демодуляции в соответствии решением, принятым в соответствии с (10) на выходе демодулятора формируются m бит сообщения, которые поступают получателю сообщений.

Естественным представляется постановка ряда вопросов, на которые необходимо дать ответы, если мы хотим построить СПИ, реализующую обсуждаемый метод передачи данных. Насколько устойчива система против раскрытия закона установления соответствия m бит сообщения – 2^m сложных сигналов, если нарушитель не ограничен временем и обладает всеми необходимыми средствами для анализа перехваченных сигналов. Имеет ли правило соответствия, которое определяет нарушитель, единственное решение (j – вариант соответствия: m бит – сложный сигнал), и если нет, то сколько приемлемых решений возможно. Какой объем данных (число элементов физического носителя информации, – сигнала) необходимо перехватить нарушителю, для того, чтобы решение стало единственно верным. Существуют ли системы, в которых вообще нельзя принять единственное правильное решение независимо от того, каков объем перехваченного в канале наблюдения.

Предположим, что имеется конечное число возможных дискретных сообщений $M_1, M_2, ..., M_N$ с априорными вероятностями $P(M_1), P(M_2), ..., P(M_N)$ и что эти сообщения

преобразуются в возможные сложные сигналы $S_1,S_2,\ldots S_N$. После того как нарушитель перехватил некоторый сигнал, он имеет возможность вычислить апостериорные вероятности сообщений, содержащихся в принятом наблюдении.

Сформулируем необходимые и достаточные условия построения абсолютно стойкой системы на уровне источника сигналов.

Пусть каждые *m* бит источника сообщений в интервале T ставятся в соответствие 2^m сложных сигналов S, выбранных из пространства {S} размерности $N \geq 2$, тогда необходимыми и достаточными условиями абсолютной стойкости на уровне источника сигналов являются условия [1]

$$P(M_i / S_i) = (M_i); \tag{10}$$

$$P(S_i / S_{i-1}, S_{i-2}, S_v, ..., S_1) = P(S_i). \tag{11}$$

Другими словами: вероятность появления S_i сигнала в канале не должна зависеть от того, какое сообщение появилось на выходе источника; вероятность появления S_i сигнала в канале не должна зависеть от того, какие сигналы до этого излучались. В этом случае перехват нарушителем сигнала не дает ему никакой информации, необходимой для определения содержания сообщения, содержащегося в полученных сигналах. С другой стороны, если эти условия равенства вероятностей не выполнены, то имеют место случаи, когда для определенного варианта соответствия *m* бит сообщения – 2^m сложных сигналов апостериорные вероятности, вычисленные нарушителем, отличаются от априорных. А это, в свою очередь, может повлиять на выбор нарушителем своих действий и, таким образом, не обеспечит абсолютной стойкости системы.

Необходимое условие следует из теоремы Байеса, в соответствии с которой [1]

$$P(M_i / S_i) = \frac{P(M_i)P(S_i / M_i)}{P(S_i)}, \tag{12}$$

где $P(M_i)$ – априорная вероятность (передачи сообщения M_i); $P(M_i / S_i)$ – апостериорная вероятность сообщения M_i при условии, что перехвачен сигнал S_i; $P(S_i / M_i)$ – условная вероятность сигнала S_i при условии, что выбрано сообщение M_i; $P(S_i)$ – вероятность получения сигнала S_i.

Для обеспечения абсолютной стойкости величины должно быть выполнено одно из равенств: или $P(M_i) = 0$ (это решение должно быть отброшено, так как требуется, чтобы равенство осуществлялось при значениях $P(M)$ или же $P(E_i / M_i) = P(E_i)$ для любых M и E, или $P(S_i / M_i) = P(S_i)$, тогда $P(M_i / S_i) = P(M_i)$ и система обладает абсолютной стойкостью. Тогда количество информации, содержащейся у нарушителя после перехвата сигнала I(E/M),

$$I(S,M) = H(M) - H(M / S) = H(M) - H(M) = 0, \tag{13}$$

где $H(M / S)$ – энтропия источника сообщения, при условиях, что перехвачен сигнал S; $H(M)$ – энтропия источника открытого сообщения.

Условие (10) является достаточным условием абсолютной стойкости. В этом случае определение *j*-варианта соответствия может быть выполнено только методом статистического опробования всевозможных вариантов, т. е. методом перебора.

Как следует из (11), вероятность появления S_i сигнала не зависит от вероятности появления всех *i*-1 сигналов. В этом случае количество информации в сигнале S_i после перехвата всех *i*-1 сигналов

$$I(S_i, S_v) = H(S_i) - H(S_i / S_v) = H(S_i) - H(S_v), \quad (14)$$

где $v = 1, i-1$.

Из выражения (11) также следует равновероятность появление сигналов, (т.е. равновероятность отображения m – бит – S_i сигнал), поэтому

$$H(S_i) = H(S_v). \quad (15)$$

Подставляя выражение (15) в выражение (14), получаем $I(S_i, S_v) = 0$.

Условие (11) является также и достаточным, так как независимость и равновероятность появления сигналов означает и равновероятность появления управляющей гаммы, символы которой статистически независимы и асимптотически равновероятны.

Сформулируем необходимое и достаточное условия абсолютной стойкости сигналов источника сложных ФМ ШПС сигналов {S}. Под абсолютной стойкостью будем понимать их идеальную структурную скрытность.

Пусть {S} есть ансамбль ФМ ШПС сигналов объема N с числом разрядов L в каждом из них, тогда для обеспечения абсолютной стойкости каждого из $S_i \in \{S\}$ сложных ФМ ШПС необходимо и достаточно, чтобы

$$P(S_{j,i} / S_{v,R}) = P(S_{j,i}), v = \overline{1, L}, R = \overline{1, N}, \quad (16)$$

т. е. чтобы вероятность появления элемента $S_{j,i}$ сложного ФМ ШПС сигнала не зависела ни от элементов ранее переданных сигналов, ни от элементов $S_{j,i-1}, S_{j,i-2}, S_{j,v}, ..., S_{j,2}, S_{j,1}$ сигнала S_j.

Необходимость условия (16) следует непосредственно из критерия абсолютной структурной скрытности сигнала [3]

$$S_c = \frac{l}{L}, \quad (17)$$

где l – число символов сложного сигнала, которые необходимо знать для определения закона формирования $L - l$ оставшихся.

Для случая,когда $l = L$

$$S_c = \frac{l}{L} = \frac{L}{L} = 1.$$

Поэтому по любому числу перехваченных символов $l < L$ S_j сигнала нельзя предсказать последующие $L - l$ символов как S_j сигнала, так и всех $S_v, v = \overline{1, i-1}, v \neq j$. Условие (16) является и достаточным.

Действительно, условная энтропия относительно закона формирования S_j сигнала после перехвата не менее R символов в v сигналах

$$H(S_{ji} / S_{v,k}) = -\sum_{i=1}^{N} P(S_{j,i} / S_{v,k}) \log P(S_{j,i} / S_{v,k}), \quad (18)$$

и среднее значение условной энтропии об источнике (законе формирования) сигналов [2]

$$H\{S\}/\{S_v\} = -\sum_{j=1}^{v+1} \sum_{i=1}^{k} P(S_{j,i} / S_{v,k}) \log P(S_{j,i} / S_{v,k}), \quad (19)$$

вследствие справедливости (16), совпадает с априорной неопределенностью H({S}) источника сигналов. Поэтому количество информации**,** получаемое нарушителем при анализе (раскрытии закона формирования сигналов)

$$I(\{S\}/\{S_v\}) = H(\{S\}) - S(\{S\}/\{S_v\}) = H(\{S\}) - H(\{S\}) = 0 .$$

Выводы

Анализ выражений (16) – (19) дает возможность сформулировать предложения по построению скрытной СПИ на основе использования сигналов с расширенным спектром:

1. Закон формирования каждого из сигналов должен быть случайным, причем даже при перехвате L-1 из L символов сигнала не должно существовать единственного решения относительно закона его формирования.

2. Абсолютно стойким, с точки зрения закона формирования, является источник сигналов со случайным формированием всех сигналов, так как только в этом случае у нарушителя отсутствует возможность принятия правильного решения относительно используемого в системе сигнала.

Список литературы: 1. *Ipatov, Valery P.* Spread Spectrum and CDMA. Principles and Applications / Valery P. Ipatov. University of Turku, Finland and St. Petersburg Electrotechnical University ‘LETI’, Russia. John Wiley & Sons Ltd, The Atrium, Southern Gate, Chichester, West Sussex PO19 8SQ, England, 2005. – 385 p. 2. Shannon C, Communication theory of secrecy system, Bell System Techn.J., 28, №4 (1949). 3. *Горбенко, І.Д., Горбенко, Ю.І.* Прикладна криптологія: Теорія. Практика. Застосування : монографія. Вид. 2-ге, перероб. і доп. – Харків : Форт, 2012. – 880 с. 4. *Помехозащищенность* радиосистем со сложными сигналами / Г. И. Тузова, В. А. Сивов и др ; под ред. Г. И. Тузова. – М. : Радиосвязь, 1985. – 264 с.

Харьковский национальный университет радиоэлектроники

Поступила в редколлегию 10.09.2012