УДК 621.391

СИСТЕМА МНОЖЕСТВЕННОГО ДОСТУПА, ИСПОЛЬЗУЮЩАЯ НЕКОГЕРЕНТНЫЙ ПОРОГОВЫЙ ПРИЕМ, ЧАСТОТНО-ПОЗИЦИОННОЕ КОДИРОВАНИЕ И ДИНАМИЧЕСКИ ВЫДЕЛЯЕМЫЙ ДИАПАЗОН ЧАСТОТ, В УСЛОВИЯХ ПОДАВЛЕНИЯ ПОЛЕЗНОГО СИГНАЛА

Д. С. Осипов,
канд. техн. наук, старший научный сотрудник
Институт проблем передачи информации им. А. А. Харкевича РАН

Рассматривается модель системы множественного доступа, использующей динамически выделяемые поддиапазоны ортогональных частот, технологию частотно-позиционного кодирования и некогерентный пороговый прием в условиях подавления сигналов, передаваемых в системе. Для подавления используются сигналы, по форме и ширине занимаемой полосы аналогичные полезным. В работе проводится сравнение различных вариантов использования такой стратегии подавления с точки зрения их влияния на максимально возможную скорость надежной передачи информации рассматриваемым пользователем.

Ключевые слова *— система множественного доступа, динамически выделяемые частотные поддиапазоны, некогерентный пороговый прием, подавление.*

Введение

Одним из важнейших требований, предъявляемых к современным системам связи, является обеспечение защиты передаваемых данных от намеренного подавления. Это требование особенно актуально для систем множественного доступа, использующих беспроводные каналы связи, так как интенсивное развитие систем такого типа и непрерывный рост числа приложений, использующих принципы разделения пользователей в системах множественного доступа, обуславливают увеличение риска потери данных вследствие применения технологий подавления полезного сигнала и возможный урон от такого рода враждебной активности. Технология псевдослучайно переключающихся радиочастот (ППРЧ) в течение долгого времени рассматривалась в качестве наиболее эффективного метода противодействия технологиям подавления полезного сигнала. Однако развитие методов подавления привело к созданию новых технологий, специально предназначенных для подавления полезного радиосигнала в системах связи, использующих ППРЧ. В связи с этим в работе [1] была предложена модификация системы ППРЧ, использующая динамическое выделение частотных поддиапазонов и пороговый прием. Благодаря этим особенностям система такого типа оказывается намного лучше защищенной от существующих методов подавления с использованием узкополосных помех (по крайней мере, в случае, когда используется некогерентный прием). Вместе с тем исследование влияния различных стратегий подавления с использованием узкополосных помех на качество работы системы описанного типа до последнего времени не проводилось. Настоящая работа является первой попыткой восполнить этот пробел.

Система множественного доступа, использующая псевдослучайное переключение радиочастот

Для того чтобы пояснить особенности решаемой нами задачи, опишем более детально проблему множественного доступа в той ее форме, которая рассмотрена в статье. Приведем ситуацию, в которой некоторый пользователь (в дальнейшем именуемый «рассматриваемым») передает данные на базовую станцию. Предположим, что од-

новременно с рассматриваемым пользователем передачу могут вести еще K пользователей (таких пользователей станем называть «мешающими», а всех пользователей, передающих данные в такой системе, «активными»), которые руководствуются при передаче теми же принципами, что и рассматриваемый пользователь, и при этом передают информацию асинхронно и некоординированно.

Рассмотрим систему множественного доступа, использующую для разделения пользователей технологию ППРЧ. Предположим, что полоса частот, предоставленная пользователям, разбита на неперекрывающиеся частотные поддиапазоны. Каждый пользователь оснащен генератором, псевдослучайно выбирающим номер поддиапазона, в котором будет вестись передача. Собственно передача ведется с использованием заранее выбранного метода модуляции (например, частотной модуляции). Переключение между выбранными поддиапазонами традиционно именуется прыжком. Обозначим длительность промежутка между двумя прыжками T_h.

Предполагается, что приемник оснащен псевдослучайными генераторами, каждый из которых засинхронизирован с псевдослучайным генератором одного из пользователей. Последнее означает, что в момент приема сигнала, соответствующего сигналу, переданному рассматриваемым пользователем, генератор выдает номер поддиапазона такой же, как и тот, что был выдан генератором рассматриваемого пользователя (заметим, что условие синхронизации генераторов означает наличие кадровой синхронизации. Иными словами, несмотря на то, что пользователи передают информацию асинхронно, каждая пара «передатчик—приемник» должна быть засинхронизирована в вышеуказанном смысле), что позволяет приемнику определить частотный поддиапазон, который был использован рассматриваемым пользователем для передачи, а затем демодулировать принятый сигнал и принять решение о переданном символе.

Традиционно при рассмотрении систем, построенных в соответствии с вышеописанным принципом, предполагалось, что псевдослучайные номера, вырабатываемые генераторами, неизвестны никому, кроме пары «передатчик—приемник». Тем самым предполагалось, что пользователь, целью которого является подавление полезного сигнала (в дальнейшем будем называть таких пользователей «враждебными»), не может определить, какие именно диапазоны используются для передачи, и, соответственно, сформировать сигнал подавления. Однако в настоящее время появились новые типы генераторов намеренных помех, позволяющие определить поддиапазоны, используемые для передачи (этот процесс занимает сравнительно небольшую долю от величины T_h), и сформировать помеху, не позволяющую корректно принять переданный символ (такая стратегия подавления оказывается тем более эффективной, чем выше порядок модуляции, который использует рассматриваемый пользователь).

В работе [1] была предложена модификация вышеописанной системы множественного доступа, использующая динамически выделяемые частотные диапазоны. Опишем более подробно модифицированную систему такого типа, использующую пороговый прием (пример системы такого типа, использующей другой способ приема, можно найти в работе [2]).

Система множественного доступа, использующая динамически выделяемые частотные диапазоны, ППРЧ и пороговый прием

Рассмотрим ситуацию, в которой $\tilde{K} = K + 1$ пользователей ведут передачу данных на базовую станцию независимо, асинхронно и некоординированно, руководствуясь одними и теми же принципами. Пусть используемая полоса частот разбита на Q непересекающихся частотных подканалов (проще и эффективнее всего реализовать это условие, применяя технологию ортогонального мультиплексирования частот OFDM, поэтому в дальнейшем мы будем рассматривать систему, в которой используется именно эта технология). В системе и передатчик, и приемник оснащены засинхронизированными генераторами, которые псевдослучайно выбирают (без повторений) q из Q номеров подканалов. Каждый пользователь передает q-ичные символы, и каждому из них поставлен в соответствие один из выбранных генератором подканалов. При передаче i-го символа пользователь передает сигнал в подканале, поставленном в соответствие этому символу.

Используя сигналы, принятые из подканалов выбранных генератором номеров подканалов, приемник вычисляет для каждого из них некоторую статистику и сравнивает каждое из вычисленных значений с некоторым порогом. В случае если превышение порога регистрируется в одном из подканалов, то принимается символ, поставленный в соответствие этому подканалу. В противном случае принимается решение о стирании. Если принятый символ отличается от переданного, говорят об ошибке.

Таким образом, описанная система может рассматриваться как модифицированный вариант системы с ППРЧ, использующей частотное манипулирование и пороговый прием. Отличие состоит в том, что в этом варианте поддиапазоны фик-

сированы, в то время как в описанной нами системе частотные поддиапазоны (представляющие собой наборы непересекающихся подканалов) выделяются динамически. В первом случае пользователь, получивший доступ к информации о характере распределения подканалов (например, вошедший в систему как легальный пользователь), может, анализируя спектр, восстановить номера поддиапазонов, которые уже используются, и, посылая сигналы в других подканалах тех же диапазонов, генерировать стирания в последовательностях, принимаемых другими пользователями. В результате пользователь, обладая достаточными энергетическими ресурсами, может сделать надежную передачу данных легальными пользователями (или, по крайней мере, значительной их части) невозможной. В системе с динамическим выделением диапазонов применение такой стратегии подавления невозможно, так как используемый для передачи каждого следующего символа поддиапазон известен лишь паре «передатчик—приемник» и выбирается вновь для передачи каждого следующего символа.

Рассмотрим систему описываемого типа, использующую прием по мощности. Такая система существенно лучше защищена от подавления сигналами, передаваемыми непосредственно в подканалах, используемых рассматриваемыми пользователями, по сравнению с системой, использующей другой вид приема или тип модуляции, так как в среднем энергия принятого сигнала возрастает. Именно эта техника подавления будет рассмотрена ниже. Для того чтобы охарактеризовать функционирование системы рассматриваемого типа в условиях подавления с использованием сосредоточенной помехи, заметим, что каждый из множества «восходящих» каналов в описанной нами системе представляет собой по сути q-ичный дискретный канал без памяти со стираниями, который в свою очередь может быть представлен как композиция симметричного q-ичного дискретного канала без памяти C1 и стирающего канала C2 (под стирающим каналом здесь подразумевается канал, в котором каждый символ переходит или сам в себя, или в стирание). Аналитическое выражение для пропускной способности канала вышеуказанного типа, характеризующегося вероятностью ошибки p_e и вероятностью стирания p_x, было получено в явном виде [3]:

$$C(p_e, p_x) = [\log_2 q + (1-\tilde{p}_e)\log_2(1-\tilde{p}_e) + \\ + \tilde{p}_e \log_2 \tilde{p}_e - \tilde{p}_e \log_2(q-1)](1-p_x),$$

где $\tilde{p}_e = \dfrac{p_e}{1-p_x}$ — вероятность ошибки в канале C1.

Следует отметить, что пропускная способность такого канала имеет смысл максимальной скорости, с которой пользователь, применяя описанный выше метод передачи, может «надежно» (здесь этот термин используется в том же смысле, что и в работе [4]) вести передачу данных по каналу, характеризуемому вероятностью ошибки p_e и вероятностью стирания p_x. Последние в действительности являются функциями как параметров, которые фиксируются на этапе проектирования (общее число подканалов; число подканалов, предоставляемых каждому из пользователей), и которыми не может управлять ни пользователь, ни проектировщик (отношение сигнал/шум, количество мешающих пользователей), так и такими параметрами, как величины порогов, которые должны выбираться. Здесь и далее будем рассматривать систему с идеальным контролем мощности, что в частности означает, что все пороги можно выбрать одинаковыми и равными Tr. Обозначим максимально возможную скорость передачи, о которой говорилось выше, как R:

$$R(Q, q, SNR, K, Tr) = C(p_e(Q, q, SNR, K, Tr), \\ p_x(Q, q, SNR, K, Tr)).$$

При условии, что все прочие параметры зафиксированы, величину порога разумно выбрать таким образом, чтобы R максимизировалась. Полученное максимальное значение

$$R_m = R_m(Q, q, SNR, K) = \max_{Tr} R_m(Q, q, SNR, K, Tr).$$

Это и есть наибольшая скорость, с которой пользователь может надежно передавать сообщения при данных значениях Q, q, K и SNR, используя вышеописанный метод передачи. Следует подчеркнуть, что эта величина не тождественна пропускной способности канала «вверх», так как методы приема и передачи фиксированы.

Функционирование системы множественного доступа описываемого типа в условиях подавления с использованием сосредоточенной помехи

Рассмотрим систему множественного доступа описанного выше типа, использующую канал с аддитивным белым гауссовым шумом, в которой мощность передаваемых сигналов выбирается таким образом, чтобы мощность сигналов на приемном конце была одинакова и равна P.

Ниже будет рассмотрена ситуация, в которой враждебный пользователь использует для подавления сигналы, аналогичные полезным, т. е. имеющие такую же форму и занимающие полосу частот той же ширины, что и любой из полезных сигналов. Следует учесть, что формирование сигнала, антиподального подавляемому, является тех-

нически нереализуемым. (Так, в реальной системе, построенной в соответствии с вышеописанными принципами, в случае, когда X стремится подавить сигнал, который пользователь A передает пользователю B для того, чтобы сформировать соответствующий сигнал X, необходимо в частности удовлетворительно оценить параметры сразу трех различных каналов: AX, XB и AB.) Будем полагать, что сигнал, который формируется враждебным пользователем, имеет случайную фазу.

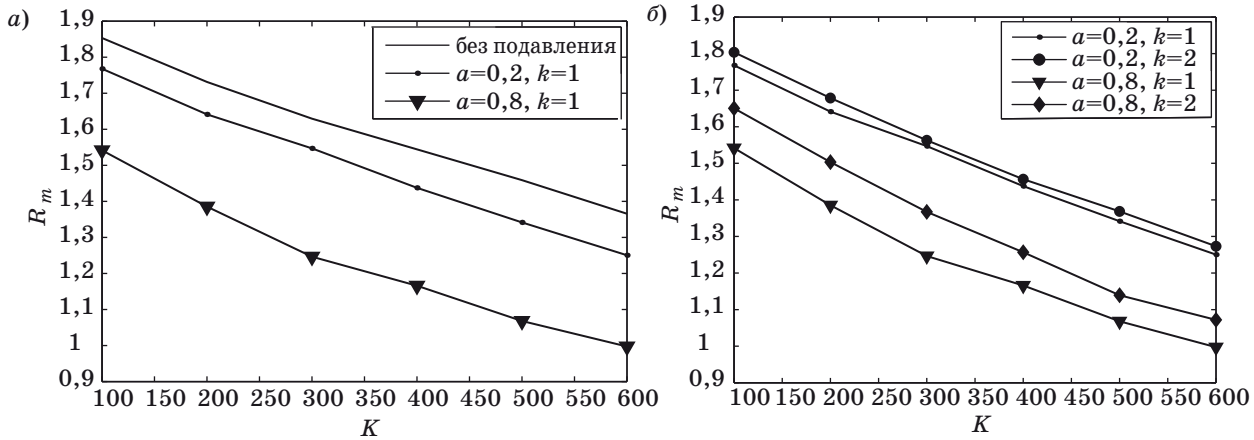
Заметим, что рассматриваемая стратегия удобна для враждебного пользователя, так как позволяет ему имитировать работу легальных пользователей и тем самым затрудняет обнаружение, и потому предлагаемая модель представляется вполне реалистичной. Вместе с тем в настоящей работе предполагается, что враждебный пользователь обладает энергетическими ресурсами большими, чем любой из легальных пользователей, т. е. как мощность каждого из сигналов, переданных враждебным пользователем, на приемном конце, так и количество сигналов, передаваемых рассматриваемым пользователем, могут быть больше (возможно, существенно больше), чем соответствующие значения для легального пользователя.

Будем считать, что враждебный пользователь способен определить подканалы, в которых ведется передача, за время τ ($\tau = gT$, $g << 1$) и сгенерировать $A = aK$ сигналов, передаваемая мощность которых такова, что мощность соответствующих сигналов на приемном конце оказывается равной $\tilde{P} = kP$, где P — мощность сигнала от легального пользователя на приемном конце. Прежде всего, рассмотрим случай (рисунок, *а*), когда $k = 1$, а количество сигналов в одном случае относительно невелико по сравнению с числом активных пользователей ($a = 0{,}2$), а во втором, напротив, сравнимо с числом активных пользователей ($a = 0{,}8$). Здесь и далее для моделирования будут использоваться следующие значения системных параметров: $Q = 4096$, $q = 4$, $SNR = 10$ дБ, $\tau = 0{,}1T$ и изменения значения числа мешающих пользователей в диапазоне значений от 100 до 600. Для сравнения приводятся значения R_m (в битах на OFDM-символ) для случая, когда подавление полезных сигналов не происходит.

Как видно из рисунка, увеличение числа подавляемых полезных сигналов A ожидаемо ведет к снижению значения максимальной скорости передачи. Тем не менее даже для сравнительно большого числа A уменьшение значения максимальной скорости передачи составляет не более 0,4 бита на один OFDM-символ (т. е. не более 20 % от максимально возможной для данного случая скорости 2 бита на один OFDM-символ). Для случая же, когда враждебный пользователь обладает существенно меньшими ресурсами (т. е. способен подавлять не более 20 % от общего числа активных пользователей), уменьшение скорости и вовсе составляет не более 0,1 бита на OFDM-символ (т. е. менее 5 % от максимально возможной скорости).

Рассмотрим теперь ситуацию (рисунок, *б*), в которой каждый из генерируемых враждебным пользователем сигналов имеет мощность большую, чем сигналы, которые используют легальные пользователи. Приведены графики для случаев $k = 1$ (мощность сигналов подавления равна мощности полезных сигналов) и $k = 2$ (мощность сигналов подавления в два раза больше мощности полезных сигналов).

Как видно из вышеприведенного графика, увеличение мощности не приводит к снижению максимально возможной скорости передачи данных. Напротив, при использовании такой техни-



■ *Зависимость максимально возможной скорости передачи от числа мешающих пользователей: а — при различном числе сигналов подавления и при отсутствии таковых; б — для различных значений числа подавляемых полезных сигналов и значений мощности сигналов преднамеренной помехи*

ки максимальная скорость передачи лишь увеличивается, причем когда сигналов подавления больше, рост этой величины оказывается более значительным, чем когда число сигналов, используемых для подавления, сравнительно невелико. Это, по-видимому, можно объяснить тем, что при сравнительно большом числе подканалов, в которые передаются сигналы подавления, вероятность того, что и сигнал от рассматриваемого пользователя окажется в числе подавляемых, возрастает. Следует отметить, что использование сигналов большей мощности лишь увеличивает среднюю мощность. Когда число сигналов сравнительно велико, это означает, что существенно снижается вероятность ошибки, так как для ошибки необходимо, чтобы порог в подканале, по которому передается полезный сигнал, не был превышен, а вероятность такого исхода уменьшается с ростом средней мощности передаваемых сигналов.

Заключение

Результаты, полученные в ходе имитационного моделирования системы описанного типа, позволяют сделать некоторые выводы относительно эффективности различных вариантов рассмотренной нами стратегии подавления. В целом, описанная выше система множественного доступа отличается хорошей устойчивостью к такой стратегии подавления, как намеренная передача сигналов, имитирующих сигналы легальных пользователей, в подканалах используемых легальными пользователями для передачи. Сравнение различных вариантов реализации этой стратегии с точки зрения снижения эффективности передачи данных легальными пользователями свидетельствует о том, что увеличение мощности передаваемых сигналов нерационально, поскольку не приводит к более эффективному подавлению. Анализ результатов моделирования показывает, что более рациональным способом использования энергетического преимущества для целей подавления является перераспределение энергии для увеличения числа подканалов, в которых происходит подавление, однако даже использование значительного числа сигналов подавления не приводит к существенному ухудшению эффективности передачи данных.

Литература

1. **Зяблов В., Осипов Д.** Об оптимальном выборе порога в системе множественного доступа, основанной на перестроении ортогональных частот // Проблемы передачи информации / ИППИ РАН. 2008. Т. 44. Вып. 2. С. 23–31.
2. **Osipov D.** On the probabilistic description of a FH-OFDMA with a MAXP receiver // Problems of redundancy in information and control systems / Proc. of the XII Symp., St.-Petersburg, May 26–30, 2009. P. 144–149.
3. **Грошев Ф. В., Осипов Д. С.** Исследование пропускной способности системы множественного доступа с пороговым приемом // Информационные технологии и системы: Сб. 32-й конф. молодых ученых и специалистов ИППИ РАН, Бекасово, Россия, 15–18 декабря 2009 г. С. 152–155.
4. **Галлагер Р.** Теория информации и надежная связь. — М.: Сов. радио, 1974. — 720 с.