



УДК 621.396
DOI 10.21685/2587-7704-2018-3-1-6



Open
Access

RESEARCH
ARTICLE

О возможностях построения систем связи с низкой вероятностью обнаружения факта передачи информации

Б. В. Султанов

Пензенский государственный университет, Россия, 440026 г. Пенза, ул. Красная, 40

В. В. Дорошкевич

Пензенский государственный университет, Россия, 440026 г. Пенза, ул. Красная, 40

В. В. Легошин

Пензенский государственный университет, Россия, 440026 г. Пенза, ул. Красная, 40

Аннотация. Рассматриваются возможные подходы к построению систем связи с низкой вероятностью обнаружения факта передачи.

Ключевые слова: низкая вероятность обнаружения, прямое расширение спектра, программная перестройка рабочей частоты, модуляция циклическим сдвигом кода, системы связи со многими несущими, множественный доступ с кодовым разделением.

Possibilities of building communication systems with a low probability of information transfer intercept

B. V. Sultanov

Penza State University, 40 Krasnaya Street, 440026, Penza, Russia

V. V. Doroshkevich

Penza State University, 40 Krasnaya Street, 440026, Penza, Russia

V. V. Legoshin

Penza State University, 40 Krasnaya Street, 440026, Penza, Russia

Abstract. Possible approaches to building communication systems with a low probability of transfer intercept are considered.

Key words: low probability of intercept, direct spectrum spread, program reorganization of operational frequency, cyclic code shift keying, multicarrier communication systems, code division multiple access.

В основе классического подхода к построению связи с низкой вероятностью обнаружения (Low Probability of Intercept (LPI)) факта передачи информации лежит использование методов расширенного спектра, обеспечивающих возможность распределения энергии передаваемого сигнала в широком диапазоне частот [1]. При этом мощность полезного сигнала не превышает мощности шума эфира.

Наряду с этим предлагался еще один способ построения подобных систем [2], основанный на оценке спектра сигнала входной антенны, характеризующего мгновенную ситуацию в эфире, выявлению областей частот, в которых уровень спектральной плотности находится ниже среднего уровня шума эфира и формирования в передатчике несущего сигнала (fundamental domination waveform (FDW) [3]), спектр которого находится внутри выявленных областей и не превышает среднего уровня

© 2018 Султанов Б. В., Дорошкевич В. В., Легошин В. В.

Данная статья доступна по условиям всемирной лицензии Creative Commons Attribution 4.0 International License (<http://creativecommons.org/licenses/by/4.0/>), которая дает разрешение на неограниченное использование, копирование на любые носители при условии указания авторства, источника и ссылки на лицензию Creative Commons, а также изменений, если таковые имеют место.

шума. Сигнал FDW модулируется циклическим сдвигом, осуществляемым в соответствии с полезной информацией, и после выполнения необходимых преобразований передается в эфир. В приемнике также анализируется спектр сигнала входной антенны, и на основании получаемой при этом информации из принимаемого в процессе передачи сигнала удаляются все составляющие спектра с частотами, соответствующими областям превышения уровнем спектральной плотности среднего уровня шума эфира. В результате остается лишь модулированный сигнал FDW, после демодуляции которого извлекается переданная информация.

Рассмотренный подход нашел свое применение в развитии систем связи с трансформацией областей преобразования сигнала, которые заложены в основу построения когнитивного радио. В настоящее время имеется большое количество публикаций по проблемам подобных систем и когнитивного радио, однако обсуждение специфики их применения и анализа характеристик в задаче обеспечения LPI в них отсутствует.

Существуют различные методы построения систем с расширенным спектром, из которых наибольшее распространение получили прямое расширение спектра (ПРС), программная перестройка рабочей частоты (ППРЧ) и их комбинации [1]. Кроме них, в задаче построения систем скрытой передачи информации используются и некоторые другие методы, такие как модуляция циклическим сдвигом кода [4], комбинация ПРС и ППРЧ в сочетании с ортогональной частотной модуляцией [5]. Ниже приводятся краткие описания этих методов и оценки их возможностей.

Прямое расширение спектра передаваемого узкополосного сигнала $u(t)$ осуществляется путем его балансной модуляции бинарной псевдослучайной последовательностью $c(t)$, состоящей из равновероятных элементов, принимающих значения ± 1 и генерируемых с частотой f_c , в N раз превышающей тактовую частоту следования информационных символов $f_T = 1/T_T$. Таким образом, длительность одного элемента данной последовательности равна $T_c = T_T/N$. При этом ширину энергетического спектра W_{SS} полученного таким образом процесса $x(t)$ можно определить как $W_{SS} = 1/T_c$.

Для снятия расширения спектра в приемнике необходимо иметь опорную последовательность $\hat{c}(t)$, когерентную с модулирующей последовательностью $c(t)$, присутствующей во входном сигнале. Трудности синхронизации генератора опорной псевдослучайной последовательности с точностью до долей наносекунд ограничивают возможности сокращения длительности $T_{\hat{c}}$, а следовательно, и предельные возможности расширения спектра этим методом.

В системах с ППРЧ расширение спектра осуществляется за счет скачкообразного изменения частоты несущего колебания при модуляции передаваемого сигнала данных. При этом вся широкая полоса частот канала W_{SS} разбивается на примыкающие друг к другу узкие полосы. На интервале длительности одного скачка частоты T_c передаваемый сигнал занимает одну из возможных частотных полос. Выбор частотной полосы в передатчике осуществляется по закону, задаваемому генератором псевдослучайной последовательности, управляющим формированием соответствующих несущих частот f_n [1].

Для снятия расширения спектра в приемнике необходимо иметь опорную последовательность гармонических колебаний с частотами $\hat{f}_n = f_n$, что предполагает установление синхронизации между выходным сигналом опорного генератора приемника, формирующего последовательность перебираемых рабочих частот \hat{f}_n , и принимаемым сигналом. Однако в данном случае требования к системе синхронизации оказываются менее жесткими. Это связано с тем, что длительность подлежащих синхронизации временных интервалов T_c в системах с ППРЧ при заданной общей ширине полосы частот энергетического спектра W_{SS} процесса $x(t)$ значительно превышает значение T_c в системах с прямым расширением спектра. Таким образом, требования к синхронизации при использовании ППРЧ не так строги, как при прямом расширении спектра. В результате в этом случае обеспечивается возможность распределения энергии передаваемого сигнала в значительно более широком диапазоне частот. Данное обстоятельство и послужило основанием для сделанного в работе [1] вывода о предпочтительности использования ППРЧ в системах скрытой передачи информации. Вместе с тем, как показано в работе [6], низкая вероятность обнаружения может быть достигнута лишь при очень ограниченной длительности сеанса связи, причем для обнаружителя безразлично, содержат ли эти символы полезную или служебную информацию. Поэтому для повышения эффективности функционирования систем скрытой связи необходимо максимальное сокращение времени выполнения служебных

процедур и, в частности, процедуры первоначальной синхронизации (поиска), являющейся ключевой и наиболее длительной при реализации ППРЧ.

В системах с модуляцией циклическим сдвигом кода (Cyclic Code Shift Keying – CCSSK) алфавит сигналов формируется циклическими сдвигами одной-единственной исходной кодовой последовательности (она же выполняет роль опорной копии сигнала в корреляторе) [3, 4]. После установления синхронизации процедура оптимального приема сводится к вычислению временной функции корреляции (ВРК) зашумленного сигнала на входе с его опорной копией. По положению корреляционного максимума приемник определяет номер циклического сдвига последовательности, задающей фазовый код принятого сигнала, относительно опорной (порождающей) последовательности алфавита. Найденный номер сдвига кода ассоциируется с некоторым переданным M -чным символом. Соответственно, один такой символ содержит $\log_2 M$ бит информации. Цифровая реализация приемника CCSSK-сигналов предполагает вычисление преобразования Фурье входного сигнала, затем – нахождение его произведения с комплексно-сопряженным спектром опорного сигнала и, наконец, – обратного преобразования Фурье от полученного результата. Данные обстоятельства и определяют основное преимущество систем с CCSSK – простоту технической реализации с точки зрения аппаратных и вычислительных затрат. Все основные операции обработки сигнала в приемнике выполняются процессором, вычисляющим быстрое преобразование Фурье (БПФ). В работе [4] приведены результаты анализа вероятности обнаружения факта передачи в системах с CCSSK в противостоянии описанному выше радиометру. В частности, в статье утверждается, что при больших значениях M (при $M > 14$) повышение вероятности детектирования при увеличении длительности наблюдения T (т.е. продолжительности сеанса связи) является не очень заметным. Это объясняется тем, что при больших M энергия символа оказывается сильно «размазанной» по времени. Однако приводимые количественные данные, иллюстрирующие этот вывод, представлены для очень ограниченных значений T . Так, при $M = 16$ вероятности ошибки в приемнике $P = 10^{-5}$; вероятности ложной тревоги $P_{FA} = 10^{-4}$; значение $P_d = 0,5 \cdot 10^{-3}$ будет иметь место при $W_{SS} \cdot T = 10^5$. Поскольку $W_{SS} = 1/T_{ch}$, где T_{ch} – длительность передачи одного элемента кодовой последовательности, это означает, что при приведенных выше параметрах обнаружения может быть передано 10^5 элементов последовательности. Так как период псевдослучайной последовательности (а следовательно, и интервал оценивания ВРК) содержит $2^M = 2^{16}$ элементов, из этого следует, что в данной ситуации не может быть передано даже два M -чных символа. К сожалению, других данных, характеризующих вероятность обнаружения при больших значениях T , в статье не приводится. Тем не менее имеющиеся результаты подтверждают тот факт, что низкая вероятность обнаружения может быть достигнута при очень короткой длительности сеанса связи. При этом опять же возникает проблема быстрой синхронизации.

Принцип построения систем связи со многими несущими, обеспечивающих множественный доступ с кодовым разделением (multicarrier CDMA (MC CDMA)), основан на комбинации метода прямого расширения спектра и ортогональной частотной модуляции (OFDM). При этом прямому расширению спектра путем балансной модуляции бинарной (адресной) псевдослучайной последовательностью $c(t)$ подвергается непосредственно сигнал данных – последовательность информационных символов данных $\{d_k\}$, принимающих на интервале длительность такта T_T передачи информационного символа с равной вероятностью значения ± 1 . Получившийся в результате этой модуляции последовательный поток чипов длительностью $T_c = T_T/N$ преобразуется в параллельный набор данных и далее модулируется посредством OFDM. В работе [5] проанализировано свойство низкой вероятности обнаружения факта передачи (LPI) в противостоянии радиометру тактической сети, предназначенной для осуществления связи на поле боя и основанной на использовании MC CDMA в комбинации с медленной ППРЧ. Смысл этой комбинации заключается в том, что с целью противодействия вносимым противником помехам полученный описанным выше образом сигнал MC CDMA модулирует гармоническое несущее колебание со случайным образом изменяющейся частотой.

Количественное измерение LPI [5] базируется на моделях сети, предложенных в статье [7], где эти модели делятся на «распределенные» (предполагающие, что перехватчик находится внутри региона, где расположены все точки сети) и «вне сети» (перехватчик находится вдали от сети). Исследования проводились при следующих значениях основных параметров моделей:

- полный диапазон частот, в который укладывается весь спектр системы – 163,84 МГц;
- длительность сеанса связи (а следовательно, и сеанса детектирования) – $T = 0,1$ с;
- частотное расстояние между поднесущими в OFDM – $f_d = 10$ кГц;

– $T_c = 1/f_d = 0,1$ мс – длительность одного чипа;

– значение вероятности детектирования (обнаружения), определяющее факт возможности и невозможности детектирования $P_d = 0,95$.

При этих данных при изменении $N = T_T/T_c$ в диапазоне от 128 до 1024 площадь детектирования в модели dispersed менялась от 86,18 до 8,85 км².

В модели stand-off-network при изменении N в диапазоне от 256 до 1024 в зависимости от числа K активных пользователей сети минимальное расстояние детектирования менялось от 8 ($K = 2$) и 13,5 ($K = 16$) км до 2 ($K = 2$) и 4 ($K = 16$) км.

Более подробную информацию о результатах исследования можно найти в работе [5].

Однако следует отметить, что при указанных параметрах за время сеанса связи может быть передано лишь $I = T/T_c = 1000$ бит информации, независимо от того, является ли она служебной (используемой для целей синхронизации) или полезной.

Таким образом, проведенный анализ различных вариантов построения систем показывает, что во всех случаях объем информации, переданной с низкой вероятностью обнаружения, является весьма ограниченным, и в связи с этим ключевой проблемой при их разработке является реализация быстрой синхронизации.

Библиографический список

1. Simon, M. K. Spread Spectrum Communication Handbook, Electronic Edition / M. K. Simon, J. K. Omura, R. A. Scholtz, B. K. Levitt. – New York : Mc Graw-Hill, Inc., 2002. – 1229 с.
2. U.S. Patent 5029184. Low Probability of Intercept Communication System / A. F. Andren et al.; Harris Corp., 1991.
3. Chakravarthy, V. TDCS, OFDM, and MC-CDMA: a brief tutorial / V. Chakravarthy, A. S. Nunez, J. P. Stephens, A. K. Shaw, M. A. Temple // IEEE Communications Magazine. – 2005. – Vol. 43, Iss. 9. – P. 511–516.
4. Dillard, G. M. Cyclic code shift keying: a low probability of intercept communication technique / G. M. Dillard, M. Reuter, J. Zeidler, B. Zeidler // IEEE Transactions on Aerospace and Electronic Systems. – 2003. – Vol. 39, № 3. – P. 786–797.
5. Ghosal, S. A multicarrier CDMA based low probability of intercept network / S. Ghosal, D. Jalihal, K. Giridhar // IEEE Conference Publications. National Conference on Communications (NCC). – 2010. – P. 1–5.
6. Зефилов, С. Л. Анализ взаимосвязи количества переданной информации с вероятностью обнаружения факта передачи в системах с расширенным спектром / С. Л. Зефилов, А. Ю. Колотков, Н. Б. Румянцева, Б. В. Султанов // Инфокоммуникационные технологии. – 2011. – № 1. – С. 48–51.
7. Mills, R. F. Detectability models for multiple access low probability of intercept networks / R. F. Mills, G. E. Prescott // IEEE Transactions on Aerospace and Electronic Systems. – 2000. – № 36. – P. 848–858.

Султанов, Б. В.

О возможностях построения систем связи с низкой вероятностью обнаружения факта передачи информации / Б. В. Султанов, В. В. Дорошкевич, В. В. Легошин // Инжиниринг и технологии. – 2018. – Vol. 3(1). – DOI 10.21685/2587-7704-2018-3-1-6.